ESTUDIO DE INGENIERÍA SOCIAL EN EL USO DE LAS REDES SOCIALES

CLAUDIA PATRICIA FLÓREZ RAMÍREZ

HAROLD MÉNDEZ COLLO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

BOGOTÁ D.C.

2017

ESTUDIO DE INGENIERÍA SOCIAL EN EL USO DE LAS REDES SOCIALES

CLAUDIA PATRICIA FLÓREZ RAMÍREZ

HAROLD MÉNDEZ COLLO

PROYECTO DE GRADO

DIRECTOR DEL PROYECTO

DOCENTE SALOMÓN GONZÁLEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

BOGOTÁ D.C.

2017

Nota de aceptación:

_____

_____

_____

_____

Firma del presidente del jurado

_____

Firma del jurado

_____

Firma del jurado

Santiago de Cali, 29 de Noviembre del 2017

DEDICATORIA

Este proyecto de seguridad informática lo dedico a mi familia, porque me han dedicado la ayuda, paciencia y la fuerza que día a día me han brindado para continuar con mis sueños de lograr los objetivos propuestos en mi proyecto de vida, gracias a Dios todo fue posible.

AGRADECIMIENTOS

Agradezco en primer lugar a Dios, por brindarme la oportunidad de vivir, por darnos las fuerzas necesarias para superar todos los obstáculos y complicaciones que se nos presentaron a lo largo del proyecto, por permitir disfrutar cada momento de mi vida y poder cumplir mis objetivos o metas trazados en mi proyecto de vida.

Le damos un agradecimiento al tutor Salomon Gonzalez, por ayudarme a corregir y guiarme paso a paso durante el trascurso del proyecto. Motivándome cada día y mostrando los puntos claros para mejorar y darme soluciones, también por su disposición para cualquier consulta tanto en vía correo o skype. Además, de agradecer su paciencia, el tiempo y su dedicación que tuvo para que este proceso investigativo culminara de una manera exitosa.

Por último, mi familia que me ha apoyado en el logro de mi proyecto de vida y por brindarme una excelente educación que me servirá en el ámbito profesional y poder transmitir ante la sociedad.

CONTENIDO

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE GRÁFICAS

Pág.

LISTA DE ANEXOS

Pág.

GLOSARIO

AMENAZAS: causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización[1].

ANTIVIRUS: es una categoría de software de seguridad que protege un equipo de virus, normalmente a través de la detección en tiempo real y también mediante análisis del sistema, que pone en cuarentena y elimina los virus. El antivirus debe ser parte de una estrategia de seguridad estándar de múltiples[2].

CONTRASEÑA: cadena exclusiva de caracteres que introduce un usuario como código de identificación para restringir el acceso a equipos y archivos confidenciales. El sistema compara el código con una lista de contraseñas y usuarios autorizados. Si el código es correcto, el sistema permite el acceso en el nivel de seguridad aprobado para el propietario de la contraseña[3].

EXPLOITS: los programas intrusos son técnicas que aprovechan las vulnerabilidades del software y que pueden utilizarse para evadir la seguridad o atacar un equipo en la red[4].

FIREWALL: un firewall es una aplicación de seguridad diseñada para bloquear las conexiones en determinados puertos del sistema, independientemente de si el tráfico es benigno o maligno. Un firewall debería formar parte de una estrategia de seguridad estándar de múltiples niveles[5].

---

[1] Guía para la Implementación de Seguridad de la Información en una MIPYME. [En línea]. Bogotá: MINTIC. 2016., 31 p. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_Guia_Seguridad_informacion_Mypimes.pdf.
[2] Op. cit., p. 6.
[3] Op. cit., p. 8.
[4] Op. cit., p. 8.
[5] Op. cit., p. 9.

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[6].

INGENIERÍA SOCIAL: método utilizado por los atacantes para engañar a los usuarios informáticos, para que realicen una acción que normalmente producirá consecuencias negativas, como la descarga de malware o la divulgación de información personal. Los ataques de phishing con frecuencia aprovechan las tácticas de ingeniería social[7].

MALWARE: el malware es la descripción general de un programa informático que tiene efectos no deseados o maliciosos. Incluye virus, gusanos, troyanos y puertas traseras. También se propaga a través de descargas inadvertidas y ataques a las vulnerabilidades de seguridad en el software. La mayoría del malware peligroso actualmente busca robar información personal que pueda ser utilizada por los atacantes para cometer acciones delictivas[8].

PHISHING: método más utilizados por delincuentes cibernéticos para estafar y obtener información confidencial de forma fraudulenta como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria de la víctima[9].

[6] BERMÚDEZ PENAGOS, Edilberto. Ingeniería Social, un factor de riesgo informático inminente en la universidad cooperativa de Colombia. Trabajo de investigación especialista en seguridad informática. Neiva. Universidad Nacional Abierta y a Distancia. Facultad de educación, 2015. 116 p.
[7] Op. cit., p. 9.
[8] Op. cit., p. 17.
[9] Op. cit., p. 10.

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[10].

[10] BERMUDEZ. Op. cit., p. 13.

RESUMEN

Este proyecto pretende identificar las debilidades de la seguridad de la información dentro de la Universidad del Valle, realizando un estudio a partir de la técnica de ataque en Ingeniería Social. Para ello se utilizaron técnicas de recolección de datos como la observación, encuestas y entrevistas.

Al final, con la información ya analizada y tabulada, se realizan las conclusiones acordes a los hallazgos de la investigación y se generan un conjunto de recomendaciones que buscan corregir las fallas encontradas y aumentar la seguridad de la información en la Universidad del Valle, planeando una cultura de protección de la información y de buenas prácticas de usuario en el recurso humano de la universidad[11].

Palabras clave: Ingeniería Social, virus, hacker, privilegios, delincuentes informáticos, criminales, sistemas de información, phishing, exploits, contraseña, antivirus.

[11] BERMUDEZ. Op. cit., p. 14.

INTRODUCCIÓN

El presente proyecto cumple con la referencia en la parte de la seguridad social y el impacto que se lleva a cabo acerca de los delitos informáticos que hoy en día son muchas de las personas que se comunican entre sí, en lo específico en el uso de las redes sociales[12]. 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.

El propósito de esta investigación es socializar la importancia y generar cultura en las personas, para que tengan cuidado al momento de acceder a publicar sus datos personales en internet. 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.

[12] Redes Sociales, una red social es una plataforma en línea que permite relacionar gente entre sí. Esta gente puede compartir intereses, actividades, conexiones en la vida real, un juego específico, etc.

1 DEFINICIÓN DEL PROBLEMA

Las vulnerabilidades a la información 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. Inicialmente las empresas en el mundo no son ajenas de las fallas de seguridad en cuanto a 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[13] los causantes de la pérdida o fuga de información en los ambientes informáticos empresariales o familiares, sino el uso y ejecución de las diferentes medios, modalidades o métodos enmarcados dentro de la Ingeniería Social.

Teniendo en cuenta lo descrito anteriormente y como punto de partida dentro de este proceso investigativo, se formula las siguientes preguntas:

¿Cuáles son las vulnerabilidades más comunes en la seguridad de la información y que hacen factible un ataque de Ingeniería Social al personal de la Universidad del Valle?

¿Cuales son las técnicas más utilizadas de Ingenería Social para el robo de la información de las redes sociales en la Universidad del Valle?

[13] Troyano, se denomina caballo de troya o troyano, a un software malicioso que se presenta al usuario como un programa aparentemente legítimo e inofensivo, pero que, al ejecutarlo, le brinda a un atacante acceso remoto al equipo infectado.

2 JUSTIFICACIÓN

Investigar sobre ingeniería social en el uso de las redes sociales dentro de la Universidad del Valle, para determinar las vulnerabilidades en las redes sociales de las personas que están en la universidad.

Por tal razón se hace importante el reconocimiento, primero; de que la información es el activo[14] 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.

Los resultados de esta información pueden ser útiles para que en el futuro se logre generar cultura y permitan resolver algunos de los problemas de ingeniería social que presenten en las universidades.

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 la mejora del ambiente laboral.

[14] Activo, son aquellos recursos (Hardware y Software) con los que cuenta una empresa.

3 OBJETIVOS

3.1 OBJETIVO GENERAL

Realizar un estudio sobre ingeniería social, en el uso de las redes sociales, aplicando metodologías, técnicas, para obtener el estado de vulnerabilidad de las personas en la sede de la universidad del valle.

3.2 OBJETIVOS ESPECÍFICOS

Realizar un levantamiento de la información en cuanto al estado actual, metodologías y antecedentes de la Ingeniería Social en universidades.

Determinar las técnicas de ingeniería social para aplicar a las personas de la universidad del valle demostrando 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 universidad.

Realizar la encuesta a la población y de esta forma obtener la información para procesarla y presentar los resultados; involucrando todos los sujetos, material y procedimiento que se investigaran directa o indirectamente en la investigación realizando un estudio sobre ingeniería social en el uso de las redes sociales, para obtener el estado de vulnerabilidad de las personas en la Universidad del Valle, en la ciudad de Cali.

4 MARCO REFERENCIAL

4.1 MARCO TEÓRICO

4.1.1 Antecedentes. Uno de los últimos alcances en la seguridad informática ha sido enfocado a las redes de datos, que nace de la integración de las tecnologías de las comunicaciones y computación. El nacimiento de las Redes en Internet trata acerca de culminar el siglo XX, exactamente el año de 1997, desde esa fecha hasta hoy numerosos sitios de redes sociales que se han creado, no todos han corrido con la misma suerte, unos tienen más usuarios y más fama que otros debido a que son más atractivos y proporcionan mejores servicios.

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"[15]. 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"[16] en el mercado, lo que puso en perspectiva un panorama que prometía generar grandes ganancias, el de la protección de la información.

[15] RAMÍREZ SANDOVAL, Jorge Iván; DÍAZ MARTÍNEZ, José Vicente y GARIZURIETA MEZA, Miguel Hugo. "Ingeniería Social, una amenaza informática". [en línea], septiembre 2009 [citado en 25 abril de 2017]. Disponible en Internet: http://es.scribd.com/doc/19394749/Ingenieria-social-una-amenaza-informatica>.

[16] FICARRA, Francisco. "Los virus informáticos: Entre el negocio y el temor". Revista Latinoamericana de Comunicación CHASQUI [en línea], junio 2002 [citado en 25 abril de 2017]. Disponible en Internet: . ISSN 1390-1079.

Se ha desarrollado estudios e investigaciones en el día a día sobre la seguridad informática, como son los proyectos de grado relacionados con el tema. La cuál existe una guía para que en las propias universidades, es decir las personas encargadas del área de sistemas se encarguen de revisar todo lo relacionado con la seguridad a partir de sus propias políticas basadas en los pasos planteados y en el presente del trabajo, el papel importante de concientizarse y de llevar a cabo todo lo implementado, actualizado y socializado para la comunidad académica.

Un caso 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 cuales 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"[17]. Otra prueba más de que los ciber-delincuentes están a la orden del día.

Pero esta problemática 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

[17] EL ESPECTADOR. "Hackean cuentas de correo de candidatos a rectoría de la Universidad Nacional" [en línea], marzo 2015 [citado en 25 abril de 2017]. Disponible en Internet: <http://www.elespectador.com/noticias/educacion/hackeancuentas-de-correo-de-candidatos-rectoria-de-uni-articulo-549936>.

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…"[18] .

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"[19], entre ellas: Harvard y Princeton.

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[20] 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.

[18] 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-paginaweb-de-la-universidad-catolica-con-sitios-pornograficos.shtml>.

[19] B:SECURE. "Hackean a la Universidad de Stanford para hurtar datos de su sistema" [en línea], julio 2013 [citado en 25 abril de 2017]. Disponible en Internet: <http://www.bsecure.com.mx/featured/hackean-a-la-universidad-de-stanford-parahurtar-datos-de-su-sistema/>.

[20] AGENCIA EFE. "Supuestos yihadistas piratean dos portales de una universidad brasileña" [en línea], enero 2015 [citado en 7 abril de 2017]. Disponible en Internet: <http://www.caracol.com.co/noticias/internacionales/supuestos-yihadistaspiratean-dos-portales-de-una-universidad-brasilena/16173/nota/2591949.aspx>.

En febrero del año 2015 condenaron a un estudiante de Los Andes por manipular el sistema de calificaciones. “Alejandro Robayo estaba en último semestre de ingeniería industrial cuando violó la plataforma de notas de su universidad y modificó algunas de sus calificaciones. Él, un estudiante destacado y becado en la Universidad de los Andes, había sacado notas bajas en algunos parciales de ese semestre, el primero de 2013, y se vio tentado a cambiarlas para no perder el privilegio de la beca ni bajar su promedio. Solo le faltaban unas pocas materias y entregar la tesis para recibir el grado. Al principio lo hizo sólo para beneficio personal, pero luego quiso lucrarse y ofreció sus servicios a otros estudiantes de la misma institución académica. Según la Unidad de Delitos Informáticos de la Dijín, que realizó la investigación, más de 20 estudiantes pudieron haberle pagado a Robayo por cambiar notas y planillas de asistencia a clases”[21].

Otro ataque fue el 6 de marzo del 2016, donde “el grupo de hackers colgó un manifiesto, que quedó en la web de la institución educativa aproximadamente por una hora y media. El grupo de hackers conocido como Anonymous atacó el sitio web de la Universidad de los Andes este domingo desde las 9:30 de la mañana, al parecer desde el exterior. Cambiaron los contenidos e inhabilitaron los accesos a las páginas de apoyo financiero, posgrados, biblioteca, entre otras. Ortega detalló que “lo que hicieron básicamente fue paralizar los sitios y colgar un manifiesto en la página de maestrías, que quedo en la web aproximadamente por una hora y media”. Anonymous es un grupo de ciberactivistas que no pertenece a ningún partido político y se encuentran distribuidos por varios países. Son reconocidos por su lema de que el conocimiento es libre. En Colombia este grupo de hackers atacó por más de 18 horas la página web de la Policía Nacional, en respuesta a lo que

[21] EL ESPECTADOR. “Universidades, víctimas de “hackers””. [En línea]. Mayo 2015. [25 abril de 2017]. Disponible en: http://www.elespectador.com/noticias/judicial/universidades-victimas-de-hackers-articulo-560884.

consideraron un abuso de autoridad, apoyando, de esta manera, una movilización convocada contra las autoridades por parte de Los indignados”[22].

Toda la comunidad universitaria tiene instituciones muy vulnerables a los ataques informáticos por los ciberdelincuentes, por lo tanto podemos decir que algunos usuarios que se conectan a las redes de datos pueden llegar a poseer cuentas para acceder a estos sistemas, junto con otros factores en las cuales nos brindan una gran importancia y relevancia necesaria para este tipo de seguridad en la información por parte de sus 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.

4.1.1.1 Ingeniería Social. Este término ha adquirió relevante importancia a pesar de que su existencia es desde hace muchísimo tiempo atrás. Es una conversación tan trivial el simple hecho de sacar la información a una amistad (edad y fecha del cumpleaños por ejemplo) o a un profesor las posibles preguntas de una examen final son formas "básicas" de hacer ingeniería social. Por qué el único objetivo es obtener información valiosa, el ingeniero social realiza esta técnica para obtener la información de las personas sin que se dé cuenta que ha sido una victima de un delito informático.

[22] EL ESPECTADOR. “Anonymous ataca el sitio web de la Universidad de los Andes”. [En línea]. Marzo 2016. [25 abril de 2017]. Disponible en: http://www.elespectador.com/noticias/actualidad/anonymous-ataca-el-sitio-web-de-universidad-de-los-ande-articulo-620617.

Auque algunas técnicas se pueden llevar a cabo a través de varios medios de comunicación y los ataques de ingeniería social suelen ser multifacéticos, podemos clasificarlos dependiendo de:

- El tipo: los aspectos más importantes para el éxito del ataque ser cualidades sociales, físicas o técnicas.
- El operador: el ataque se ejecuta con una persona o se puede automatizar con un software.
- El canal: el medio por el cual se lleva a cabo el ataque es el e-mail, la mensajería instantánea, el teléfono, una red social, la nube, una página web o en persona.[23]

4.1.1.2 Tipos de ingeniería social. El ser humano es el eslabón más débil dentro de la seguridad informática así que de nada sirve un antivirus o un firewall actualizados debido que mediante una conversación, un correo electrónico o una llamada en donde prima el engaño se pueden obtener datos privados de la víctima. Por tal motivo esta es la razón de este tipo de ataques es muy difícil defenderse ya que no se puede eliminarse con software o hardware, simplemente se puede minimizar el riesgo de sufrir estos ataques con el conocimiento de que existen estas técnicas de engaño.

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

[23] K. Krombholz, H. Hobel,M. Huber and E. Weippl "Advanced Social Engineering Attacks". Web https://www.sba-research.org/wp-content/uploads/publications/jisa_revised.pdf.

confidencialidad, integridad y disponibilidad de su sistema de información"[24].

Tabla 1 Intereses de los delincuentes en la elección de la víctima.

INTERESES	DESCRIPCIÓN	OBSERVACIÓN
Personal	Interés propio para obtener datos personales y confidenciales.	El atacante lleva a cabo un proceso de inteligencia e investigación para conocer a la víctima más a fondo: sus familiares y amistades; sus amigos cercanos que comentan en fotos y videos; sus temas de interés, aficiones, hobbies; los lugares que frecuenta usualmente, etc. Toda la información que pueda encontrarse visible en su perfil para planificar el engaño y ganarse a la víctima generando confianza antes de atacar.
Financiero	Ofrece este tipo de servicios tales como "investigador" a cambio de cobrar por el ataque.	
Auto superación	Por gusto, para llevar acabo sus propias habilidades y probar la efectividad de diferentes técnicas y situaciones.	

4.1.1.3 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.

Suplantación de identidad. En este método el ingeniero social asume un personaje que represente autoridad o necesidad, por ejemplo: puede

[24] 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-seguridadinformatica?start=1>.

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 electrónico. 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.

Espiar por encima del hombro (Shoulder Surfing[25]). 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 antiespías en las pantallas de los dispositivos móviles como celulares o tabletas.

[25] Santabaya, C. (2017). Ingeniería Social : Cuáles son los tipos de ataque, 1–6. Retrieved from http://www.redusers.com/noticias/ingenieria-social-cuales-son-los-tipos-de-ataque/

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.

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.

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].

[26] HINOJOSA JARAMILLO, Op. cit., p. 57.

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.

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 email 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].

.

4.1.1.4 Ingeniería Social basada en computadores. Son métodos que usan la ingeniería social 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.

[27] Ibid., p. 60.

Phishing. El "phishing" es una forma donde el delincuente busca un objetivo con el cual se encarga de intentar y obtener de un usuario sus respectivos datos, claves, cuentas bancarias, números de tarjeta de crédito, identidades, y entre otras. Se concluye como el termino "todos los datos posibles" con el fín de ser usados de forma fraudulenta. Se puede resumir de forma fácil, engañosa al posible estafador, "suplantando la imagen de una empresa o una entidad publica", de esta manera se hacen "creer" a la posible víctima que realmente este tipo de datos solicitados proceden del sitio "Oficial" cuando en realidad no lo es.

Los sitios Web a visitar en la dirección URL en la barra de direcciones. NUNCA POR ENLACES PROCEDENTES DE CUALQUIER SITIO. Las entidades bancarias contienen certificados de seguridad y cifrados seguros NO TENGA MIEDO al uso de la banca por internet[28].

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].

[28] ASÓCIAT. “Qué es el phishing y cómo protegerse.”. [En línea]. Mayo 2005. [25 abril de 2017]. Disponible en: http://seguridad.internautas.org/html/451.html.

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

La instalación de estas aplicaciones se puede acarrear en una de las pérdidas o el secuestro de la información, la cual lleva a permitir que se alojen en la computadora o en otra serie de virus, que a su vez pueden convertirse en un zombi para lanzar un ataque escalado, y puede abrir puertas traseras o inundarla de publicidad. Lo mismo sucede con los programas de “tuning” que surgen en acelerar el funcionamiento de las computadoras pero que al final resultan ser software malicioso.

Por esta razón es importante contar con un software antivirus licenciado y actualizado, y por supuesto, hacer uso de las buenas prácticas de usuario.

Spam. Este nombre como lo indica es aquel nombre que llamamos spam, y que se encuentra en el correo en la parte de basura o sms basura a estos mensajes no solicitados, habitualmente este tipo publicitario, son enviados en cantidades masivas que por lo tanto se perjudican de una u otra manera al receptor. Aunque este tipo de mensajes se puede hacer por distintas vías, pero la más fácil y utilizada entre el público en general es la que se lleva al el correo electrónico. Otro tipo de tecnologías de Internet han sido objeto de que el correo basura se incluyen grupos de noticias usenet, motores de búsqueda, wikis, foros, blogs, también a través de popups, tipos de imágenes y textos en la Web[30].

[30] CASTELLANOS CRESPO, Raquel. Instalación y administración de servicios de correo electrónico. [En línea]. Bogotá: Servicios de red e internet. 2016., 31 p. Disponible en: https://seguridadasir.files.wordpress.com/2012/02/tema_6.pdf.

El correo basura además puede tener como objetivo los teléfonos móviles (a través de mensajes de texto) y los sistemas de mensajería instantánea como por ejemplo Outlook, Kmail, Webmail, etc[31].

Igualmente se llama spam a los virus sueltos en la red y páginas filtradas (casino, sorteos, premios, viajes y pornografía), se activa cuando se accede por medio de links cuando se ingresa a páginas de comunidades o grupos[32].

Estás son algunas de los casos que observamos diariamente con el uso del correo electrónico, esto lleva a que al final nuestra laptop en el menor de los casos sea infectada con cualquier programa maligno (malware), a continuación algunos ejemplos más comunes a diario en nuestras redes.

Algunos ejemplos que se pueden citar:

- La ejecución de un virus troyano por parte del usuario, adjunto a un correo electrónico enviado por una dirección que le es familiar o simplemente con un interesante título al destinatario como "es divertido, pruébalo", "mira a Shakira desnuda", etc.
- También lo podemos ver con este típico asunto en que promueve mensajes publicitarios y cosas del estilo "hágase millonario mientras duerme".
- Descarga los últimos emoticones de este link y disfruta de las nuevas variedades.[33]

[31] Ibíd., p. 30.
[32] Ibíd., p. 30.
[33] UNIR. “La Ingeniería Social, acercándonos a los molestos Spam, Phishing y Hoax”. [En línea]. Mayo 2008. [25 abril de 2017]. Disponible en: http://www.monografias.com/trabajos60/ingenieria-social-spam/ingenieria-social-spam2.shtml#xspam.

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[34].

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.

4.1.1.5 Seguridad informática. De un tiempo acá las Redes Sociales se han convertido como una de las partes de la vida cotidiana de los internautas ya sea por moda o por necesidad lo cierto es que muchos usuarios de internet la utilizan. Podemos decir es que donde la seguridad comienza a verse seriamente afectada ya que los malhechores informáticos (crackers, phishers y/o hackers) la cual se refleja en una enorme cantidad de información que puede ser obtenida sobre todo cuando hay gente que por negligencia o descuido la comparte.

4.1.1.6 Mecanismos de seguridad. Todo aquello de naturaleza hardware como software que se utiliza para crear, reforzar y mantener la seguridad informática.

[34] "What is a pop-up ad?". Microsoft.

Se clasifican en:

- Preventivos: Actúan antes de que se produzcan ataques. Su misión es evitarlos.
- Detectores: Actúan cuando el ataque se ha producido y antes que cause daños en el sistema.
- Correctores: Actúan después de que haya habido un ataque y se hayan producido daños. Su misión es la de corregir las consecuencias del daño.

4.1.1.7 Clasificación de ataques

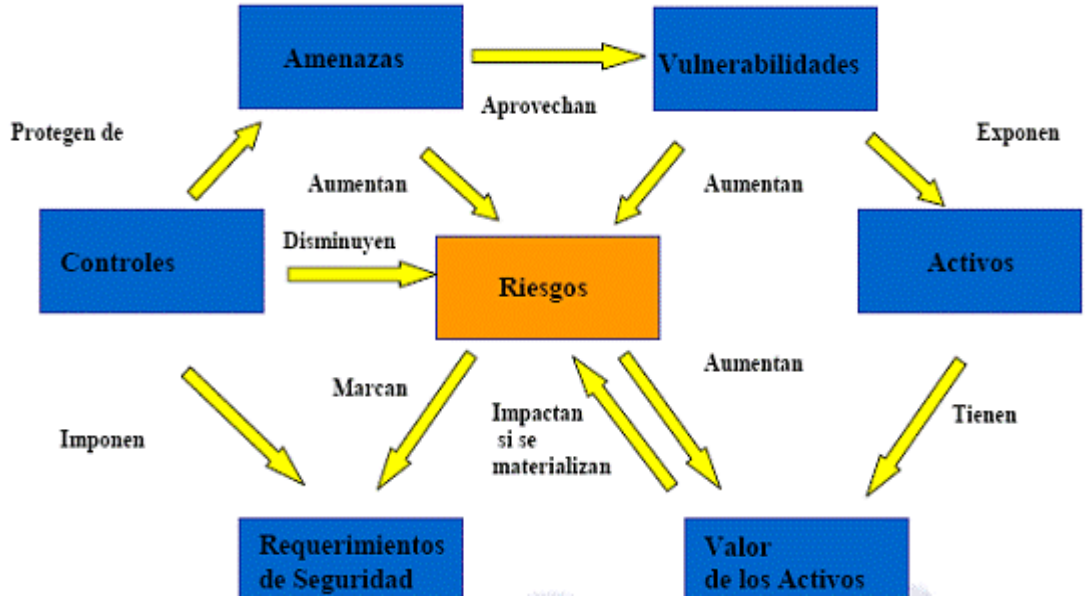
Ataques Pasivos: Consiste en sólo observar comportamientos o leer información, sin alterar el estado del sistema ni la información. En este sentido, un ataque pasivo sólo afecta la confidencialidad o privacidad del sistema o de la información[35].

Ataques Activos: Por el contrario, tiene la capacidad de modificar o afectar la información o el estado del sistema o ambos. En consecuencia, un ataque activo afecta no sólo la confidencialidad o privacidad sino también la integridad y la autenticidad de la información o del sistema[36].

Riesgos: Se denomina riesgo a la posibilidad de que se materialice o no una amenaza aprovechando una vulnerabilidad[37].

[35] SORIANO, Miguel. Seguridad en redes y seguridad de la información. [En línea]. Bogotá: Improvet. 2017., 80 p. Disponible en: http://improvet.cvut.cz/project/download/C2ES/Seguridad_de_Red_e_Informacion.pdf.
[36] SORIANO. Op. cit., p. 14.
[37] SORIANO. Op. cit., p. 34.

Figura 1 Riesgos



Fuente: http://www.iso27000.es/download/doc_sgsi_all.pdf [38]

4.1.2 Normas ISO sobre gestión de seguridad de la información. "Norma: es un documento cuyo uso es voluntario y que es fruto del consenso de las partes interesadas y que deben aprobarse por un organismo de normalización reconocido". La Gestión de la Seguridad de la Información se complementa con las buenas prácticas o controles establecidos en la norma ISO 27002[39].

El ISO (International Organization for Standardization, Organización Internacional para la Estandarización[40]). Permite a las organizaciones la evaluación del riesgo y la aplicación de los controles necesarios para

[38] ISO 27000. [En línea]. Bogotá: ISO -International Organization for Standardization. 2011., 4 p. Disponible en: http://www.iso27000.es/download/doc_sgsi_all.pdf.
[39] GARCIA, Alonso y ALEGRE RAMOS. María del Pilar. SEGURIDAD INFORMATICA ED.11 Paraninfo. Madrid: Paraninfo, 2011. 163p. ISBN 8497328124, 9788497328128.
[40] Acrónimo de International Organization for Standardization (www.iso.org) por sus siglas en inglés. Organización Internacional de Normalización/Estandarización.

mitigarlos o eliminarlos, la define como aquella cualidad de la información que le permite ser accesible y utilizable solo por una entidad autorizada[41].

4.1.2.1 ISO 27000. La serie de normas ISO/IEC 27000 se denomina requisitos para la especificación de sistemas de gestión de la seguridad de la información (SGSI[42]), proporciona un marco de estandarización para la seguridad de la información para que sea aplicado en una organización o empresa y comprende un conjunto de normas sobre las siguientes materias[43]:

- Sistema de gestión de la seguridad de la información
- Valoración de riesgos
- Controles

Serie de normas:

ISO 27001: Que sustituye a la ISO 17799-1, abarca un conjunto de normas relacionadas con la seguridad informática. Se basa en la norma BS 7799-2 de British Estándar, otro organismo de normalización. Según esta norma, que es la principal de la serie, la seguridad de la información es la prevención de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento[44].

[41] Anon, (2017). [online] Available at: http://190.90.112.209/curso_segurinfo.pdf [Accessed 5 Nov. 2017].
[42] Puede encontrarse también como ISMS por sus siglas en inglés de Information Security Management System
[43] ISO 27000. [En línea]. Bogotá: ISO -International Organization for Standardization. 2011., 14 p. Disponible en: http://www.iso27000.es/download/doc_sgsi_all.pdf.
[44] Ibíd., p. 3.

ISO 27002: que se corresponde con la ISO 17799, y que describe un código de buenas prácticas para la gestión de la seguridad de la información y los controles recomendados relacionados con la seguridad[45].

ISO 27003: que contiene una guía para la implementación de SGSI e información acerca del uso del modelo PDCA y de los requerimientos de sus diferentes fases[46].

ISO 27004: que contiene los estándares en materia de seguridad para poder evaluar el sistema de gestión de la seguridad de la información[47].

ISO 27005: que recoge el estándar para la gestión del riesgo de la seguridad[48].

ISO 27006: requisitos a cumplir por las organizaciones encargadas de emitir certificaciones ISO 27001[49].

ISO 27007: Es una guía de auditoría de un SGSI. Como un complemento a lo especificado en la ISO 19011[50].

ISO 17000. No describen un sistema de gestión de calidad (el sistema de gestión de calidad es solamente uno de los requisitos de estas normas), sino que establecen los requisitos específicos que cada uno de los

[45] Ibíd., p. 4.
[46] Ibíd., p. 4.
[47] Ibíd., p. 4.
[48] Ibíd., p. 4.
[49] Ibíd., p. 4.
[50] Ibíd., p. 5.

organismos de evaluación de la conformidad (laboratorios, certificadores e inspectores) deben cumplir para demostrar su competencia[51].

Selección**:**

- Especificación de las normas u otros documentos en los cuales se evaluará la conformidad.
- Selección de los ejemplos del objeto que se debe evaluar. Especificación de técnicas de muestreo estadístico si es aplicable.

Determinación:

- Ensayos para determinar las características específicas del objeto de evaluación.
- Inspección de las características físicas del objeto de la evaluación.
- Auditoría de los sistemas y registros relacionados con el objeto de la evaluación.
- Examen de las especificaciones y los planos para el objeto de la evaluación.
- Revisión y atestación.
- Revisión de las evidencias relevantes en la etapa de determinación para resolver las no conformidades.
- Elaborar y emitir una declaración de conformidad.
- Coloca una marca de conformidad de productos conformes.

[51] RUAY AGUILAR, Marcelo. Documentación Para La Acreditación, Según Norma ISO 17025, Aplicada al Laboratorio LEMCO. Tesis para optar al título de: Ingeniero Constructor. Chile.: Universidad Austral de Chile. Facultad de Ciencias de la Ingeniería Escuela de Construcción Civil. 2006. 110 p.

Vigilancia:

- Llevar a cabo actividades de determinación en el punto de producción o en la cadena de suministro al mercado
- Llevar a cabo actividades de determinación en el mercado.
- Llevar a cabo actividades de determinación en el lugar de uso.
- Revisar los resultados de las actividades de determinación.
- Volver a la etapa de determinación para resolver no conformidades.
- Elaborar y expedir confirmación de continuidad de la conformidad.
- Iniciar acciones correctivas y preventivas en el caso de no conformidades.

4.1.2.2 Políticas generales de seguridad. Las políticas de seguridad se comprometen a mantener y mejorar su Sistema de Gestión de la Seguridad de la Información (SGSI) basado en el estándar internacional ISO 27001.

El activo más importante en las organizaciones empresariales son la información, donde se toman todas las precauciones necesarias, para mantener y preservar la información, y sus políticas de seguridad que han venido desarrollando y evolucionando con su modelo de seguridad de la información la cual es soportada en tres pilares fundamentales que son confidencialidad, integridad y disponibilidad; teniendo en cuenta las buenas prácticas en cuanto al tipo de gestión y administración en las Tecnologías de la Información[52].

[52] Anon, (2017). [en linea] Available at: https://www.clubensayos.com/Español/Importancia-De-Los-Activos-En-Las-Organizaciones-Empresariales/201435.html

4.1.2.3 Elementos de una política de seguridad informática. En relación a la seguridad, dependen de las PSI (Políticas de Seguridad Informáticas)[53], cada usuario debe estar en una disposición de aportar lo necesario para llevar a cabo a una conclusión correcta de las cosas que son importantes en una empresa u organización de cualquier institución de educación superior, que deben ser protegidas. Es por esto que una PSI debe tener los siguientes elementos:

- El tipo de rango de una acción en las políticas. Esto se refiere a las personas sobre las cuales se maneja la ley, como también son los sistemas a los que afecta.
- El proceso del reconocimiento de la información como uno de los principales activos de la empresa.
- Su verdadero objetivo principal de la política y objetivos secundarios de la misma. Si se hace referencia a un elemento particular, hacer una descripción de dicho elemento.
- Las responsabilidades generales de cada uno de los miembros y sistemas de la empresa. Cómo son la política que cubre ciertos dispositivos y sistemas, las cuales deben tener un mínimo nivel de seguridad. Se debe definir este umbral mínimo.
- La responsabilidad que tienen los usuarios frente a la información a la que tienen acceso.

Podemos añadir que es muy importante tener en cuenta estos tipo de elementos a la hora de establecer las políticas de seguridad, siendo así como unas de las pautas fundamentales en las buenas prácticas de la protección de la información en los entornos tecnológicos. De igual manera

[53] Políticas de Seguridad Informática, Co-investigator, N. (2013). Politicas de seguridad informatica. Journal of Chemical Information and Modeling, 53, 1689–1699. https://doi.org/10.1017/CBO9781107415324.004

es importante conocer las características y las recomendaciones para lograr el objetivo.

4.1.2.4 Características de las PSI. Siempre se debe tener en cuenta cuáles son las expectativas de la organización frente a las PSI, qué es lo que espera de ellas en cuanto a seguridad y eficacia[54].

Siempre que se redacten, las PSI deben permanecer libres de tecnicismos que dificulten su comprensión por parte de cualquier persona de la organización[55].

Las características del PSI debe ser vigilada por un ente, una autoridad, la cual debe cumplir y aplicarse con todos los correctivos necesarios. Por lo tanto, no debe confundirse entre una PSI con una ley, sino de verse como tal. Así como las características y los elementos de una empresa cambian, también se deben hacerlo con las PSI, donde se debe tenerse en cuenta, al redactarlas, y que se deben establecer en un esquema de actualizaciones constantes, la cual depende de las características de la organizaciones[56].

[54] ALZATE CASTAÑEDA, Cristian Camilo y GALEANO VILLA, Jorge Luis. Protocolo de Políticas de Seguridad Para las Universidades de Risaralda. Trabajo de grado Profesional en Ingeniero de Sistemas y Telecomunicaciones. Risaralda.: Universidad Católica de Risaralda. Facultad de ciencias básicas e ingeniería, 2013. 100 p.
[55] Ibid., p. 46.
[56] Ibid., p. 46.

4.1.2.5 Recomendaciones para las PSI. Antes que nada, se debe hacer una evaluación de riesgos informáticos[57], para valorar los elementos sobre los cuales serán aplicadas las PSI. Las razones para instaurar políticas de seguridad informáticas PSI, es su objetivo actual crear un manual de procedimientos para su empresa, a través del cual la proteja todo tipo de vulnerabilidades sin embargo, para llegar a este manual de procedimientos, se deben llevar a cabo diversas actividades previas, la cual se debe entender la forma en la que se hacen los procedimientos[58].

4.1.2.6 Puesta en marcha de una política de seguridad. Una buena política de seguridad debe asegurar que el acceso a la información sólo pueda realizarse por aquellos que tengan permiso de acceso a los datos, contar con unas buenas herramientas de control para los mismos y poseer la identificación correspondiente[59].

Al momento de realizar una política de seguridad se debe tener en cuenta algunos aspectos tales como:

- Elaboración de procedimientos y reglas, para cada servicio que se presente y de acuerdo al servicio prestado por la organización.
- Definir las acciones necesarias y el personal encargado para evitar una posible intrusión.
- Ofrecer sensibilización a quienes operen estos sistemas para que tengan capacidad de detectar posibles problemas de seguridad[60].

[57] Riesgos Informáticos, el riesgo es una condición del mundo real, en el cual hay una exposición a la adversidad conformada por una combinación de circunstancias del entorno donde hay posibilidad de pérdidas. Los riesgos informáticos son exposiciones tales como atentados y amenazas a los sistemas de información.
[58] Ibid., p. 47.
[59] Ibid., p. 48.
[60] Ibid., p. 48.

4.1.3 Protocolos. El protocolo consiste en que es una serie de pasos bien definidos, en este contexto, significa que este protocolo cubre todas las posibles situaciones que pueden surgir durante su ejecución.

El protocolo tiene que complementarse para cubrir todas las necesidades que requieren el conjunto de actividades que tienen lugar cuando en los actos oficiales y en la realización de otras series de actividades que se deben regular y organizar[61].

4.1.4 Medidas para evitar ser víctimas de la Ingeniería Social. La principal herramienta para ser utilizada y protegida de los ataques en ingeniería social es proceso del sentido común. Podemos decir que es uno de los pequeños métodos que se pueden aconsejar para identificar las estrategias usadas en la ingeniería social y sobre todo para poder evitar ser víctima de este tipo de ataques :

- Nunca revele por teléfono o e-mail datos confidenciales (como claves de acceso, números de tarjetas de crédito, cuentas bancarias, etc.).
- Nunca haga click en un enlace a una página web que le llegue a través de un e-mail en el que le piden datos personales.
- Desconfíe de cualquier mensaje de e-mail en el que se le ofrece la posibilidad de ganar dinero con facilidad.
- Si es usuario de banca electrónica o de cualquier otro servicio que implique introducir en una web datos de acceso, asegúrese de que la dirección de la web es correcta.

[61] Editorial, p. (2017). ¿Qué es el Protocolo? Su aplicación Oficial y social. [online] Protocolo y Etiqueta. Available at: https://www.protocolo.org/social/etiqueta-social/que-es-el-protocolo-su-aplicacion-oficial-y-social.html [Accessed 4 Nov. 2017].

- No confíe en las direcciones de los remitentes de e-mail o en los identificadores del número llamante en el teléfono: pueden falsearse con suma facilidad.
- Instale en su ordenador un buen software de seguridad que incluya si es posible funcionalidad antivirus, antiphising, antispyware y antimalware para minimizar los riesgos.
- Utilice el sentido común y pregúntese siempre que reciba un mensaje o llamada sospechosa si alguien puede obtener algún beneficio de forma ilícita con la información que le solicitan[62].

4.2 MARCO CONCEPTUAL

El término "ingeniería social" hace referencia al arte de manipular personas para eludir los sistemas de seguridad.

Los atacantes de este tipo dentro de la ingeniería social[63] buscan la manera de obtener resultados ante este uso de fuerza persuasiva y se aprovechan de la inocencia del usuario haciéndose pasar por un compañero de trabajo, un técnico o un administrador, etc.

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,

[62] TICSCONSULTING. "Ingeniaría Social: explotar por medio de la manipulación y el engaño el eslabón más débil de la cadena de seguridad: factor humano". [En línea]. Enero 2011. {11 mayo de 2017}. Disponible en: http://www.ticsconsulting.es/blog/generar-claves-seguras-3.

[63] La Ingeniería Social es la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos.

factor que a su vez es el de mayor abandono o rezago frete a temas de seguridad informática.

- **Servicio de Red Social en Internet:** "Se enfoca en construir comunidades de gente en-línea que comparten intereses y/o actividades, o que están interesadas en explotar los intereses y actividades de otros. Los servicios de Red Social son basados en Web y proporcionan una variedad de vías para interactuar con el usuario, tales como chat, mensajería, blogs, grupos de discusión, tienda virtual, etc[64]".

- **Redes Sociales en Internet:** "Definimos como Redes Sociales en Internet o Sitios de Redes Sociales (SRS) a los servicios basados en la Web que permiten a los individuos (1) construir un perfil público o semi-público dentro de un sistema delimitado, (2) articular una lista de otros usuarios con los que comparten una conexión, y (3) ver y recorrer su lista de conexiones y aquellas hechas por otros dentro del sistema."[65]

- **Redes Sociales:** "Son estructuras sociales (población con una organización y una tecnología, que vive y se desarrolla en un medio ambiente) compuestas de grupos de personas, las cuales están conectadas por uno o varios tipos de relaciones, tales como amistad, parentesco, intereses comunes o que comparten conocimientos."

[64] ROS-MARTIN, Marcos. Evolución de los Servicios de Redes Sociales en Internet. [en línea] Septiembre 2009. Disponible en: <http://www.documentalistaenredado.net/859/evolucion-de-los-servicios-de- redes-sociales-en-internet/> Consulta: En el presente trabajo de investigación, se hace necesario al marco en la cual 21/03/2017

[65] Mc142.uib.es. (2017). Citar un sitio web - Cite This For Me. [en linea] Disponible en: http://mc142.uib.es:8080/rid%3D1HY8TVCBB-15599LW-1S6Z/redes_sociales.pdf [Accessed 4 Nov. 2017].

Permite definir los conceptos relevantes para el tema de seguridad de la información y de la ingeniería social la cual es aplicada a las redes de comunicación, se han definido tres conceptos centrales que son: seguridad social, seguridad informática y sistemas de detección de intrusos.

4.3 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 en Latinoamérica. La ley de Código Penal colombiano el Título denominado "De la Protección de la información y de los datos" que divide en dos capítulos, a saber: “De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos” y “De los atentados informáticos y otras infracciones”[66].

A continuación, la legislación vigente y pertinente en materia de delitos informáticos, junto a un breve resumen de las observaciones realizadas sobre el marco jurídico aplicable por país.

[66] BERMUDEZ. Op. cit., p. 54.

Tabla 2 Legislación vigente de los Delitos Informáticos en Latinoamérica.[67]

PAÍS	LEGISLACIÓN	CARACTERÍSTICAS GENERALES
Argentina	Código Penal, Ley 26.388 (2008), Ley 25.326 (2000)	A partir de Junio de 2008, la Ley 26.388 conocida como la "ley de delitos informáticos" ha incorporado y realizado una serie de modificaciones al Código Penal argentino. Es decir, la misma no regula este tipo de delitos en un cuerpo normativo separado del Código Penal (CP) con figuras propias o independientes, sino que dicha ley modifica, sustituye e incorpora figuras típicas a diversos artículos del CP actualmente en vigencia. Se modificó el Epígrafe del Capítulo III cuyo nuevo título es "Violación de Secretos y de la Privacidad", Los artículos que modifica o agrega son: 128, 153, 153 bis, 155, 157, 157 bis, 173, 183, 184, 197, 255. El art. 157 bis ya había sido incorporado por la Ley 25.326 de Protección de Datos Personales (2000) pero fue modificado por la Ley 26.388.
Bolivia	Código Penal, Ley 1.768 (1997), Ley 3325 (2006)	La Ley 1.768 realiza una reforma general al Código Penal. Allí incorpora como Capítulo XI, del Título XII, del Libro Segundo del Código Penal, el de "DELITOS INFORMÁTICOS". entro de este capítulo, se incorporan 2 artículos: 363 bis y ter, en cuyos textos se tipifica algunos delitos informáticos.
Brasil	Ley 12.737 (2012), Ley 11.829 (2008)	La Ley 12.737 es una ley reciente (año 2012), en la cuál se dispone la tipificación criminal de los delitos informáticos y otras providencias. En su regulación incorpora modificaciones para los artículos 154-A, 154-B, 266 y 298. Por su parte, la Ley 11.829 regula el Estatuto de la Niñez y la Adolescencia, para mejorar la lucha contra la producción, venta y distribución de pornografía infantil, así como tipificar como delito la adquisición y posesión de dicho material y otros comportamientos relacionados con la pedofilia en Internet.

[67] TEMPERINE, Marcelo. Delitos Informáticos en Latinoamérica: Un estudio de derecho comparado. 1ra. Parte. Buenos Aires, 2013, 12p. Trabajo de investigación (Doctorando en Derecho). Universidad Nacional del Litoral. Facultad de Ciencias Jurídicas y Sociales. Argentina.

Tabla 3 (Continuación)

PAÍS	LEGISLACIÓN	CARACTERÍSTICAS GENERALES
Chile	Ley 19.223 (1993), Ley 20.009 (2005), Ley 18.168 (2002)	La Ley 19.223 es una ley “Relativa a Delitos Informáticos” de acuerdo a su propio título, donde regula cuatro artículos, desde loscuáles se tipifican varios delitos informáticos. La Ley 20.009 regula la responsabilidad para el caso de robo, hurto o extravío de tarjetas de crédito, en cuyo texto se sancionan algunas conductas relacionadas con estos speectos. La Ley 18.168 (modificada por diferentes normativas) regula de manera general las telecomunicaciones, incorporando algunos tipos penales sobre la interferencia o captación ilegítima de señales de comunicación.
Colombia	Ley 1.273 (2009), Ley 1366 (2009)	La ley 1.273, de reciente sanción legislativa (año 2009), modifica el Código Penal, creando un nuevo bien jurídico tutelado denominado "de la protección de la información y de los datos”. Se afirma que dicha normativa busca preservar integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones. A través de esta incorporación, suma el CAPITULO I, titulado "De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos", a partir del cuál regula una serie de artículos penales que van desde el artículo 269A hasta el artículo 269J. Adicionalmente se incorpora el artículo 58, considerando como agravante general “si la realización de alguna de las conductas punibles, se realicen utilizando medios informáticos, electrónicos o telemáticos”.

Tabla 4 (Continuación)

PAÍS	LEGISLACIÓN	CARACTERÍSTICAS GENERALES
Ecuador	Ley Nº 67/2002 (2002)	La Ley No. 67/2002 regula el Comercio Electrónico, Firmas y Mensajes de datos. En dicha norma, dentro del Capítulo I del Título V, titulado "DE LAS INFRACCIONES INFORMÁTICAS", el art. 57 afirma que "Se considerarán infracciones informáticas, las de carácter administrativo y las que se tipifican, mediante reformas al Código Penal, en la presente ley." En artículo siguiente, agrega y modifica varios artículos al Código Penal, incorporando diferentes figuras de delitos informáticos.
Paraguay	Código Penal – Ley 1.160 (1997), Ley 2.861	No se ha encontrado legislación especial referida a la materia. Sin embargo, a partir de distintas reformas al Código Penal Paraguayo, se han adaptado algunos delitos para la posibilidad de comisión a través de las nuevas tecnologías y en otros casos se ha incorporado tipos penales específicos (como el caso del art. 175 de Sabotaje de Computadoras). Los artículos son 144, 146, 173 a 175, 188, 189, 220, 239, 248 y 249.
Perú	Ley 27.309 (2000), Ley 28.251 (2004)	La Ley 27309 incorpora al Código Penal del Perú los Delitos Informáticos, a través de un artículo único que modifica el Título V del Libro Segundo del Código Penal, promulgado por Decreto Legislativo No 635, introduciendo allí los artículos 207 – A – B y C y 208. En otro orden, la Ley 28.251 actualizó e incorporó distintos delitos contra la integridad sexual, entre ellos, tipificando la pornografía infantil, a través de la modificación del art 183-A. Además Perú posee la Ley 28.493 (2005) que regula el uso del correo electrónico no solicitado (spam), sin embargo en la misma no incluye ningún tipo de sanción penal.

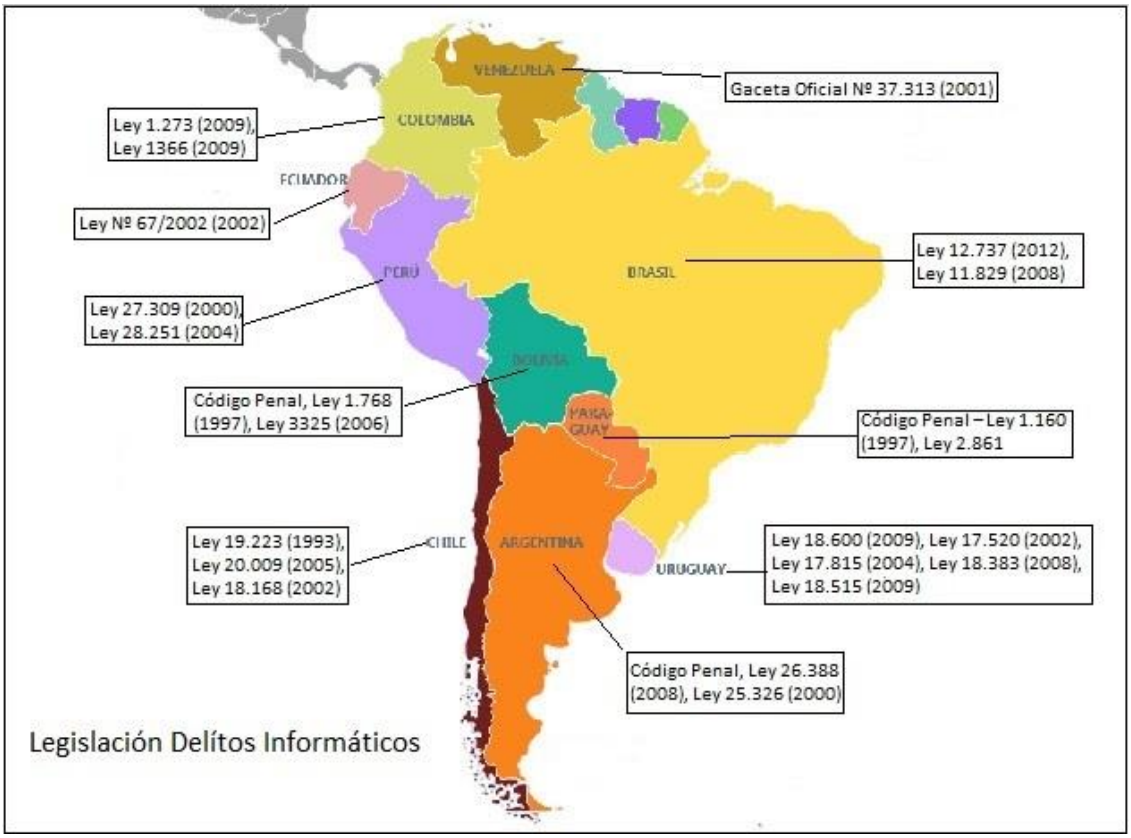
Tabla 5 (Continuación)

PAÍS	LEGISLACIÓN	CARACTERÍSTICAS GENERALES
Uruguay	Ley 18.600 (2009), Ley 17.520 (2002), Ley 17.815 (2004), Ley 18.383 (2008), Ley 18.515 (2009)	Si bien no se ha encontrado legislación especial en la materia, se han encontrado diferentes normativas parcialmente aplicables a la materia. El art. 7 de la Ley 17.815, afirma que "constituye delito de comunicación la comisión, a través de un medio de comunicación, de un hecho calificado como delito por el Código Penal o por leyes especiales.", permitiendo así la aplicación de los tipos clásicos del CP. La Ley N° 17.520, penaliza el uso indebido de señales destinadas exclusivamente a ser recibidas en régimen de abonados. La Ley Nº 17.815 regula la violencia sexual, comercial o no comercial cometida contra niños, adolescentes e incapaces que contenga la imagen o cualquier otra forma de representación.
Venezuela	Gaceta Oficial Nº 37.313 (2001)	Posee una ley especial sobre Delitos Informáticos. Contiene 33 artículos y están clasificados en 5 Capítulos a saber: Contra sistemas que utilizan TI; Contra la propiedad; Contra la privacidad de las personas y las comunicaciones; Contra niños y adolescentes; Contra el orden económico.

Fuente: http://conaiisi.unsl.edu.ar/2013/82-553-1-DR.pdf

El desarrollo de leyes y normativas han 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 2 Panorama jurídico frente a los delitos informáticos en Sudamérica[68]



Fuente: http://mapadeamerica.net/mapa-de-sudamerica-con-nombres

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.

[68] Mapa de América. (2017). Mapa de Sudamérica con nombres - Mapa de América. [online] Available at: http://mapadeamerica.net/mapa-de-sudamerica-con-nombres.

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”[69].

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”[70]. 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"[71].

[69] GÓMEZ VIEITES, Álvaro. Auditoría de seguridad informática. Madrid: Ra-Ma, 2014. 147 p. ISBN 978-84-9964-328-1.
[70] Ibid., p. 88.
[71] 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.

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"[72].

El 5 de enero del año 2009, el Congreso de la República de Colombia promulgó la Ley 1273[73] Por medio del 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"[74].

De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos

Artículo 269A: Acceso abusivo a un sistema informático. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en

[72] EL ESPECTADOR. "En busca de cura para los delitos informáticos" [en línea], mayo 2014 [citado en 25 abril de 2017]. Disponible en Internet: <http://www.elespectador.com/noticias/politica/busca-de-cura-los-delitos-informaticos-articulo-492170>.
[73] LEY 1273 DE 2009 (Enero 05) 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.
[74] BERMUDEZ. Op. cit., p. 57.

pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes[75].

Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor[76].

Artículo 269C: Interceptación de datos informáticos. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses[77].

Artículo 269D: Daño Informático. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes[78].

[75] COLOMBIA, CONGRESO DE LA REPUBLICA. Ley 1273 de 2009. (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. El departamento. Bogotá D.C., 2009 4 p.
[76] Ibíd., p. 1.
[77] Ibíd., p. 1.
[78] Ibíd., p. 2.

Artículo 269E: Uso de software malicioso. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes[79].

Artículo 269F: Violación de datos personales. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes[80].

Artículo 269G: Suplantación de sitios web para capturar datos personales. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave[81].

En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave. La pena

[79] Ibíd., p. 2.
[80] Ibíd., p. 2.
[81] Ibíd., p. 2.

señalada en los dos incisos anteriores se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito[82].

Artículo 269H: Circunstancias de agravación punitiva: Las penas imponibles de acuerdo con los artículos descritos en este título, se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere:

1. Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.

2. Por servidor público en ejercicio de sus funciones.

3. Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.

4. Revelando o dando a conocer el contenido de la información en perjuicio de otro.

5. Obteniendo provecho para sí o para un tercero.

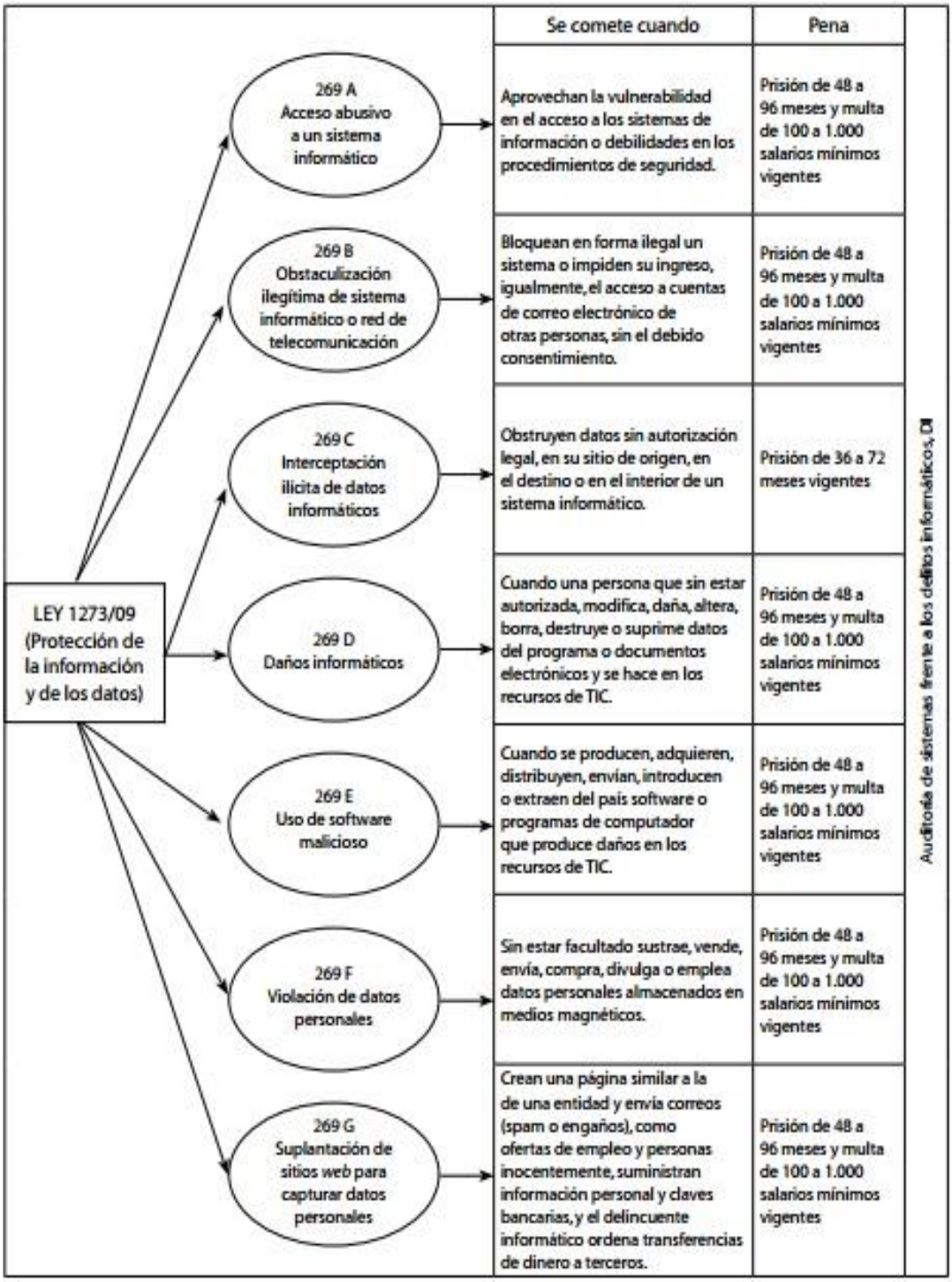
6. Con fines terroristas o generando riesgo para la seguridad o defensa nacional.

7. Utilizando como instrumento a un tercero de buena fe.

8. Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales[83].

[82] Ibíd., p. 2.
[83] Ibíd., p. 2.

Figura 3 Legislación penal colombiana frente a los delitos informáticos (artículo 1 de la Ley 1273 de 2009).



Fuente: http://www.scielo.org.co/pdf/cuco/v11n28/v11n28a03.pdf

4.3.1 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" [84].
- **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[85]".
- **Ley estatutaria 1581 de 2012** "por la cual se dictan disposiciones generales para la protección de datos personales"[86] . 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.

[84] 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.

[85] 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.

[86] 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.

4.4 GENERALIDADES DE LA UNIVERSIDAD

4.4.1 Historia. Ordenanza No 12 de 1945 (junio 11) Por la cual se ordena la fundación de la Universidad Industrial del Valle del Cauca y se dictan otras disposiciones. Con Tulio Ramírez como primer rector, la Universidad Industrial del Valle empezó labores el lunes 29 de octubre de 1945 en el claustro del Colegio Republicano de Santa Librada. Inicialmente contó con la Escuela de Comercio Superior y Administración de Negocios, la Escuela de Enfermería y la Facultad de Agronomía[87].

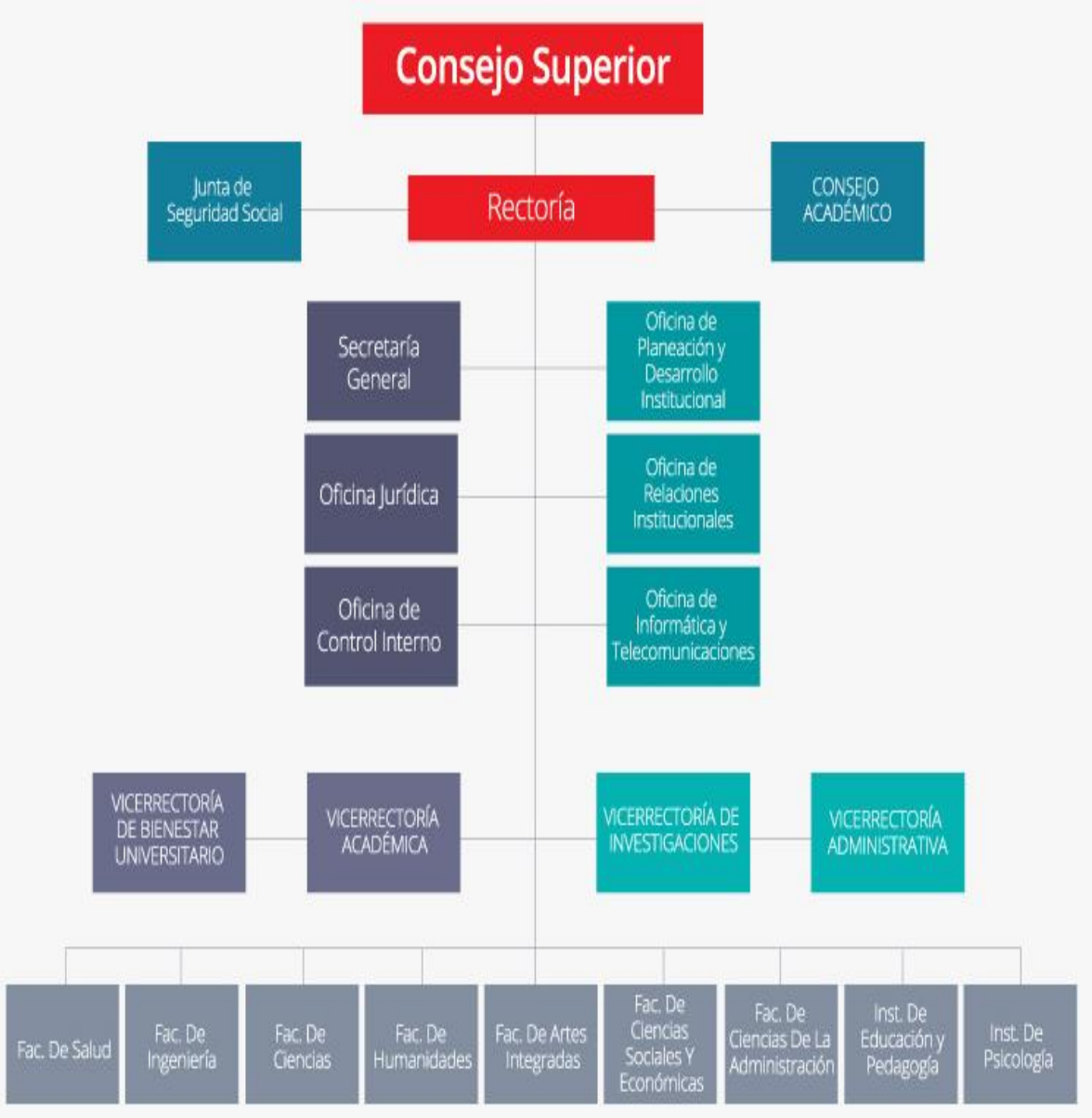
4.4.2 Misión. "La Universidad del Valle tiene como misión formar en el nivel superior, mediante la generación, transformación, aplicación y difusión del conocimiento en los ámbitos de las ciencias, la técnica, la tecnología, las artes, las humanidades y la cultura en general. Atendiendo a su carácter de universidad estatal, autónoma y con vocación de servicio social, asume compromisos indelegables con el desarrollo de la región, la conservación y el respeto del medio ambiente y la construcción de una sociedad más justa y democrática" [88].

4.4.3 Visión. "Ser reconocida como una Universidad incluyente con altos estándares de calidad y excelencia, referente para el desarrollo regional y una de las mejores universidades de América Latina" [89].

[87] Universidad del Valle. «Reseña Histórica – Antecedentes». Universidad del Valle, 60 años. Consultado el 25 de Abril de 2017.
[88] UNIVERSIDAD DEL VALLE. "Misión" [en línea], 2015 [citado en 25 abril de 2017]. Disponible en Internet: <http://www.univalle.edu.co/la-universidad/acerca-de-univalle/mision>.
[89] UNIVERSIDAD DEL VALLE. "Misión" [en línea], 2015 [citado en 25 abril de 2017]. Disponible en Internet: <http://www.univalle.edu.co/la-universidad/acerca-de-univalle/vision>.

4.4.4 Organigrama. “Esta es la estructura organizacional actual de la Universidad de Valle, de acuerdo con el Acuerdo No 020 del Consejo Superior del 10 de febrero de 2003”[90] .

Figura 4 Organigrama de la Universidad del Valle.



Fuente: http://www.univalle.edu.co/la-universidad/acerca-de-univalle/organigrama

[90] UNIVERSIDAD DEL VALLE. “Misión” [en línea], 2015 [citado en 25 abril de 2017]. Disponible en Internet: <http://www.univalle.edu.co/la-universidad/acerca-de-univalle/organigrama>.

4.4.5 Ubicación. "La Universidad del Valle tiene su sede en Cali, capital del departamento del Valle del Cauca, una de las regiones de mayor desarrollo industrial en Colombia conocida por su alta capacidad de exportación de azúcar de caña a nivel internacional. Son unas tierras muy fértiles donde se encuentran grandes empresas agrícolas. La ciudad de Cali es sede, actualmente, de siete Universidades, en las que se destaca la Universidad del Valle por su amplio cubrimiento en las áreas de humanidades, así como por el desarrollo de las áreas de investigación científica y de tecnología aplicada, para lo cual ha contado con el decidido y decisivo apoyo de entidades internacionales y de otras universidades a través de convenios de cooperación interinstitucional" [91].

[91] UNIVERSIDAD DEL VALLE. "Misión" [en línea], 2015 [citado en 25 abril de 2017]. Disponible en Internet: <http://www.univalle.edu.co/la-universidad/acerca-de-univalle/ubicacion>.

5 DISEÑO METODOLÓGICO

5.1 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, y cuya temática es la Auditoria de Sistemas. A través de esta investigación se pretende determinar cuáles son las vulnerabilidades 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. 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 las redes sociales. Para esto se realizara una estadística de las encuestas acerca de la ingeniería social para la Universidad.

5.2 POBLACIÓN Y MUESTRA

Como población y muestra, a la vez, para esta labor investigativa se tomó el 100% de la planta administrativa y estudiantil, incluyendo algunos docentes de tiempo completo que cumplen esta función dentro la sede de la Universidad del Valle de Cali - 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 66 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.

5.3 FUENTES Y TÉCNICAS DE RECOLECCIÓN DE INFORMACIÓN

En función de los objetivos definidos en el presente estudio, donde se plantea el estudio de la ingeniería social en el uso de las redes sociales de las personas en la sede de la universidad del valle, se emplearon como técnica común y característica de este nivel de investigación, la encuesta, el cual será orientado de manera esencial para alcanzar los fines propuestos en el presente trabajo de investigación.

5.4 RECURSOS DISPONIBLES

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

5.4.1 Talento humano. La investigación fue ejecutada por dos ingenieros Claudia Patricia Flórez Ramírez y Harold Méndez Collo, estudiantes de la Especialización en Seguridad Informática dictada por la UNAD, quienes somos los únicos encargados del desarrollo de la presente propuesta de trabajo de grado

5.4.2 Materiales y equipos. Para el desarrollo de esta investigación se contó con dos computadores portátiles uno de marca (ACER aspire 4743z-4492 y un vostro) y (DELL Vostro 5470: Laptop Intel Core i4, 2 Cores, Cache 3MB, Ram 2GB DDR3, SSD 128GB, Pantalla 14.0'', LAN Port Gigabit, Wi-Fi, Bluetooth 4.0, USB 2.0, USB 3.0, HDMI, Cámara Web HD 720p); con sistema operativo Ubuntu 16.06 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 centos (sin soporte actual). Dicho equipo tiene open office (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.

5.4.3 Recursos financieros. La ejecución de este proyecto investigativo no implicó mayor costo para los investigadores ni para la organización en la que se llevó a cabo ya que es un trabajo investigativo.

5.4.4 Cronograma de trabajo. Tener un orden en la elaboración de alguna tarea es un aspecto sumamente importante y más aún, cuando se trata de las actividades académicas en las que se hace uso de una metodología específica, como es el proceso 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.

Figura 5 Cronograma de trabajo

Nombre de la tarea	Duración	Inicio	Finalizar
PREPARACIÓN DEL PROYECTO	21d	15/11/16	05/12/16
ANALISIS INVESTIGATIVO DEL PROYECTO	90d	20/11/16	17/02/17
EL SISTEMA DE CONSTRUCCIÓN DEL PROYECTO	45d	15/11/16	29/12/16
DISEÑO METODOLOGICO	30d	16/11/16	15/12/16
TIPOS DE INVESTIGACIÓN	120d	30/11/16	29/03/17
FUENTES Y TÉCNICAS DE RECOLECCIÓN DE LA INFORMA(	90d	30/11/16	27/02/17
DESARROLLO DE ENCUESTAS	30d	28/02/17	29/03/17
POBLACIÓN	50d	30/11/16	16/01/17
MUESTRA	60d	30/11/16	28/01/17
DESARROLLO DE LA PROPUESTA	30d	15/11/16	14/12/16
IMPACTOS	90d	30/11/16	27/02/17
RECOMENDACIONES	120d	30/11/16	29/03/17
ANEXOS	120d	30/11/16	29/03/17
ENTREGA DEL PROYECTO I	14d	30/11/16	13/12/16
ENTREGA FINAL DEL PROYECTO SUSTENTADO	210d	30/11/16	30/06/17

Fuente: El autor

6 RESULTADOS Y EVIDENCIAS

Los resultados iniciales de esta investigación se obtuvieron a través de la aplicación de una encuesta (Ver anexo A). Para ello, se aprovechó al personal que ingresa a la biblioteca de la Universidad del Valle de Cali y al que asiste todo el personal administrativo, estudiantil, docentes e invitados que labora en la institución. Allí se solicitó la colaboración de los asistentes para el diligenciamiento de la encuesta ya mencionado.

Se logró que 167 asistentes respondieran el cuestionario, incluyendo al personal de servicios generales, manteniendo, auxiliares, jefes y directivos de todas las áreas, y docentes de tiempo completo e invitados o personal ajeno a la universidad.

Los resultados a continuación es el 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 167 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.

6.1 RESULTADOS DE LA ENCUESTA

Los resultados mostrados a continuación solo detallan las cifras que representan un riesgo de ingeniería social en el uso de las redes sociales. Los encuestados a la pregunta 1. ¿Tienes cuenta en redes sociales? las personas encuestadas respondieron lo siguiente:

Tabla 6 Pregunta 1 General en cantidades

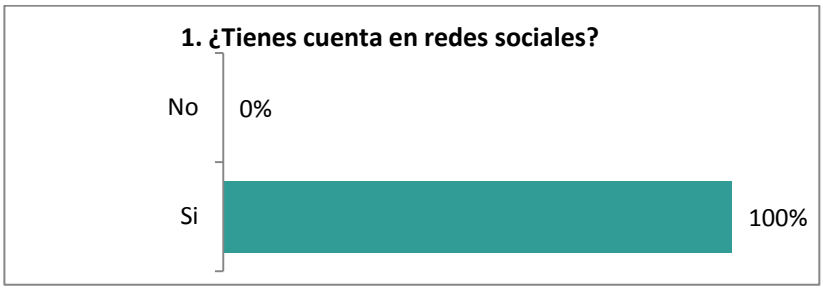
1. ¿Tienes cuenta en redes sociales?	
Opciones	Cantidad
1. SI	167
2. No	0
Total	167

Fuente: El autor

1. 167 de las 167 personas encuestadas dijeron que tenia cuenta en redes sociales, lo que representa un 100% de la población, un alto porcentaje de usuarios que tienen cuentas en redes sociales y que pueden ser víctimas de ataques informáticos.
2. Ninguna de la personas encuestados respondieron no tener una cuenta, un 0%, respondieron negativamente, como se muestra en la gráfica 1.

En el siglo XXI las redes sociales se han convertido en el vehículo de comunicación más rápido y de más actualidad del momento. Formar parte de grupos, seguir a gente que le interesa, cargar y etiquetar fotos, dejar comentarios, darle al botón favorito 'me gusta', retuitear, etc. Ofrecen un sinfín de posibilidades y muchísimas finalidades, desde para darse a conocer, pasando por la promoción de un producto o una empresa, hasta simplemente hacer nuevos amigos.

Gráfica. 1 Pregunta 1 General en %



Fuente: El autor

De la siguiente pregunta de la encuesta 2. ¿Para qué utilizas las redes sociales?. El siguiente es el resultado que se encontró.

1. 98 de 167 encuestados dicen que utilizan las redes sociales para estar en contacto con sus amigos.
2. 41 personas ´para conocer gente nueva.
3. 17 encuestados para contactar amigos a los que hace tiempo no ve.
4. Por último, 11 personas las utilizan para otros temas.

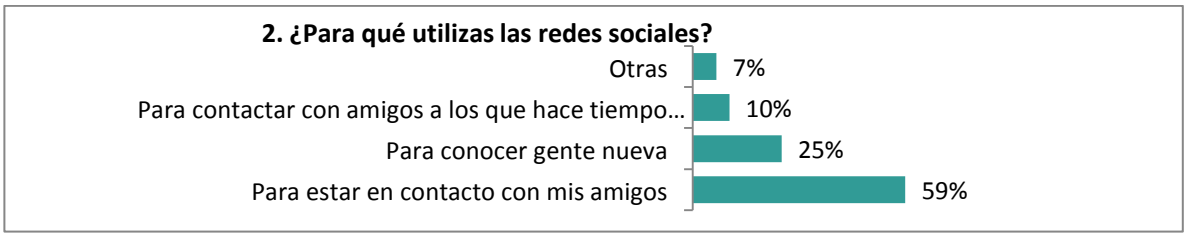
Tabla 7 Pregunta 2 General en cantidades.

2. ¿Para qué utilizas las redes sociales?	
Opciones	**Cantidad**
1. Para estar en contacto con mis amigos	**98**
2. Para conocer gente nueva	**41**
3. Para contactar con amigos a los que hace tiempo que no veo	**17**
4. Otras	**11**
Total	**167**

Fuente: El autor

La siguiente grafica demuestra que el 59% de encuestados que son la mayoria, utilizan las redes sociales para estar en continua comunicación con los amigos esto se debe a que los sitios de las redes sociales proveen las posibilidades para estar en contacto con sus amistades, familiares y compartir archivos como fotos, jugar juegos en linea, y organizar eventos, entre muchas otras actividades de comunicación. Hasta que se puede utilizar para promocionar su empresa o negocio, o para buscar trabajo.

Gráfica. 2 Pregunta 2 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. Las contraseñas son necesarias para todo. Ya sea para las redes sociales, a la hora de registrarse en el lugar de trabajo o en el ordenador personal, el usuario requiere de una clave de acceso. Páginas web como "How Secure Is My Password", permiten comprobar el nivel de fortaleza de tu contraseña**.** El sitio te dirá cuán segura es, y también te dará una estimación de cuánto tiempo le podría llevar a un hacker entrar a tu cuenta mediante fuerza bruta. Pero la mayoría de los expertos en ciberseguridad te dirán que deberías usar al menos catorce caracteres. Lo cual significa que debes combinar letras, números y símbolos en una contraseña. Por la cua se les pregunto 3. ¿Cuántos caracteres utilizas en las contraseñas para registrarse en la cuenta en las redes sociales?

1. 92 de los encuestados correspondientes al 55% de la población respondió 5-8 caracteres con letras y números combinados.
2. 68 que equivalen al 41% respondieron 9-12 caracteres con letras y números combinados.
3. El restante, 7 personas o el 4% dijo 13-16, caracteres con letras y números combinados.

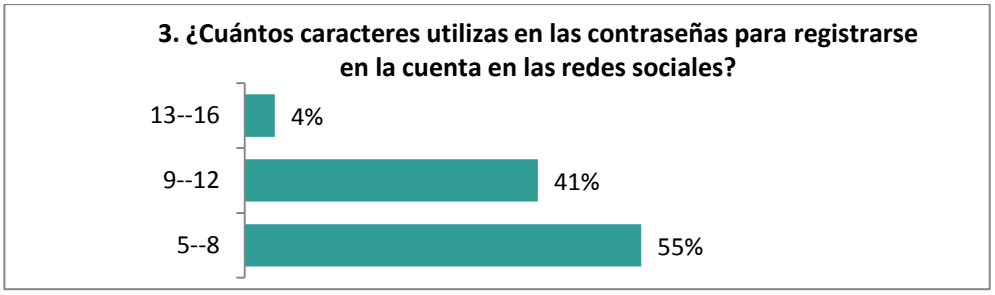
Tabla 8 Pregunta 3 General en cantidades.

3. ¿Cuántos caracteres utilizas en las contraseñas para registrarse en la cuenta en las redes sociales?	
Opciones	**Cantidad**
1. 5—8 caracteres con letras y números combinados	92
2. 9—12 caracteres con letras y números combinados	68
3. 13—16 caracteres con letras y números combinados	7
Total	**167**

Fuente: El autor

En esta etapa se logra deducir que un gran porcentaje de los encuestados tienen un porcentaje (55%) de los usuario dentro de la universidad, la cual no tienen la suficiente conciencia a la hora de crear sus contraseñas de acceso y pueden ser víctimas de la ingeniería social. Por lo tanto podemos decir que se debe tomar las siguientes reglas para una protección segura de las contraseñas, ya que una contraseña diferente para cada servicio, tiene las opciones de recuperación para mentes olvidadizas, y las contraseñas en lugares seguros entre sea más larga y compleja, mucho mejor su protección.

Gráfica. 3 Pregunta 3 General en %



Fuente: El autor

Respecto a la pregunta número 4. ¿En qué redes sociales tienes perfil?

1. 23 de los 167 encuestados, equivalentes al 14 % de la población, respondieron que tenían cuenta en Lindkdln.

2. Asi como 160 de los 167 encuestados, equivalentes al 96 % de la población, respondieron que tenían cuenta en Facebook.
3. El 99 de los 167 encuestados, equivalentes al 59 % de la población, respondieron que tenían cuenta en Twiter.
4. 130 de los 167 encuestados, equivalentes al 78 % de la población, respondieron que tenían cuenta en Instagram.
5. Finalmente, 45 de los 167 encuestados, equivalentes al 27 % de la población, respondieron que tenían otra cuenta, como se muestra en la siguiente tabla.

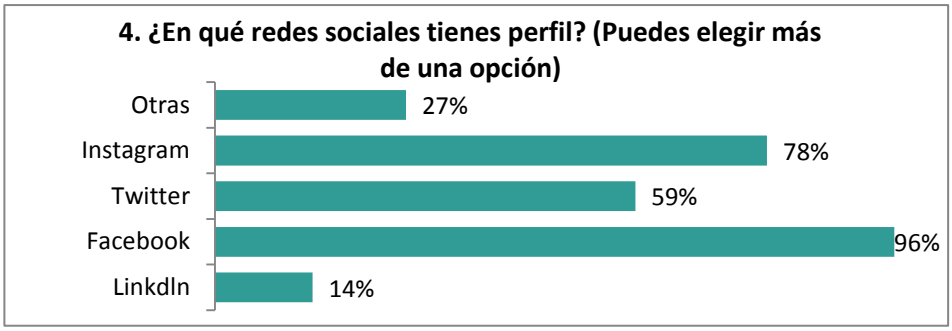
Tabla 9 Pregunta 4 General en cantidades.

4. ¿En qué redes sociales tienes perfil? (Puedes elegir más de una opción)	
Opciones	**Cantidad**
1. Linkdln	**23**
2. Facebook	**160**
3. Twitter	**99**
4. Instagram	**130**
5. Otras	**45**
Total	**457**

Fuente: El autor

Al considerar el estudio, señala que el 96 por ciento de los encuestados señala que la red social a la que destinan más tiempo es Facebook, así como Instagram con un 78 por cieno y 59 por ciento que resalta a Twiter. Y, al igual que las categorías anteriores, en las que menos tiempo emplean son Linkdln con un 14 por ciento de las menciones y otras con un 27 por ciento, como se muestra en la siguiente figura.

Gráfica. 4 Pregunta 4 General en %



Fuente: El autor

En cuanto al tema de la pregunta 5. ¿Con qué frecuencia utilizas las redes sociales?

1. Se logró evidenciar que 167 de los encuestados o el 100% de la población utiliza las redes sociales más de una vez al día.
2. Se concluye que las personas utilizan las redes sociales con mucha frecuencia para mantener contacto y encontrarse con gente que ya conoce: amigos del colegio, la universidad, el trabajo, la familia u otros grupos y seguir en comunicación con ellos por más lejos que se encuentren y aunque ya no se vean con tanta frecuencia, actualidad y falta de hacer algo más interesante.
3. Las personas adicional las utilizan para buscar contenido divertido o de entretenimiento.

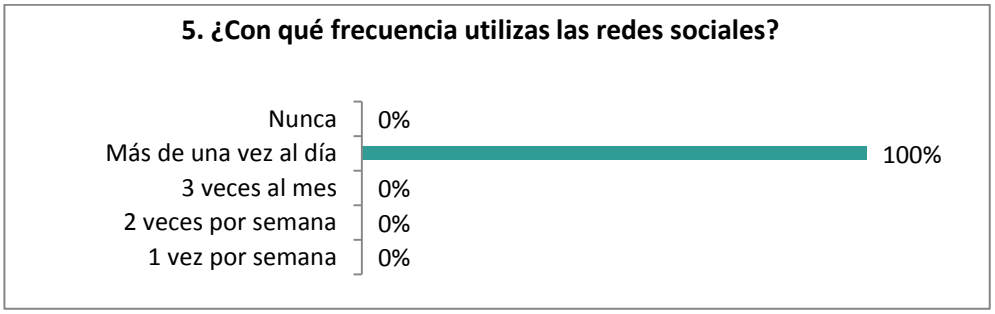
Tabla 10 Pregunta 5 General en cantidades.

5. ¿Con qué frecuencia utilizas las redes sociales?	
Opciones	**Cantidad**
1. 1 vez por semana	**0**
2. 2 veces por semana	**0**
3. 3 veces al mes	**0**
4. Más de una vez al día	**167**
5. Nunca	**0**
Total	**167**

Fuente: El autor

4. En resumen, el 100% de las personas encuestadas usan las redes sociales para estar en contacto con amigos, nos interesa las actividades que están realizando, saber qué pasa en la actualidad y saber cuales son las últimos hechos o noticias, la actualidad, conocer personas nueva, nos gusta compartir información con nuestros amigos, por último, finalmente nos gusta darnos a conocer tal y como somos de manera abierta.

Gráfica. 5 Pregunta 5 General en %



Fuente: El autor

De la pregunta 6. ¿Usted qué cargo tiene?.

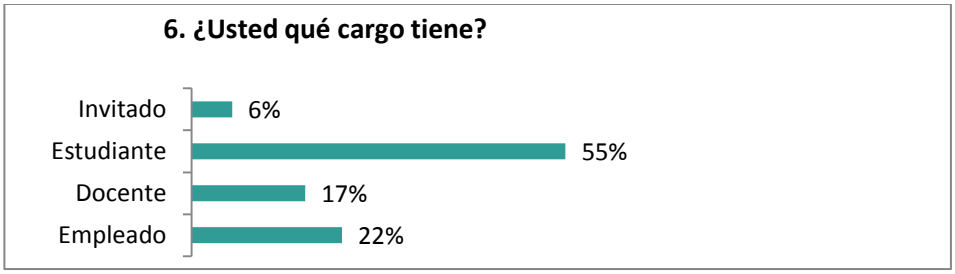
1. El 37 de los 167 encuestados, equivalentes al 32% de la población, son empleados.
2. Continuando, 28 de los 167 encuestados, equivalentes al 17% de la población es personal docente.
3. 92 de los 167 encuestados, equivalentes al 55% de la población son estudiantes.
4. Finalmente, 10 de los 167 encuestados, equivalentes al 6% de la población son invitados o personal ajena a la institución.

Tabla 11. Pregunta 6 General en cantidades.

6. ¿Usted que cargo tiene?	
Opciones	**Cantidad**
1. Empleado	**37**
2. Docente	**28**
3. Estudiante	**92**
4. Invitado	**10**
Total	**167**

Fuente: El autor

Gráfica. 6 Pregunta 6 General en %



Fuente: El autor

En conclusión a la pregunta anterior, las personas que más contestaron la encuesta fueron los estudiantes con un 55% del total de personas encuestadas, esto se debe a que la mayoría del personal en la universidad es estudiantil.

A la pregunta 7. ¿Crees que se pueden correr peligros con las redes sociales?

1. 5 personas o el 3% respondieron que no se corre con ningún peligro.
2. 140 de las personas encuestados o el 84% de la población cree que si hay peligros en las redes sociales.
3. 22 o el 13% de las personas respondieron no estar seguro.

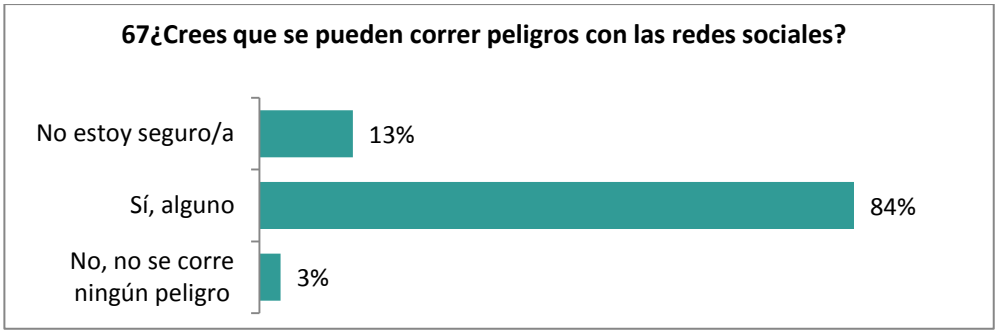
Tabla 12 Pregunta 7 General en cantidades.

7. ¿Crees que se pueden correr peligros con las redes sociales?	
Opciones	**Cantidad**
1. No, no se corre ningún peligro	**5**
2. Sí, alguno	**140**
3. No estoy seguro/a	**22**
Total	**167**

Fuente: El autor

En la siguiente gráfica los resultados demuestran que la mayoría de la personas encuestadas están seguras que se corren peligros en las redes sociales, un bajo porcentaje respondieron que no se corre ningún peligro y muy pocas personas respondieron no estar seguros, como se muestra en la siguiente gráfica.

Gráfica. 7 Pregunta 7 General en %



Fuente: El autor

Actualmente, las redes sociales pueden ser un buena herramienta para encontrarse con las amistades y conocer nueva gente, pero no está excento de peligros. Así que lo mejor siempre será conocer los riesgos, las amenazas y las herramientas que existen para prevenirlas.

En cuanto al tema de ingeniería social, se les preguntó a los encuestados sobre si 8. ¿Sabes qué es Ingeniería Social? los siguientes fueron los resultados obtenidos.

Tabla 13 Pregunta 8 General en cantidades.

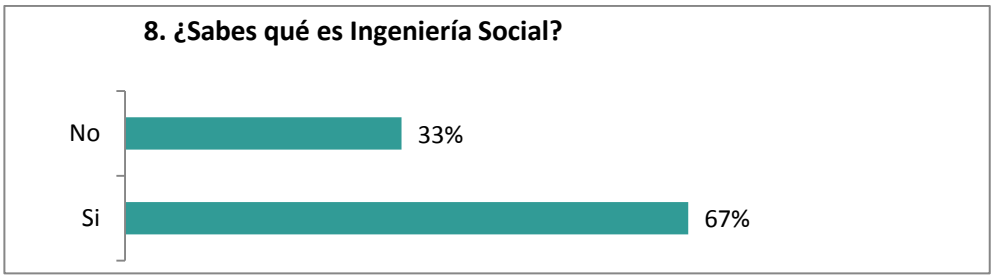
8. ¿Sabes qué es Ingeniería Social?	
Opciones	**Cantidad**
1. Si	**112**
2. No	**55**
Total	**167**

Fuente: El autor

1. 112 encuestados, un 67%, respondieron afirmativamente.
2. 55 de las 167 personas encuestadas dijeron no saber qué es la Ingeniería Social, lo que representa un 33% de la población, un alto porcentaje de usuarios que pueden ser víctimas de ataques informáticos de este tipo.

El asunto de la Ingeniería Social es muy distinguido por los psicólogos y abogados; por su contenido legal, también, por las personas de las áreas de informática o áreas tecnológicas. De ahí que de las 67% de personas que reconocen el tema la mayoría son profesionales en estas tres ramas.

Gráfica. 8 Pregunta 8 General en %



Fuente: El autor

En la encuesta se preguntó también sobre 9. ¿si ha sido víctima de la ingeniería social?

1. 88 de los 167 encuestados, equivalentes al 53% de la población, respondieron afirmativamente frente a ser vítima de la ingeniería social.
2. Mientras que los 79 encuestados o el 47% respondieron negativamente.

En conclusión, en este punto 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 Phishing, Vishing, Baiting, Quid pro quo, etc. En especial, a las cuenta de correo personales o de dominios ajenos al de la Universidad del Valle.

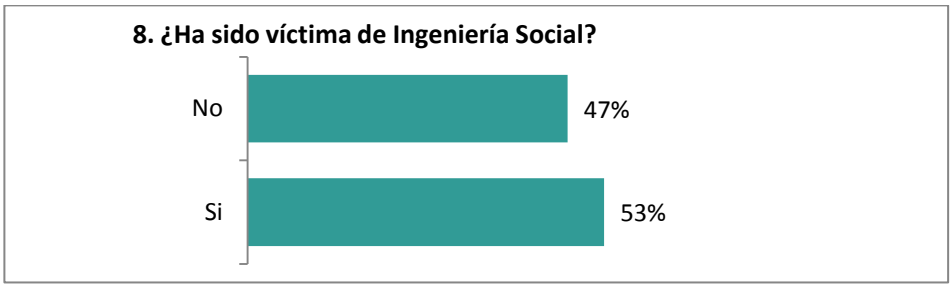
Tabla 14 Pregunta 9 General en cantidades.

9. ¿Ha sido víctima de Ingeniería Social?	
Opciones	**Cantidad**
1. Si	**88**
2. No	**79**
Total	**167**

Fuente: El autor

En la siguiente gráfica los resultados demuestran que la mayoría de la personas encuestadas han sido víctima de la ingeniería social.

Gráfica. 9 Pregunta 8 General en %



Fuente: El autor

El ingeniero social se aprovecha de que a las personas les gusta ganar algo a cambio de poco, por esta razón la estrategia de usar los mensajes de texto donde quien los recibe se hace ganador de un gran premio y para hacerlo efectivo debe enviar una pequeña suma de dinero para efecto de trámites sea tan efectiva.

De la pregunta número 9 de la encuesta 10. ¿De los siguientes medios de comunicación, cuál cree usted que es más vulnerable a una amenaza informática? Su importancia radica en que en la institución no existen mayores controles de la amenazas, riesgos y vulnerabilidades frente al uso del internet.

1. Como resultado se encontró que 64 de los 167 encuestados dijeron que el E-mail era el medio más propenso para materializar una amenaza.
2. 56 dijeron que las redes sociales.
3. 35 encuestados descargas en internet.
4. 12 no tenia idea.

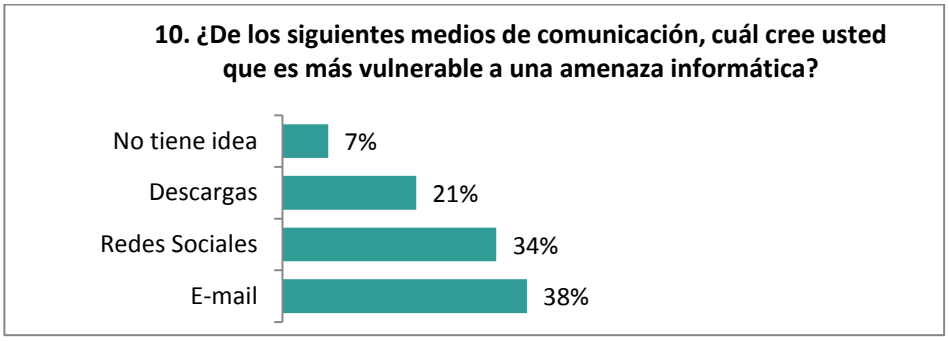
Tabla 15 Pregunta 10 General en cantidades.

10. ¿De los siguientes medios de comunicación, cuál cree usted que es más vulnerable a una amenaza informática?	
Opciones	**Cantidad**
1. E-mail	**64**
2. Redes Sociales	**56**
3. Descargas	**35**
4. No tiene idea	**12**
Total	**167**

Fuente: El autor

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 y al personal ajeno.

Gráfica. 10 Pregunta 10 General en %



Fuente: El autor

Se concluye que en este punto desarrollado en la encuesta se acerca al tema del correo e-mail, que es como la parte mayor de la probabilidad para permitir de que la materialización de una amenaza, fue seleccionado de manera creciente del uso de los gestores de correos electrónicos por parte de los diferentes sitios web. Estos gestores no son explícitos a la hora de los procesos de ejecución y coaccionan al usuario donde la cual instalen un sinfín de aplicaciones maliciosas que es lo único que se logran es iniciar un proceso de daño y poner en riesgo el sistema de información.

6.2 RECOMENDACIONES DE LA ENCUESTA

Mediante la utilización de las encuestas realizadas a los estudiantes, personal administrativo, profesores y persona ajenas de la universidad, se pudo conocer que tienen poco conocimiento o desconocimiento acerca de la Ingeniería Social y se dan las siguientes recomendaciones:

Concientizar del uso de las redes sociales y la manipulación de la información tanto para los estudiantes, administrativos y profesores, sobre los riesgos que existen para no ser víctima de la Ingeniería Social.

Usar múltiples contraseñas en las cuentas que el usuario tiene en redes sociales o correos electrónicos, ya que es común que tengan varias. Si el delincuente informático tiene ingreso a una de las cuentas puede ingresar a todas, adicional se debe estar cambiando la contraseña periódicamente[92].

Uso de antivirus: Tener y mantener el antivirus de los computadores actualizado y funcionando, para protegerse de cualquier virus que pueda entrar a través del navegador, memorias extraíbles o archivos adjuntos[93].

Uso de contraseñas seguras, para protegerse se debe hacer las siguientes recomendaciones:

- La longitud de las contraseñas no debe ser inferior a ocho caracteres, a mayor longitud más difícil será de reproducir y mayor seguridad ofrecerá.
- Construir las contraseñas con una combinación de caracteres alfabéticos donde se combinen las mayúsculas, las minúsculas y caracteres especiales, adicional se debe cambiar la contraseña regularmente o periódicamente.
- No compartir las contraseñas por medio de correos electrónicos, ni por teléfono o mensajes de texto. Se debe desconfiar de correos electrónicos que la soliciten la contraseña porque puede ser víctima de este ataque.

[92] LÓPEZ VILLA, Oscar y RESTREPO GIL, Wilmar. ANÁLISIS Y DESARROLLO DE ESTRATEGIAS PARA LA PREVENCIÓN DEL USO DE LA INGENIERÍA SOCIAL EN LA SOCIEDAD DE LA INFORMACIÓN. En: Ing. USBMed. Diciembre, 2013. vol. 4, n° 2, p. 16-22.
[93] LÓPEZ VILLA. Op. cit., p. 7.

- No se deben escribir las contraseñas en un lugar público y al alcance de los demás por ejemplo: escrita en papel y dejarla encima del portátil o la mesa de escritorio, etc. Tampoco en documento de texto dentro del ordenador.
- Cambiar periódicamente las claves. Esto aumenta el nivel de seguridad de las credenciales.
- Prestar atención cuando se accede a los servicios desde espacios públicos (café internet, etc.). Existen programas que facilitan la interferencia de las plataformas y pueden almacenar las pulsaciones del teclado.
- Elegir una contraseña que el usuario pueda recordarse fácilmente y que pueda escribirse rápidamente, sin que sea necesario mirar el teclado[94].

Correo electrónico no deseado, los siguientes son algunos consejos básicos para protegernos:

- No compartir la dirección con cualquiera.
- No abras los correos no deseados, es una de las principales fuentes de infección.
- No conteste a los correos no deseados.
- Utilizar activamente los filtros antispam[95].

Implementar un mecanismo en el cual genere un control que evite que cualquier tipo de usuarios puedan compartir recursos en la red. Esto con el fín de que se puede hacer negándole los privilegios a las cuenta de cada usuario en un equipo o desde el controlador de dominio.

[94] INTECO. Política de contraseñas y seguridad de la información. [En línea]. Bogotá: Instituto Nacional de Tecnologías de la Comunicación. 2017., 7 p. Disponible en: https://www.unirioja.es/servicios/si/seguridad/difusion/politica_contrasenas.pdf.
[95] Ibid., p. 7.

Disuadir a los colaboradores y estudiantes para que manejen de forma adecuada su información personal y el uso de las resdes sociales.

Socializar las leyes que actúan ante los ataques de Ingeniería Social aplicados por medios informáticos.

6.3 CASO TEÓRICO

El ejercicio descrito a continuación explica las fases de un ataque de ingeniería social y 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 Universidad del Valle de manera teórica, 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.

La primera fase implica un acercamiento para generar confianza con la víctima, en este caso, cualquier funcionario de la Univerisdad del Valle. **Luego, la segunda fase el reconocimiento**, en esta se realiza la indagación de la seguridad interna de la Universidad del Valle, esto se logra por medio de correos, haciéndose pasar por personal técnicos de algún servicio o incluso mediante una presentación formal en una charla. En esta última modalidad, es necesario que la persona que va a realizar el ataque de ingeniería social se muestre simpático, sin dar a la víctima ningún motivo de sospecha. En esta etapa, el esfuerzo es fundamental para captar cualquier información valiosa. Dentro de las instalaciones, se 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.

> "Si bien, los más vulnerables son aquellos que trabajan atendiendo al público, se puede decir que también entran aquellos que son confiados, aquellos que no siguen buenas políticas de seguridad, aquellos que rompen reglas o simplemente las desconocen", dice Abraham al respecto. Por su parte, la ingeniera Jacqueline sostiene que "los niños, las empleadas del servicio y las amas de casa son extremadamente vulnerables a la ingeniería social. De igual manera, en el ámbito empresarial, los hombres son fácilmente seducidos por mujeres muy atractivas y viceversa[96]".

La tercera fase, es el de crear el escenario, el ingeniero social suplanta la página del login del correo institucional de la universidad con el objetivo de acceder a información confidencial manejada por los usuarios para lograr recopilar la mayor cantidad de nombres de usuarios y password de los funcionarios de la Universidad del Valle.

La cuarta fase es la realización del ataque, con las herramientas y la información obtenida, mediante una técnica denominada Password Harvesting[97], por medio del phishing intentamos recopilar contraseñas de los funcionarios de la Universidad del Valle. Para conseguir su objetivo, en primer lugar, comienzan enviando correos electrónicos suplantando la imagen de la Universidad del Valle conocida que aporta la confianza necesaria. El email contiene un enlace falsificado donde mediante el uso del engaño consiguen que el usuario entre en él. Una vez en la página a la cual dirige el enlace, se solicita a la persona que introduzca sus datos personales. Este, al confiar en el email, los otorga y ahí es cuando pasa a ser víctima del Phishing. Es una de las técnicas más utilizadas porque las webs que falsifican son muy similares a las originales y legítimas y el phisher utiliza la imagen corporativa de la institución en los emails para que sean más fiables.[98]

[96] TECNOLOGÍAS PARA EMPRESAS. "INGENIERÍA SOCIAL: EL HACKEO SILENCIOSO". [En línea]. Marzo 2016. [29 abril de 2017]. Disponible en: http://www.enter.co/guias/tecnoguias-para-empresas/ingenieria-social-el-hackeo-silencioso/.

[97] Cosecha y pesca de contraseñas

[98] LEGUIZAMON, Mayra. EL PHISHING. España, 2014, 47p. TRABAJO FINAL DE GRADO (GRADO EN CRIMINOLOGIA Y SEGURIDAD). Universidad Jaime I. España.

La quinta fase es la recogida de los datos. Se debe esperar a que la víctima ingrese sus datos confidenciales para así poder obtenerlos.

La sexta fase es la ejecución del fraude: Este proceso de la siguiente fase, es como una vez que el ingeniero social tiene la información y logra su meta, los utiliza para beneficio propio o vende la información a terceros para que estos realicen el delito informático.

La séptima fase es el post-ataque. En este punto, el phisher tiene como objetivo, eliminar todo rastro que pudiera luego inculparle de este delito.

En el siguiente cuadro están algunas de las técnicas más usadas de Ingeniería Social que los delincuentes informáticos pueden utilizar en la universidad.

Tabla 16 Técnicas de Ingeniería Social.

TÉCNICAS	DESCRIPCIÓN	MODUS OPERANDI	COMO PREVENIRLA
Phishing	Es una modalidad de estafa con el objetivo de intentar obtener de un usuario sus datos, claves, cuentas bancarias, de crédito, identidades, etc. Resumiendo "todos los datos posibles" para luego ser usados de forma fraudulenta[99].	El phishing puede producirse de varias formas, desde un simple mensaje a su teléfono móvil, una llamada telefónica, una web que simula una entidad, una ventana emergente, y la más usada y conocida por los internautas, la recepción de un correo electrónico. Página Web o ventana emergente; es muy clásica y bastante usada. En ella se simula suplantando visualmente la imagen de una entidad oficial , empresas, etc. pareciendo ser las oficiales. El objeto principal es que el usuario facilite sus datos privados. La más empleada es la "imitación" de páginas Web de bancos, siendo el parecido casi idéntico pero no oficial [100].	Para prevenir el phishing se debe evitar en todo momento no hacer clic en enlaces incluidos en mensajes de correo electrónico, ya que pueden albergar malware. Sé precavido cuando recibas mensajes de proveedores o terceros; nunca hagas clic en las direcciones URL.[101]
			Para visitar sitios Web, dar click en la dirección URL en la barra de direcciones, nunca por enlaces procedentes de cualquier sitio.
			Tener un firewall de primera línea, todos los equipos deben tener el antivirus actualizado y contar con un antispam dinámico e inteligente.

[99] GONZÁLEZ, Carlos. Programa Integración de Tecnologías a la Docencia. [En línea]. Medellín: Universidad de Antioquia. 2016., 4 p. Disponible en: http://aprendeenlinea.udea.edu.co/lms/moodle/pluginfile.php/99876/mod_resource/content/0/Modulo1/Navegadores.pdf.

[100] Ibid., p. 4.

[101] Latam.kaspersky.com. (2017). [online] Available at: https://latam.kaspersky.com/resource-center/preemptive-safety/phishing-prevention-tips.

Tabla 17 (Continuación)

TÉCNICAS	DESCRIPCIÓN	MODUS OPERANDI	COMO PREVENIRLA
Pretexting	El pretexting (pretextos) implica llamar por teléfono al usuario y pedirle cierta información, generalmente simulando ser alguien que precisa su ayuda. Esta técnica puede funcionar bien si se usa mediante aquellos usuarios de bajo nivel técnico y que tengan acceso a información sensible[102].	Cuando el atacante se hace pasar por un empleado de soporte técnico de la empresa en la cual trabaja la víctima. De esta manera trata de generar empatía para ganar credibilidad, pero acto seguido presenta algún tipo de excusa o pretexto (pretexting), como alertar a la víctima de un comportamiento inadecuado en su equipo, el cual requiere de su intervención. Así podrá dar instrucciones específicas que terminarán en la instalación de algún tipo de malware, concretando así su objetivo (tomar el control del equipo, obtener datos sensibles, etc)[103].	Solicitar datos más específicos, de modo que sean poco probables de ser hallados en Internet, para que el ciberdelincuente no pueda hacerse pasar fácilmente por el usuario ante los teleoperadores.
			Envío de las facturas por mail o a través de la descarga desde el portal de usuario. Además, si es posible, para la recuperación de contraseñas de acceso se debe recomendar el uso de correos electrónicos con soluciones de doble factor de autenticación.
			Precisar una autenticación doble, en especial, cuando se traten datos sensibles (tarjetas de crédito, perfiles…) o incluso combinar el acceso protegido mediante una contraseña inicial que tenga limitados los errores sucesivos de acceso y la solicitud de un "pin" parcial mediante teclado para autorizar transacciones.

[102] SHACKLEFORD, Dave. Pruebas de penetración en ingeniería social: cuatro técnicas efectivas. [En línea]. TechTarget. 2012., 4 p. Disponible en: http://searchdatacenter.techtarget.com/es/consejo/Pruebas-de-penetracion-en-ingenieria-social-cuatro-tecnicas-efectivas.

[103] PISCITELLI, Emiliano. Ingeniería Social: Cuáles son los tipos de ataque. [En línea]. RedUSERS. 2015., 5 p. Disponible en: http://www.redusers.com/noticias/ingenieria-social-cuales-son-los-tipos-de-ataque/.

Tabla 18 (Continuación)

TÉCNICAS	DESCRIPCIÓN	MODUS OPERANDI	COMO PREVENIRLA
Media Dropping	La descarga en medios suele implicar la presencia de un disco USB en un lugar razonable, como un aparcamiento o la entrada al edificio. El ingeniero social busca el interés de la persona que, al utilizar esta unidad flash, lanza un ataque contra el equipo donde se conecta[104].	Otra de las técnicas más conocidas y efectivas es dejar una USB en el parqueadero o en un sitio cercano a la oficina (como un café o un restaurante) para que algún empleado la lleve y la conecte a su computador. La USB, en principio, parece inofensiva, pero en realidad está cargada con malware que puede poner en peligro todo el sistema corporativo. Muchas compañías han deshabilitado los puertos USB de sus computadores, pero eso lo quita bastante funcionamiento al equipo.[105].	Educar a los empleados o personal y hacerles caer en cuentas las consecuencias que puede tener una vulnerabilidad informática[106]. Tener un firewall de primera línea, todos los equipos deben tener el antivirus actualizado y contar con un antispam dinámico e inteligente[107].

[104] SHACKLEFORD. Op. cit., p. 7.
[105] ENTER. LA INGENIERÍA SOCIAL: EL ATAQUE INFORMÁTICO MÁS PELIGROSO. [En línea]. ENTER.CO. 2016., 7 p. Disponible en: http://www.enter.co/guias/lleva-tu-negocio-a-internet/ingenieria-social/
[106] Ibid., p. 6.
[107] Ibid., p. 6.

Tabla 19 (Continuación)

TÉCNICAS	DESCRIPCIÓN	MODUS OPERANDI	COMO PREVENIRLA
Tailgating: acceso a zonas restringuidas	El tailgating supone lograr acceso a una instalación física mediante engaño a su personal, o simplemente colándose dentro. El objetivo de este test es demostrar que el atacante puede superar a la seguridad física[108].	Los atacantes deberían ser capaces de obtener información sensible o poder instalar un dispositivo rápidamente para mostrar su éxito, ya que tienen poco tiempo para hacerlo antes de salir de la instalación. Si el atacante instalar un sistema de pruebas dropo box con acceso a la red Wifi podrá acceder posteriormente a los datos sensibles de la empresa[109].	Guardias de seguridad que realicen una inspección visual.
			Torniquetes que permitan el acceso individual.
			Sensores que detecten múltiples personas.
			Controles biométricos.
			Cámaras con reconocimiento facial.

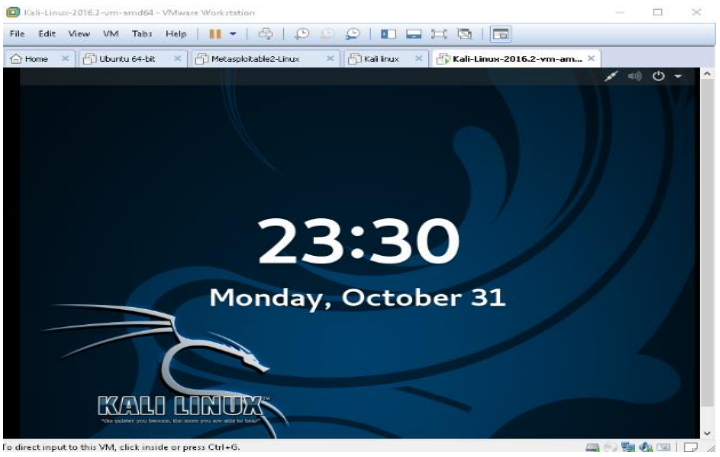
Fuente: http://searchdatacenter.techtarget.com/es/consejo/Pruebas-de-penetracion-en-ingenieria-social-cuatro-tecnicas-efectivas

[108] SHACKLEFORD. Op. cit., p. 3.
[109] Ibid., p. 3.

6.4 CASO PRÁCTICO

A continuación se crea una máquina virtual y se instala el software de virtualización (VirtualBox[110], Virtual PC[111] o VMWare Player[112]) e instalación de Kali Linux[113] como se muestra en la siguiente imagen.

Figura 6 Instalación Kali Linux



Fuente: Autor

Seguidamente, se identifica la Ip del equipo atacante “192.168.119.137” ingresando el comando “ifconfig” en el terminal.

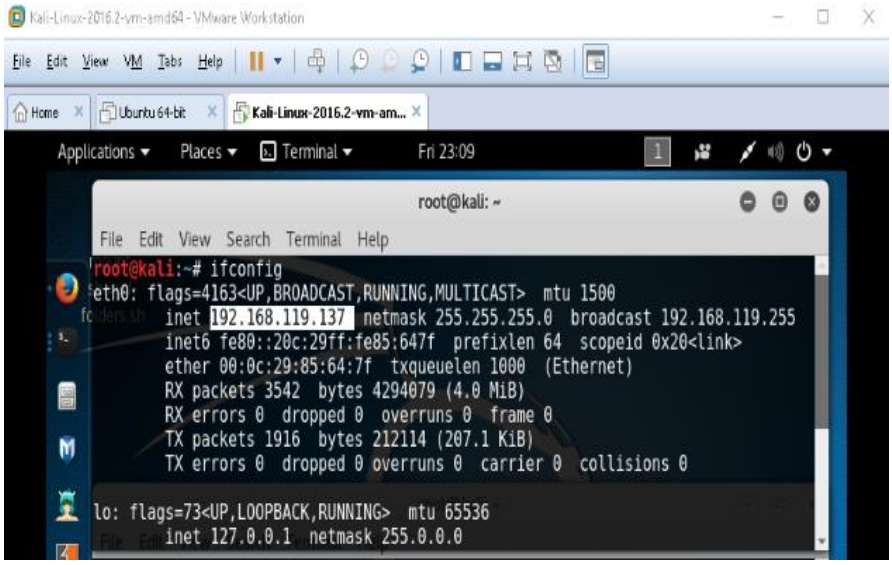
[110] VirtualBox es una herramienta de virtualización de código abierto multiplataforma disponible para Windows, Linux y Mac OS X u otros sistemas operativos, que permite crear unidades de disco virtuales donde podemos instalar un sistema operativo invitado dentro del que utilizamos normalmente en nuestro equipo.

[111] Windows Virtual PC. Windows Virtual PC (antes llamado Microsoft Virtual PC, luego renombrado Windows Virtual PC en Windows 7) es un software gestor de virtualización desarrollado por Connectix y comprado por Microsoft para crear equipos virtuales.

[112] Use VMware Workstation Player para crear, ejecutar, evaluar y compartir software que se ejecute en máquinas virtuales: Crear: use VMware Workstation Player para crear máquinas virtuales con los últimos sistemas operativos de Windows y Linux de 32 y 64 bits.

[113] Kali Linux es una distribución de Linux avanzada para pruebas de penetración y auditorías de seguridad. Kali es una completa re-construcción de BackTrack Linux desde la base hacia arriba, y se adhiere completamente a los estándares de desarrollo de Debian.

Figura 7 IP del atacante.

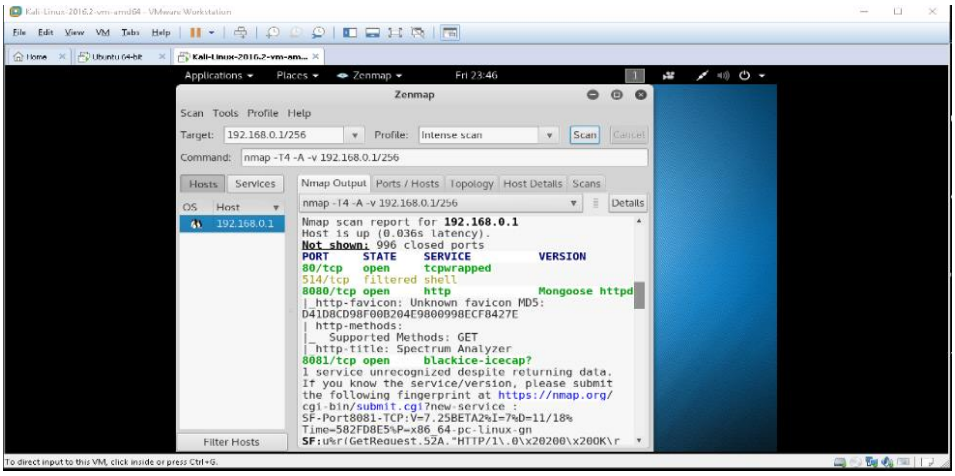


Fuente: Autor

Asimismo, para realizar pruebas se debe instalar una máquina virtual con el sistema operativo linux Ubuntu que va hacer la máquina atacada. A continuación, abrir la herramienta Zepmap[114] que está instalada en Kali linux para identificar los equipos que hay en la red donde se va a realizar el ataque, como se evidencia en la siguiente figura. Donde muestra los resultados del escaneo y se valida los equipos que están activos en la red, sistemas operativos, etc.

[114] Nmap es un programa de código abierto que sirve para efectuar rastreo de puertos escrito originalmente por Gordon Lyon (más conocido por su alias Fyodor Vaskovich) y cuyo desarrollo se encuentra hoy a cargo de una comunidad. Fue creado originalmente para Linux aunque actualmente es multiplataforma.

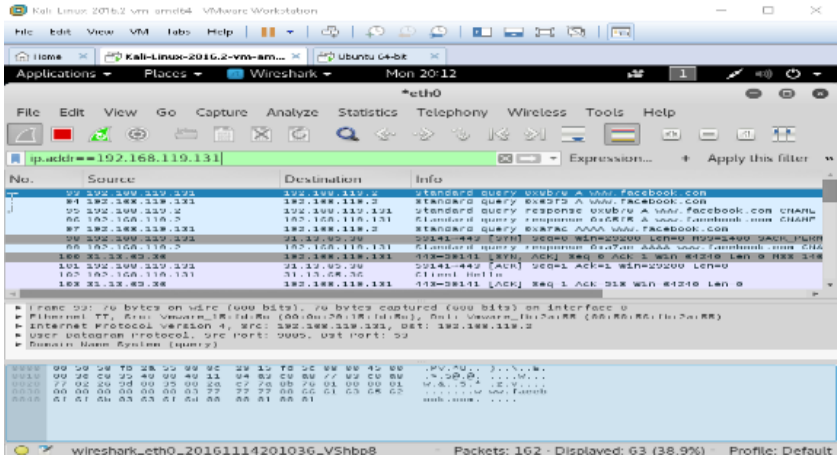
Figura 8 Escaneo con Zenmap



Fuente: Autor

Luego, abrir la herramienta Wireshark[115] para monitorear el tráfico de la red para identificar la dirección Ip y las páginas que está usando nuestra victima a la que se le va a dirigir el ataque.. Se observa que el usuario 192.168.119.131 ”host victima” está usando Facebook “trusted host”.

Figura 9 Escaneo con Wireshark

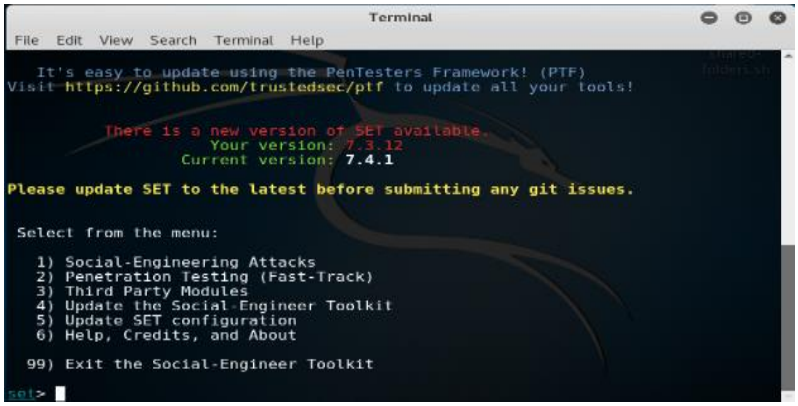


Fuente: Autor

[115] Wireshark es una herramienta imprescindible con la que podemos capturar y analizar el tráfico que transita a través de nuestra red. En la entrada de hoy vamos a ver cómo instalar Wireshark en Ubuntu y además veremos cómo ejecutar esta aplicación 100% operativa sin necesidad de ser root.

Ahora bien, para realizar la clonación de la página se utiliza la herramienta "Setoolkit[116]" que está instalada en Kali Linux, SET "Social Engineer Toolkit", y se selecciona la opción 1 "Social-Engineering Attacks".

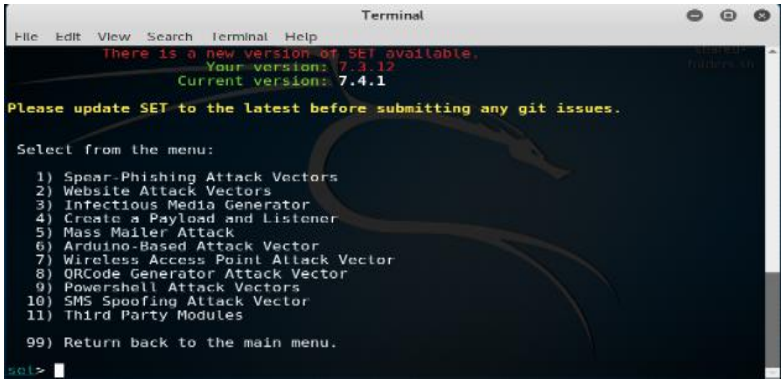
Figura 10 Ejecución de Setoolkit



Fuente: Autor

Posteriormente, la opción 2 "Website Attack Vector" como se muestra en la siguiente imagen.

Figura 11 Herramienta Setoolkit

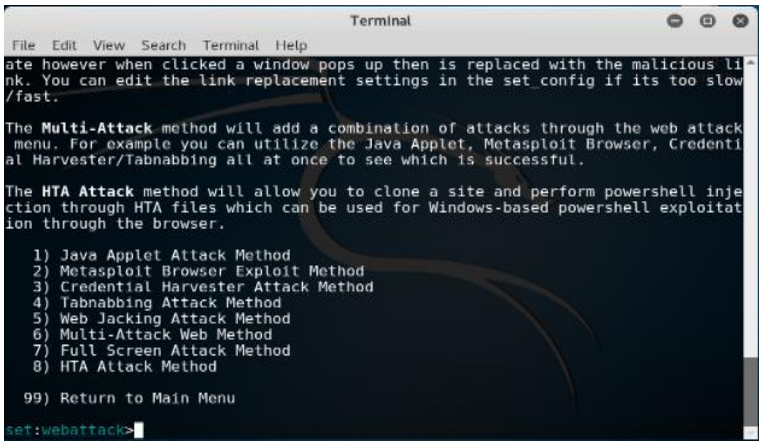


Fuente: Autor

[116] SET es una completísima suite dedicada a la ingeniería social , que nos permite automatizar tareas que van desde el de envío de SMS (mensajes de texto) falsos, con los que podemos suplantar el numero telefónico que envía el mensaje, a clonar cualquier pagina web y poner en marcha un servidor para hacer phishing en cuestión de segundos.

A continuación, la opción 3 “Credential Harvester Attack Method”.

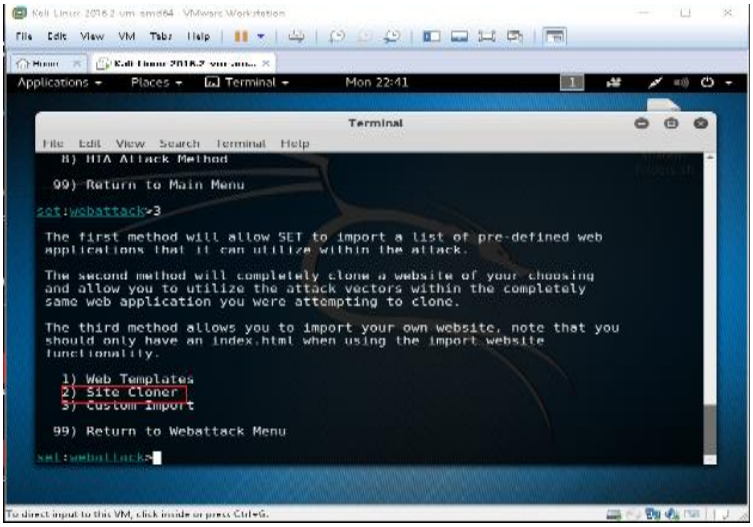
Figura 12 Herramienta Setoolkit



Fuente: Autor

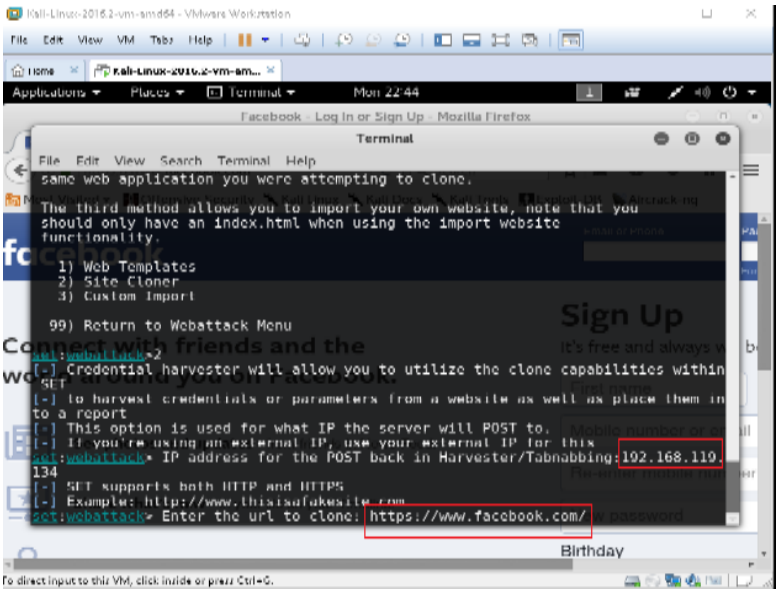
Asi mismo, seleccionar la opción 2 “Site Cloner” e ingresar los datos de la dirección IP del atacante 192.168.119.134 y la dirección de la página a clonar en este caso www.facebook.com, como se muestra en las siguientes figuras.

Figura 13 Selección de Site Cloner



Fuente: Autor

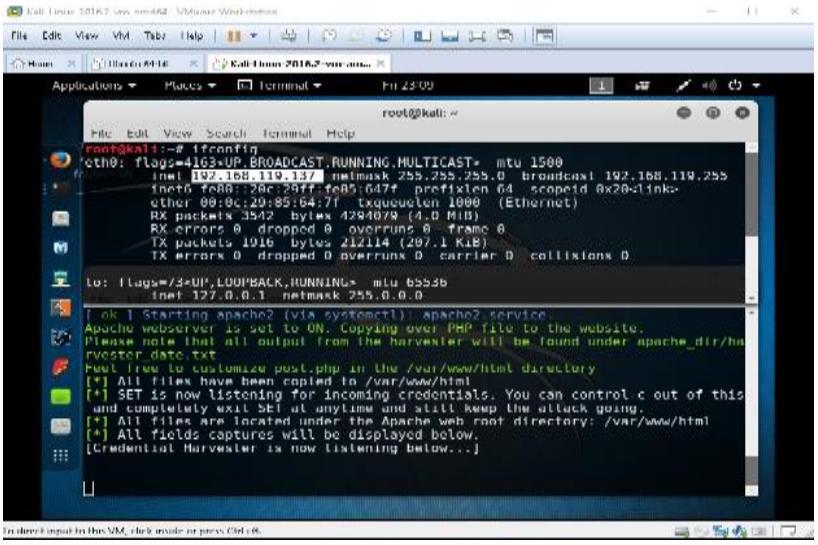
Figura 14 Ingreso de la página a clonar



Fuente: Autor

Finalmente, sitio web de Facebook esta clonado como se muestra en la siguiente imagen.

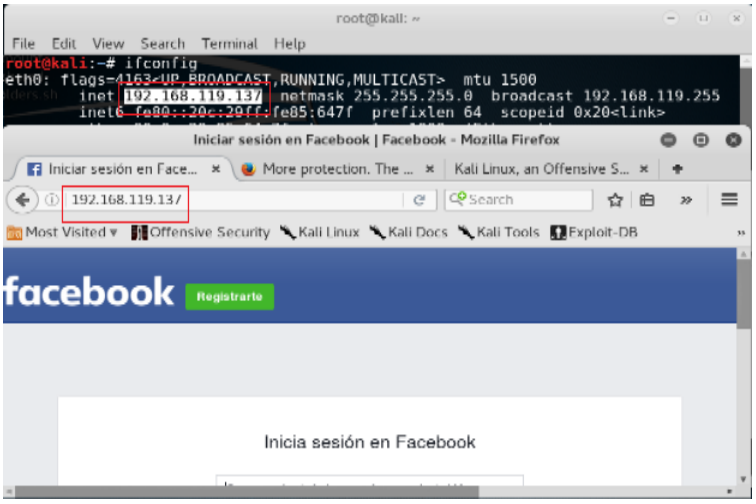
Figura 15 Clonación de Facebook



Fuente: Autor

A continuación comprobamos que la página web este clonada ingresando la dirección IP y como se evidencia en la siguiente imagen.

Figura 16 Comprobación Ip clonada



Fuente: El autor

Ahora bien, se procede a configurar nuestro Sniffer[117], para este proceso se utiliza Ettercap[118] que es una herramienta que esta instalada en Kali Linux. Abrir el terminal e ingresar como super usuario “root” para poder modificar el firewall local, utilizar el siguiente comando leafpad /etc/Ettercap/etter.conf y modificamos las siguientes líneas:

ec_uid = 65534 (por defecto) por “ec_uid = 0”.

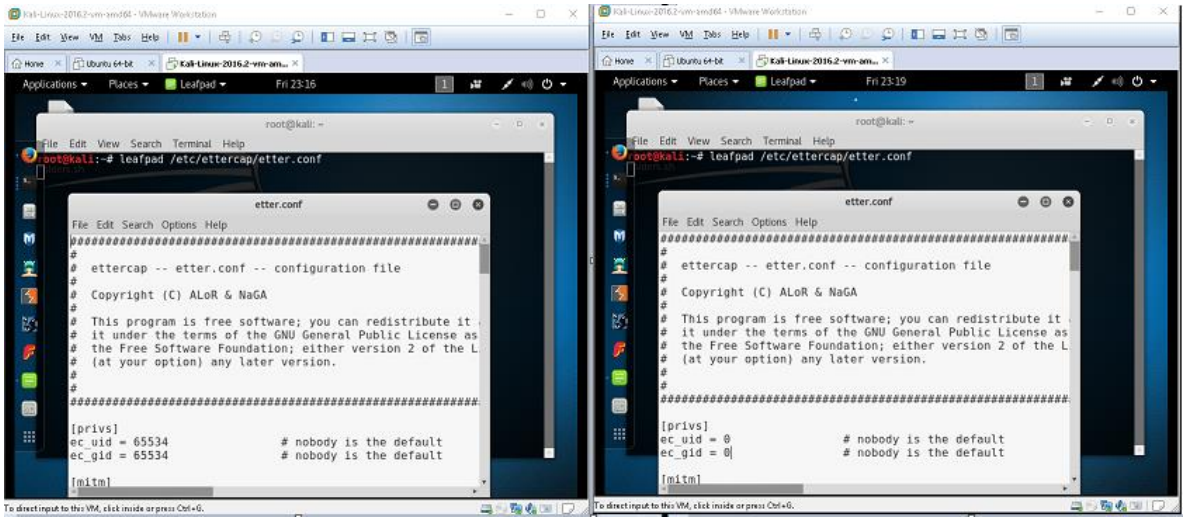
ec_gid = 65534 (por defecto) por “ec_uid = 0”.

[117] Un sniffer es una aplicación especial para redes informáticas, que permite como tal capturar los paquetes que viajan por una red. Este es el concepto más sencillo que podemos dar al respecto, pero profundizando un poco más podemos decir también que un sniffer puede capturar paquetes dependiendo de la topología de red.

[118] Ettercap es un interceptor/sniffer/registrador para LANs con switch. Soporta direcciones activas y pasivas de varios protocolos (incluso aquellos cifrados, como SSH y HTTPS).

A continuación, se muestras los cambios realizados del punto anterior.

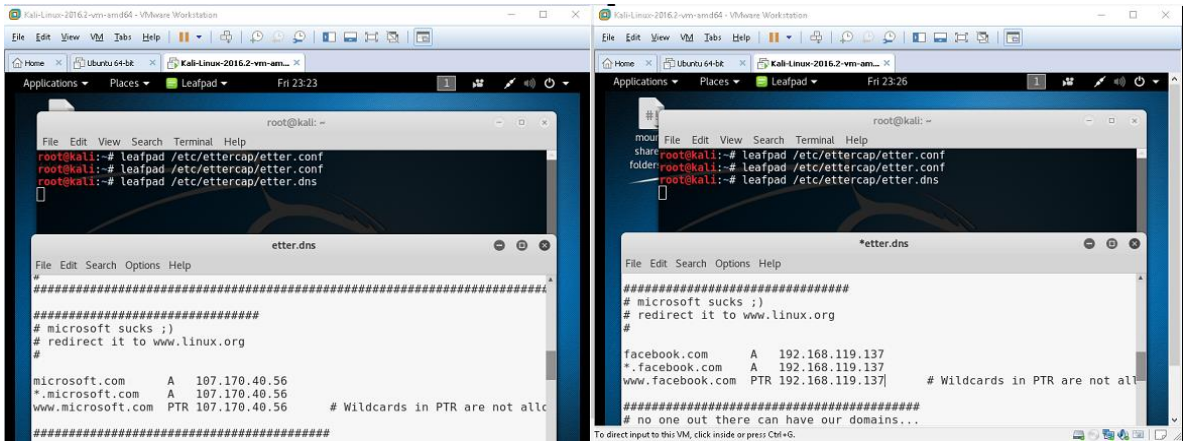
Figura 17 Configuración del Ettercap



Fuente: El autor

Ahora, modificar el archivo DNS “etter.dns”, ingresando el siguiente comando ”**leadpad /etc/ettercap/éter.dns**” y cambiar Microsoft.com por Facebook la cual se quiere realizar el ataque DNS Spoof, se modifica las siguientes líneas como se evidencia a continuación.

Figura 18 Configuración DNS.

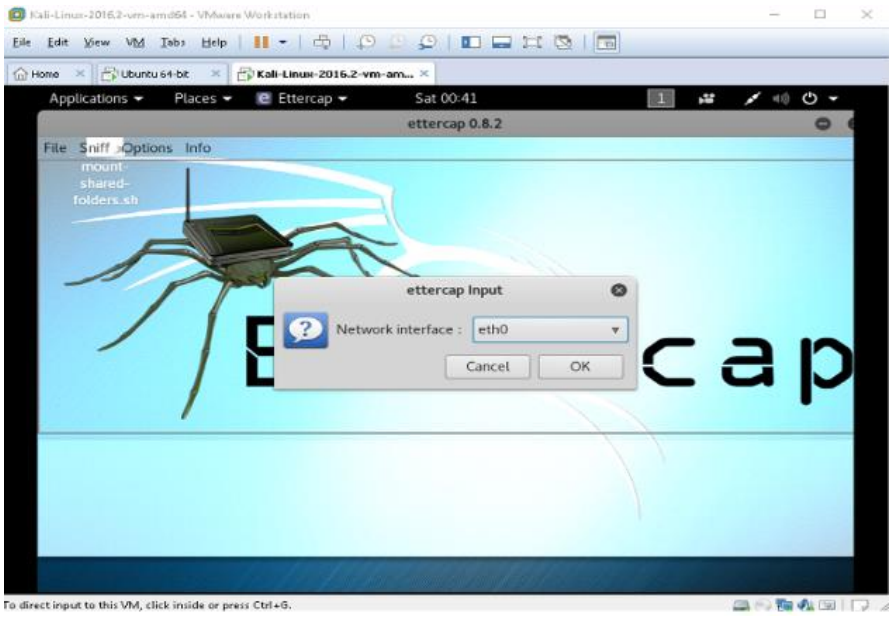


Fuente: El autor

Finalmente, terminamos la configuración del ettercap con los parámetros que se necesitan, configurando el Sniffer para capturar y detectar los datos cuando el usuario atacado ingrese a la página Facebook, redirecccionando a la página clonada.

Seguidamente, se procede a abrir Ettercap para empezar con el ataque y seleccionar la tarjeta de red para que todo el tráfico que se genere en la PC victima pase por esta.

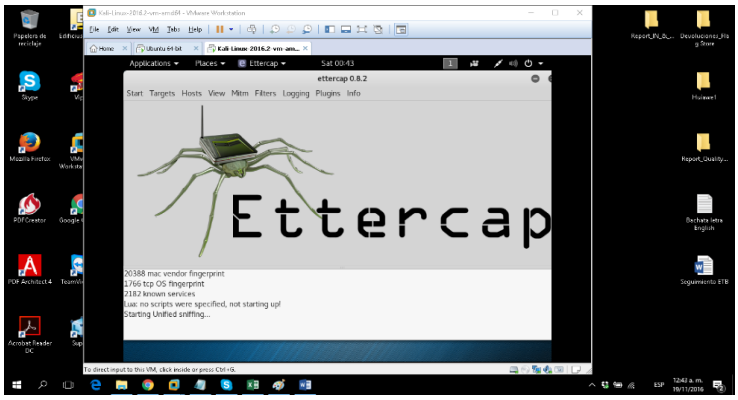
Figura 19 Herramienta Ettercap



Fuente: El autor

Luego, se realiza el escaneo para ver que equipos están en la red para configurar el ataque e identificar la IP Gateway y el equipo víctima. Ingresamos a la opción Host y seleccionamos Host List.

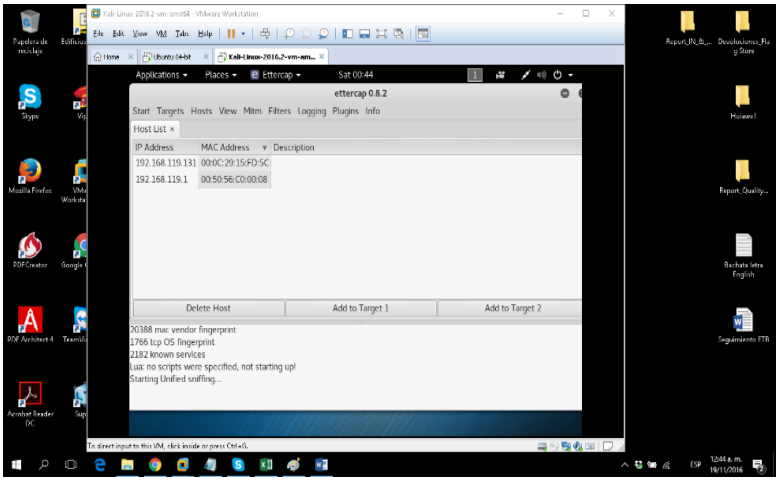
Figura 20 Escaneo con Ettercap



Fuente: El autor

Ahora, se determina que para la opción Add to Target1 se asigna la Ip Gateway y la IP del equipo víctima a Target 2

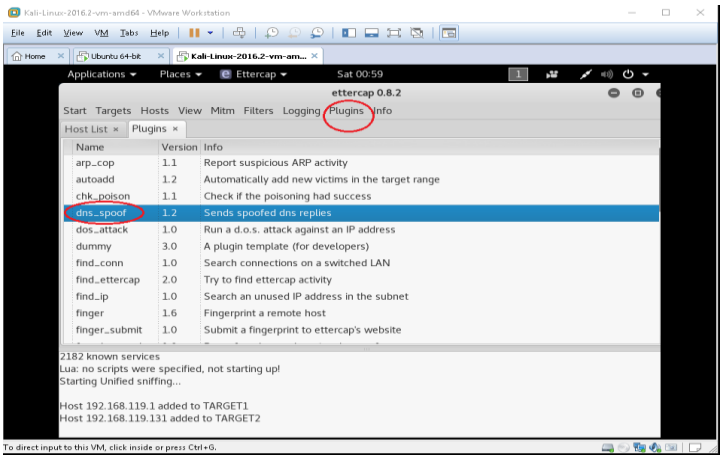
Figura 21 Asignación de IP.



Fuente: El autor

A continuación, seleccionar Plugins - Manage the plugins – Dns Spoof, como se muestra en la siguiente imagen.

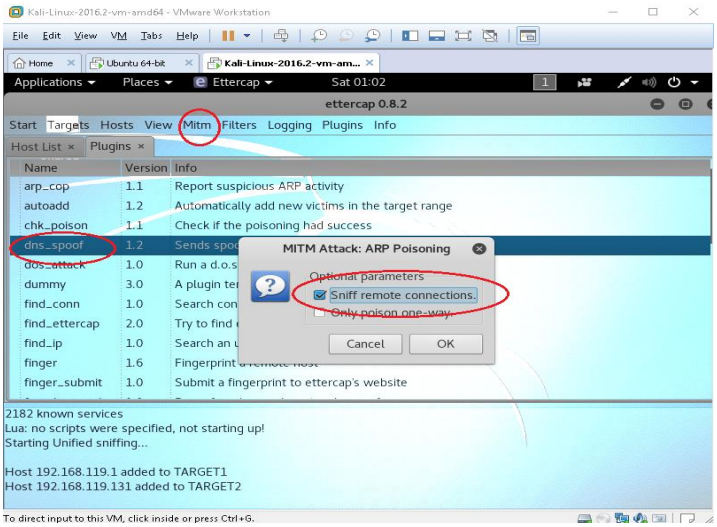
Figura 22 Selección del Plugins



Fuente: El autor

Seguidamente, seleccionar Mitm (Man in the middle)-ARP poisoning y Sniff remote connections.

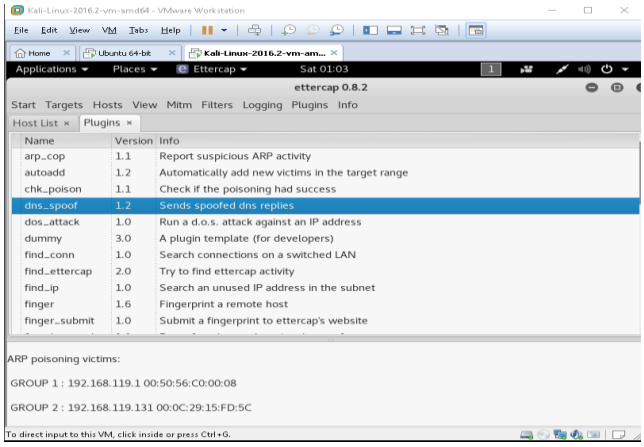
Figura 23 Selección Mitm y Sniff.



Fuente: El autor

Finamente, queda configurado el esquema para realizar el ataque, como se muestra en la siguiente imagen.

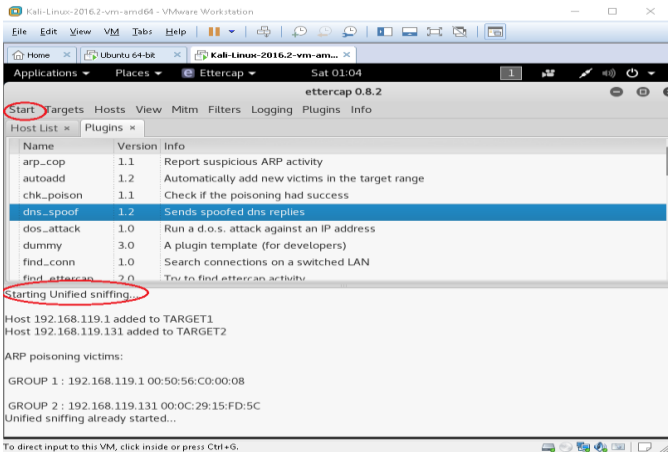
Figura 24 Configuración del Ettercat



Fuente: El autor

En esta fase, se empieza a realizar el ataque a la víctima ya que todo esta configurado, dar click en la opción Start y se debe esperar a que ingrese a la página clonada.

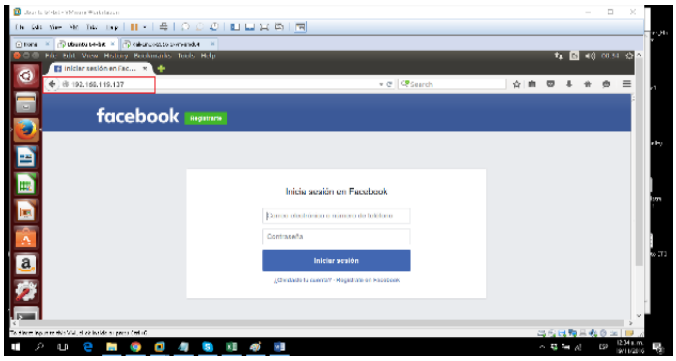
Figura 25 Cominezo del ataque con ettercap.



Fuente: El autor

Para realizar la prueba virtual se debe ingresar a la máquina virtual Ubuntu la cual es la víctima y abrir el navegador e ingresar a Facebook y registrar los datos, como se evidencia en la siguiente imagen.

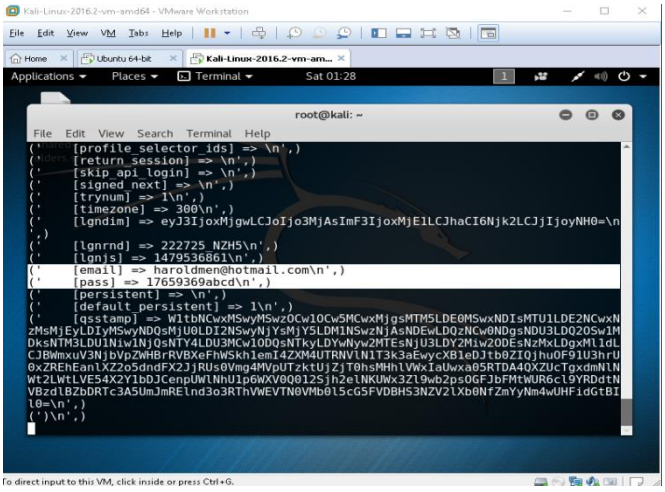
Figura 26 Máquina de la victima



Fuente: El autor

Finalmente, se puede identificar el ID y Password que ingreso el usuario atacado sin que él se diera cuenta, como se muestra en la siguiente imagen. Para esta prueba se realizo con una cuenta personal de Facebook.

Figura 27 Ataque completo



Fuente: El autor

6.5 RECOMENDACIONES DEL CASO PRÁCTICO

A continuación se debe tener en cuenta las siguientes recomendaciones o consejos para no ser víctima de ingeniería social del tipo de ataque anterior:

- Políticas de seguridad a nivel de sistema operativo.
- Análisis con antivirus de todos los correos electrónicos recibidos.
- Capacitación al personal y de que sean conscientes del riesgo potencial de estos ataques de ingeniería social.
- Ponga atención en la URL del sitio web y asegurarse que sea correcta. Los sitios web maliciosos pueden parecer idénticos a los sitios legítimos, pero la URL puede tener variaciones o un dominio diferente.
- Nunca haga click en un enlace a una página web que le llegue a través de un e-mail en el que le piden datos personales.
- Cuando navegue por Internet, busque páginas de confianza, de ser posible, avaladas por sellos o certificados de calidad, evitando contenidos dudosos.
- No envíe información sensible a través de Internet antes de verificar la seguridad del sitio web.
- Mantener el sistema operativo y el navegador actualizados oportunamente.
- Conocer los riesgos asociados al uso de Internet. ¡Hay que mantenerse al día! Es aconsejable estar suscrito a los boletines de correo de la OSI, que incluyen los últimos avances de actualidad[119].

En síntesis se puede decir que “La mejor manera de estar protegido contra la ingeniería social y sus técnicas, es el conocimiento[120]”.

---

[119] HERALDO. “10 consejos para prevenir un ataque informático” [en línea], marzo 2015 [citado el 09 noviembre de 2017]. Disponible en Internet: < http://www.heraldo.es/noticias/comunicacion/2015/03/31/diez_consejos_para_prevenir_ataque_informatico_348654_311.html>.

[120] CAVIEDES FIGUEROA, Viviana Andrea y PEDRAZA GARZÓN, Carmen Lucia. GUÍAS PRÁCTICAS PARA USO DE TÉCNICAS DE INGENIERÍA SOCIAL CON LA HERRAMIENTA SET INCKUIDA EN LA DISTRIBUCIÓN BACKTRACK 4

CONCLUSIONES

Con el desarrollo de esta labor investigativa se logró visibilizar las vulnerabilidades encontradas, no solo a través de la observación y la experiencia, sino también, con los resultados de la encuesta, para sus respectivas estadísticas. Como primera instancia no existe un plan o programa de capacitación permanente al personal de la universidad respecto a los temas de la seguridad informática y de la información.

La Universidad se ingresa fácilmente a los distintas áreas y de igualmente a las oficinas de cada edificio y pasan por las zonas restringidas dentro de ellas. Muchas de las dependencias tiene fallas de diseño y organización, la cual permite que los usuarios tengan alcance a documentos y equipos de cómputo. Estas áreas como las salas de docentes, las coordinaciones laboratorio y entre otras, son muy fáciles de acceder por personal externo. También permiten una fácil visualización de las pantallas y teclados de los trabajadores.

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, programas de juego, por lo tanto la navegación no tiene mayores complicaciones, aumentando las probabilidades de infección de “malware”, llegada de “spam” o intentos de “phishing”.

Respecto a las pruebas, se realizaron en ambientes controlados considerando las leyes que nos regulan. Con los resultados obtenidos es importante la actualización del software porque de lo contrario pueden ser explotadas las vulnerabilidades y el

---

R2. Tesis De Grado Para Obtener El Título De TECNOLOGO EN REDES Y SEGURIDAD INFORMÁTICA. Colombia.: Corporación Universitaria Minuto de Dios. Facultad de Ingeniería. 2011. 58 p.

delincuente informático puede tomar el control de la máquina víctima. Por otra parte, se deben realizar capacitaciones de las consecuencias de la Ingeniería Social y de como identificarlos o neutralizarlos.

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.

7 RECOMENDACIÓN

Lo que se pretende involucrar es no incomodar a los usuarios (estudiantes) a la hora de ingresar a las instalaciones de la Universidad del Valle, establecer controles de acceso rápidos y seguros, como la identificación biométrica, o electrónica a través de los códigos de barras de los carnets. Este procedimiento debe estar complementado desarrollado para un plan de concientización que persuada a los usuarios de las ventajas de los controles en las entrada de los bloques de la administración, resaltando las necesidades se seguridad que se requieren, tanto para su protección, como para la de los empleados, de planta física e inmobiliaria.

Una de las recomendaciones acerca del aseguramiento sería el resguardo en las distintas oficinas respecto a los tipos de accesos es un punto relevante en la seguridad de la información, no es solamente en lo que se encuentra a la mano tales como documentos impresos, CD's, USB's, u otros sino también, de los computadores y los diferentes datos que en ellos se almacena. 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.

Implementar un mecanismo en el cual genere un control que evite que cualquier tipo de usuarios puedan compartir recursos en la red. Esto con el fín de que se puede hacer negándole los privilegios a las cuenta de cada usuario en un equipo o desde el controlador de dominio.

La ingeniería social parece ser una parte más común e importante de las tendencias del malware actual y futuro. Se acabaron los días de la simple explotación de las fallas de un sistema para acceder a su información personal y financiera, ahora los

delincuentes cibernéticos son ayudados por la víctima, inexperta en la manipulación difícil de algunos hackers.

Es importante tener en cuenta la ampliación del número de cámaras de seguridad dentro de 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.

La universidad cuenta con uno de los mejores antivirus del mercado, pero vale la pena recalcar que los funcionarios del departamento de gestión tecnológica deben tener en cuenta acerca del monitoreo permanente de su funcionamiento, sobre todo en todos 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. Por lo tanto se debe tener en cuenta también que 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.

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 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.

Mediante la utilización de las encuestas realizadas a los estudiantes, personal administrativo y profesores se pudo conocer que tienen poco conocimiento acerca de la Ingeniería Social.

A partir de la información obtenida mediante las encuestas se pudo obtener el resultado del conocimiento o desconocimiento acerca de la Ingeniería Social.

Socializar las leyes que actúan ante los ataques de Ingeniería Social aplicados por medios informáticos.

Utilizar Sistemas de Prevención de Pérdidas de Datos. Implementar un Sistema de Prevención de Pérdidas de Datos que pueda identificar donde reside la información sensible, controle su uso y lo proteja a esta información de perdidas.

Aplicar una política eficiente de contraseñas. Asegúrese de que las contraseñas sean fuertes, que contengan por lo menos de 8 a 10 caracteres de longitud y que incluyen una mezcla de letras y caracteres alfa-numéricos. Animar a los usuarios para que eviten reutilizar las mismas contraseñas en diferentes sitios web y prohibir el intercambio de contraseñas. Las contraseñas deben cambiarse regularmente, al menos cada 90 días. Evite escribir las contraseñas.

Se recomienda que en la universidad debe divulgar más este tipo de información acerca del tema de ingeniería social, para que las directivas se encarguen de tomar decisiones en cuanto al proceso de comunicaciones vía correo, noticias, web, y emisora universitaria.

Se recomienda concientizar más sobre el tema y el uso de las redes sociales tanto para los estudiantes, administrativos y profesores para que sepan el peligro que puede llevar a cabo este tipo de redes en nuestro sistema.

Se recomienda que en 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 que son necesarias para todo. El sitio te dirá cuánto segura y lo que significa la combinación de letras, números y símbolos en una contraseña, por la cual debe protegerse el usuario.

Se recomienda que se debe concientizar a todos los usuarios del uso de la red y la manipulación de información sobre los riesgos que existen en cada día.

Se debe implementar un sistema de políticas y procedimientos para el uso y el manejo de la información a través de medios electrónicos.

La ingeniería social parece ser una parte más común e importante de las tendencias del malware actual y futuro. Se acabaron los días de la simple explotación de las fallas de un sistema para acceder a su información personal y financiera, ahora los delincuentes cibernéticos son ayudados por la víctima, inexperta en la manipulación difícil de algunos hackers.

Se recomienda que este proceso investigativo se debe concretar la manera de pensar entre un delincuente informático. Lo que se busca para ser ejecutado paso a paso acerca de un ataque de Ingeniería Social dentro de las instalaciones de la institución, con el objetivo de demostrar que es factible lo que se materialicen este tipo de amenazas aprovechando las vulnerabilidades existentes, que no es solo a nivel tecnológico, sino también, en el recurso humano de la institución.

Estar al tanto sobre nuevas amenazas de red además de tener un control sobre el tráfico de red. Se debe monitorear y registrar los intentos de intrusión así como el

tráfico sospechoso en la red, identificar los intentos de conexión de hosts sospechosos. Recibir y estar atentos a nuevas alertas de vulnerabilidades y amenazas de distintas empresas para llevar a cabo acciones preventivas.

En menos frecuencia encontramos que los ingenieros sociales utilizan otras técnicas de Phishing como son:

- Explotar vulnerabilidad de sitios web.
- Aplicaciones falsas para dispositivos móviles.
- VoIP, específicamenteen el uso de skype.

Antivirus basado en la nube: Los antivirus son las herramientas más utilizadas para detectar y detener archivos maliciosos, sin embargo los antivirus convencionales fallan al no poder detectar muchas de las amenazas modernas y su creciente complejidad ha dado lugar a vulnerabilidades que están siendo explotadas por malwares.

Algunas tendencias presentadas en la Universidad acerca del tema de ingenieria social son:

La universidad es la práctica para obtener información confidencial a través de la manipulación de usuarios legítimos, aprovechando la tendencia natural de la gente a confiar. Es el mayor agujero de seguridad con el que podemos encontrarnos en una entidad, ya que es indetectable y no sabemos a priori cómo de vulnerables son nuestros usuarios a este tipo de artimañas.

Basándose en la interacción directa o indirecta con los usuarios dentro de la Universidad, obteniendo un acceso directo a los sistemas de información de dichos usuarios con algunas tendencias en ingenieria social.

Una de las tendencias que se presenta en la universidad es acerca del correo electrónico con anotaciones anonimas pero que para conseguirlo tienes que acceder a uno u otro enlace, o incluso facilitar algunas de tus claves. Son aquellas técnicas de manipulación y engaño es lo que se conoce como Ingeniería Social, y que buscan la manera táctica explotada cada vez más por los hackers para obtener dicha información acerca de su objetivo o páginas web.

Técnicas como el envío de mensajería instantánea para infiltrar malware, o mensajes a dispositivos móviles en los que los usuarios almacenan gran cantidad de información personal.

Elegir contraseñas que no tengan nada que ver con nosotros, totalmente aleatorias pero que sigan una lógica que sólo el propietario conoce.

No compartir nuestras contraseñas con nadie, incluso aunque sea de confianza.

Evita escribir tus contraseñas o credenciales en papel.

No abrir correo de desconocidos.

BIBLIOGRAFÍAS

AGENCIA EFE. “Supuestos yihadistas piratean dos portales de una universidad brasileña”. [En línea]. Enero 2015. [25 abril de 2017]. Disponible en: http://www.caracol.com.co/noticias/internacionales/supuestos-yihadistas-pirateandos-portales-de-una-universidad-brasilena/16173/nota/2591949.aspx.

ALZATE CASTAÑEDA, Cristian Camilo y GALEANO VILLA, Jorge Luis. Protocolo de Políticas de Seguridad Para las Universidades de Risaralda. Trabajo de grado Profesional en Ingeniero de Sistemas y Telecomunicaciones. Risaralda.: Universidad Católica de Risaralda. Facultad de ciencias básicas e ingeniería, 2013. 100 p.

ASÓCIAT. “Qué es el phishing y cómo protegerse.”. [En línea]. Mayo 2005. [25 abril de 2017]. Disponible en: http://seguridad.internautas.org/html/451.html.

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-parahurtar-datos-de-su-sistema/.

BERMÚDEZ PENAGOS, Edilberto. Ingeniería Social, un factor de riesgo informático inminente en la universidad cooperativa de Colombia. Trabajo de investigación especialista en seguridad informática. Neiva. Universidad Nacional Abierta ya Distancia. Facultad de educación, 2015. 116 p.

CANDELARIO, Gilberto y González, Hernán. El internet. [En línea]. Internet Insiders. 2009., 4 p. Disponible en: http://teacherweb.com/WQ/MiddleSchool/ElInternet/Phishing4B.pdf.

CASTELLANOS CRESPO, Raquel. Instalación y administración de servicios de correo electrónico. [En línea]. Bogotá: Servicios de red e internet. 2017., 31 p. Disponible en: https://seguridadasir.files.wordpress.com/2012/02/tema_6.pdf.

CAVIEDES FIGUEROA, Viviana Andrea y PEDRAZA GARZÓN, Carmen Lucia. GUÍAS PRÁCTICAS PARA USO DE TÉCNICAS DE INGENIERÍA SOCIAL CON LA HERRAMIENTA SET INCKUIDA EN LA DISTRIBUCIÓN BACKTRACK 4 R2. Tesis De Grado Para Obtener El Título De TECNOLOGO EN REDES Y SEGURIDAD INFORMÁTICA. Colombia.: Corporación Universitaria Minuto de Dios. Facultad de Ingeniería. 2011. 58 p.

Claves para crear contraseñas seguras | ODS Seguridad Informática. ODS | Seguridad Informática. [En línea]. 2017. Disponible en: https://opendatasecurity.io/es/claves-para-crear-contrasenas-seguras/

COLOMBIA, CONGRESO DE LA REPUBLICA. Ley 1273 de 2009. (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. [En línea]. <http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492> [citado en 23 de marzo 2017]

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.

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 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 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.

CONTRERAS, Gerardo “Introducción a la seguridad en internet y aplicaciones”. [En línea]. [13 marzo de 2017] disponible en: (http://www.capacinet.gob.mx/Cursos/Tecnologia%20amiga/desarrolladordesoftware/Seguridad_Internet_SE.pdf).

Editorial, p. (2017). ¿Qué es el Protocolo? Su aplicación Oficial y social. [En línea] Protocolo y Etiqueta. Available at: https://www.protocolo.org/social/etiqueta-social/que-es-el-protocolo-su-aplicacion-oficial-y-social.html [Accessed 4 Nov. 2017].

EL ESPECTADOR. “Anonymous ataca el sitio web de la Universidad de los Andes”. [En línea]. Marzo 2016. [25 abril de 2017]. Disponible en: http://www.elespectador.com/noticias/actualidad/anonymous-ataca-el-sitio-web-de-universidad-de-los-ande-articulo-620617.

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>.

EL ESPECTADOR. “Hackean cuentas de correo de candidatos a rectoría de la Universidad Nacional”. [En línea]. Marzo 2015. [25 abril de 2017]. Disponible en: http://www.elespectador.com/noticias/educacion/hackean-cuentas-de-correo-decandidatos-rectoria-de-uni-articulo-549936.

EL ESPECTADOR. “Universidades, víctimas de “hackers””. [En línea]. Mayo 2015. [25 abril de 2017]. Disponible en: http://www.elespectador.com/noticias/judicial/universidades-victimas-de-hackers-articulo-560884.

El futuro del Malware: Cuidado, Nuevas Tendencias y Ataques - Remove Spyware & Malware with SpyHunter - Enigma Software Group USA LLC. 2017. [En línea]. https://www.enigmasoftware.es/futuro-malware-nuevas-tendencias-ataques/

ENTER. LA INGENIERÍA SOCIAL: EL ATAQUE INFORMÁTICO MÁS PELIGROSO. [En línea]. ENTER.CO. 2016., 7 p. Disponible en: http://www.enter.co/guias/lleva-tu-negocio-a-internet/ingenieria-social/

FANDIÑO SOTO, Libardo. Diseño de un plan de negocio de una empresa de consultoría en servicio al cliente, etiqueta y protocolo empresarial en la ciudad de Bucaramanga y su área metropolitana. Bucaramanga, 2010, 122p. Trabajo de investigación (programa de administración de empresas). Universidad EAN. Facultad de educación. Cundinamarca.

FICARRA, Francisco. “Los virus informáticos: Entre el negocio y el temor”. Revista Latinoamericana de Comunicación CHASQUI. [En línea]. Junio 2002. [25 abril de 2017]. Disponible en: http://www.redalyc.org/articulo.oa?id=16007810.

GARCIA, Alonso y ALEGRE RAMOS. María del Pilar. SEGURIDAD INFORMATICA ED.11 Paraninfo. Madrid: Paraninfo, 2011. 163p. ISBN 8497328124, 9788497328128

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

GONZALEZ AGUDELO, Daniel. El riesgo y la faculta de políticas de seguridad informática una amenaza en las empresas certificadas. Bogotá, 2014, 22p. Trabajo de investigación (administración de la seguridad y salud ocupacional). Universidad Militar Nueva Granada. Facultad de relaciones internacionales, estrategia y seguridad. Cundinamarca.

GONZÁLEZ, Carlos. Programa Integración de Tecnologías a la Docencia. [En línea]. Medellín: Universidad de Antioquia. 2016., 4 p. Disponible en: http://aprendeenlinea.udea.edu.co/lms/moodle/pluginfile.php/99876/mod_resource/content/0/Modulo1/Navegadores.pdf.

Guía para la Implementación de Seguridad de la Información en una MIPYME. [En línea]. Bogotá: MINTIC. 2016., 31 p. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_Guia_Seguridad_informacion_Mypimes.pdf.

HERALDO. “10 consejos para prevenir un ataque informático” [en línea], marzo 2015 [citado el 09 noviembre de 2017]. Disponible en Internet: < http://www.heraldo.es/noticias/comunicacion/2015/03/31/diez_consejos_para_prevenir_ataque_informatico_348654_311.html>.

INSTITUTO COLOMBIANO DE CRÉDITO EDUCATIVO Y ESTUDIOS TÉCNICOS EN EL EXTERIOR. MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN. Bogotá. ICETEX, 2014.

INSTITUTO TECNICO NACIONAL DE COMERCIO. Políticas y Estándares de Seguridad Informática Versión: 01. Cali. INTENALCO, 2011.

INTECO. Política de contraseñas y seguridad de la información. [En línea]. Bogotá: Instituto Nacional de Tecnologías de la Comunicación. 2017., 7 p. Disponible en: https://www.unirioja.es/servicios/si/seguridad/difusion/politica_contrasenas.pdf.

ISO 27000. [En línea]. Bogotá: ISO -International Organization for Standardization. 2011., 14 p. Disponible en: http://www.iso27000.es/download/doc_sgsi_all.pdf.

La seguridad no puede ser una ocurrencia posterior. Web.mit.edu. 2017. [En línea]. Disponible en: http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-isa-es-4/s1-philosophy-security.html

LA TERCERA. “Hackean página web de la Universidad Católica con sitios pornográficos”. [En línea]. Marzo 2012. [25 abril de 2017]. Disponible en: http://www.latercera.com/noticia/nacional/2012/03/680-437360-9-hackean-paginaweb-de-la-universidad-catolica-con-sitios-pornograficos.shtml.

LEGUIZAMON, Mayra. EL PHISHING. España, 2014, 47p. TRABAJO FINAL DE GRADO (GRADO EN CRIMINOLOGIA Y SEGURIDAD). Universidad Jaime I. España.

LÓPEZ VILLA, Oscar y RESTREPO GIL, Wilmar. ANÁLISIS Y DESARROLLO DE ESTRATEGIAS PARA LA PREVENCIÓN DEL USO DE LA INGENIERÍA SOCIAL EN LA SOCIEDAD DE LA INFORMACIÓN. En: Ing. USBMed. Diciembre, 2013. vol. 4, n° 2, p. 16-22.

MIFSUD, Elvira. “Introducción a la seguridad informática”. [En línea]. Marzo 2012. [25 mayo de 2017]. Disponible en: http://recursostic.educacion.es/observatorio/web/ca/software/softwaregeneral/1040-introduccion-a-la-seguridad-informatica?start=1.

PISCITELLI, Emiliano. Ingeniería Social: Cuáles son los tipos de ataque. [En línea]. RedUSERS. 2015., 5 p. Disponible en: http://www.redusers.com/noticias/ingenieria-social-cuales-son-los-tipos-de-ataque/.

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 25 abril de 2017]. Disponible en Internet: http://es.scribd.com/doc/19394749/Ingenieria-social-una-amenaza-informatica>.

RUAY AGUILAR, Marcelo. Documentación Para La Acreditación, Según Norma ISO 17025, Aplicada al Laboratorio LEMCO. Tesis para optar al título de: Ingeniero Constructor. Chile.: Universidad Austral de Chile. Facultad de Ciencias de la Ingeniería Escuela de Construcción Civil. 2006. 110 p.

SANCHEZ ARTEAGA, Juan Miguel. Estudio y análisis del uso de las redes sociales en la ciudad de Cuenca y elaboración de un manual de buenas prácticas de usuario. Cuenca, 2011, 140p. Trabajo de investigación (Ingeniero en sistemas). Universidad Politécnica Salesiana. Facultad de educación. Cuenca.

SHACKLEFORD, Dave. Pruebas de penetración en ingeniería social: cuatro técnicas efectivas. [En línea]. TechTarget. 2012., 4 p. Disponible en: http://searchdatacenter.techtarget.com/es/consejo/Pruebas-de-penetracion-en-ingenieria-social-cuatro-tecnicas-efectivas.

SORIANO, Miguel. Seguridad en redes y seguridad de la información. [En línea]. Bogotá: Improvet. 2017., 80 p. Disponible en: http://improvet.cvut.cz/project/download/C2ES/Seguridad_de_Red_e_Informacion.pdf

TECNOLOGUÍAS PARA EMPRESAS. “INGENIERÍA SOCIAL: EL HACKEO SILENCIOSO”. [En línea]. Marzo 2016. [29 abril de 2017]. Disponible en: http://www.enter.co/guias/tecnoguias-para-empresas/ingenieria-social-el-hackeo-silencioso/.

TEMPERINE, Marcelo. Delitos Informáticos en Latinoamérica: Un estudio de derecho comparado. 1ra. Parte. Buenos Aires, 2013, 12p. Trabajo de investigación (Doctorando en Derecho). Universidad Nacional del Litoral. Facultad de Ciencias Jurídicas y Sociales. Argentina.

TICSCONSULTING. “Ingeniaría Social: explotar por medio de la manipulación y el engaño el eslabón más débil de la cadena de seguridad: factor humano”. [En línea].

Enero 2011. [11 mayo de 2017]. Disponible en: http://www.ticsconsulting.es/blog/generar-claves-seguras-3.

UNIR. “La Ingeniería Social, acercándonos a los molestos Spam, Phishing y Hoax”.
TEMPERINE, Marcelo. Delitos Informáticos en Latinoamérica: Un estudio de derecho comparado. 1ra. Parte. Buenos Aires, 2013, 12p. Trabajo de investigación (Doctorando en Derecho). Universidad Nacional del Litoral. Facultad de Ciencias Jurídicas y Sociales. Argentina.

UNIVERSIDAD DEL VALLE. “Misión” [en línea], 2015 [citado en 25 abril de 2017]. Disponible en Internet: <http://www.univalle.edu.co/la-universidad/acerca-de-univalle/mision>.

UNIVERSIDAD DEL VALLE. “Misión” [en línea], 2015 [citado en 25 abril de 2017]. Disponible en Internet: <http://www.univalle.edu.co/la-universidad/acerca-de-univalle/vision>.

UNIVERSIDAD DEL VALLE. “Misión” [en línea], 2015 [citado en 25 abril de 2017]. Disponible en Internet: <http://www.univalle.edu.co/la-universidad/acerca-de-univalle/organigrama>.

UNIVERSIDAD DEL VALLE. “Misión” [en línea], 2015 [citado en 25 abril de 2017]. Disponible en Internet: <http://www.univalle.edu.co/la-universidad/acerca-de-univalle/ubicacion>.

ANEXOS

ANEXO A. ENCUESTA

ENCUESTA
ENCUESTA SOBRE EL ESTUDIO DE INGENIERIA SOCIAL EN EL USO DE LAS REDES SOCIALES EN LA UNIVERSIDAD DEL VALLE

Con el objetivo de conocer el grado de apropiación del tema de la ingeniería social en el uso de las redes sociales de las personas en la Universidad del Valle, la presente encuesta es para mitigar el riesgo de la información y de los sistemas informáticos.

1. ¿Tienes cuenta en redes sociales?
- ◯ SI
- ◯ NO

Nota: si no tiene cuenta en redes sociales no continuar la encuesta y decir ¿porque?

2. ¿Para qué utilizas las redes sociales?
- ◯ Para estar en contacto con mis amigos
- ◯ Para conocer gente nueva
- ◯ Para contactar con amigos a los que hace tiempo que no veo
- ◯ Otras

3. ¿Cuántos caracteres utilizas en las contraseñas para registrarse en la cuenta en las redes sociales?
- ◯ 5-8
- ◯ 9-12
- ◯ 13-16

4. ¿En qué redes sociales tienes perfil? (Puedes elegir más de una opción)
- ☐ Linkdln
- ☐ Facebook
- ☐ Twitter
- ☐ Instagram
- ☐ Otras

5. ¿Con qué frecuencia utilizas las redes sociales?
- ◯ 1 vez por semana.
- ◯ 2 veces por semana.
- ◯ 3 veces al mes
- ◯ Más de una vez al día.
- ◯ Nunca

6. ¿Usted qué cargo tiene?
- ◯ Empleado.
- ◯ Docente.
- ◯ Estudiante.
- ◯ Invitado.

7. ¿Crees que se pueden correr peligros con las redes sociales?
- ◯ No, no se corre ningún peligro
- ◯ Sí, alguno
- ◯ No estoy seguro/a

8. ¿Sabes qué es Ingeniería Social?
- ◯ SI
- ◯ NO

Nota: si no tiene la respuesta decir ¿Porque?

9. ¿Ha sido víctima de Ingeniería Social?
- ◯ SI
- ◯ NO

10. ¿De los siguientes medios de comunicación, cuál cree usted que es más vulnerable a una amenaza informática?
- ◯ E-mail
- ◯ Redes Sociales
- ◯ Descargas
- ◯ No Tiene idea

ANEXO B AUTORIZACIÓN UNIVERSIDAD DEL VALLE

Santiago de Cali, 28 de abril de 2017

Profesor
Salomón González
Universidad UNAD
Bogotá

Cordial Saludo.

Deseo informar que la señora Claudia Patricia Flórez Ramírez está autorizada para aplicar su encuesta sobre uso de redes sociales en las instalaciones de la Biblioteca Mario Carvajal de la Universidad del Valle de manera personalizada a los usuarios que la frecuentan.

Cordialmente

Fernando Betancur L.
Fernando Betancur López
Director
División de Bibliotecas
Universidad del Valle

ANEXO C EVIDENCIA FOTOGRÁFICA – DILIGENCIAMIENTO DE LA ENCUESTA

Figura 28 Registro fotográfico de la encuesta.

Fuente: Autor

ANEXO D RESUMEN ANALÍTICO EN EDUCACIÓN – RAE

Universidad Nacional Abierta y a Distancia	**FORMATO**
	RESUMEN ANALÍTICO EN EDUCACIÓN - RAE
Código: 001	**Versión: 01**
Fecha de Aprobación: 24-05-2017	**Página 122 de 129**

1. Información General	
Tipo de documento	Trabajo de grado.
Acceso al documento	Universidad Nacional Abierta y a Distancia.
Título del documento	Estudio de Ingeniería Social en el uso de las redes sociales.
Autor(es)	Méndez Collo, Harol y Florez Ramírez, Claudia Patricia
Director	Salomón González, Méndez Collo, Harol.
Publicación	Bogotá, Universidad Nacional Abierta y a Distancia, 2017. 105 p.
Unidad Patrocinante	Ninguna
Palabras Claves	Ingeniería Social, Hacker, Virus, Phishing, Malware,

2. Descripción
El presente trabajo de grado para optar al titulo de Especialista en Seguridad Informática tiene como objetivo realizar un estudio sobre ingeniería social, en el uso de las redes sociales, aplicando metodologías, técnicas, para obtener el estado de vulnerabilidad de las personas en la sede de la universidad del valle.
3. Fuentes
37 fuentes bibliográficas entre libros, artículos, revistas, tesis, portales y consultas a páginas gubernamentales.
4. Contenidos
El objetivo de este proyecto es buscar la manera de identificar todas las debilidades en cuanto a la seguridad de la información dentro de la Universidad del valle, todo esto relacionado con la Ingeniería Social y así mismo determinando cuáles son las técnicas de los ataque aplicables, al personal administrativo, a las zonas físicas y/o dependencias en los sistemas de información. Para ello debemos utilizar las técnicas de recolección de datos como son la observación, encuestas y entrevistas. Al final de este proyecto, contamos con la información ya analizada y tabulada, se realizaran las conclusiones acordes a los hallazgos de la investigación y se generan un conjunto de recomendaciones para que así mismo se busquen corregir todas las fallas encontradas y poder aumentar la seguridad de la información en la Universidad del Valle, planeando en si mismo una cultura de protección de la

información y de buenas prácticas de usuario en el recurso humano de la universidad.

Con este tipo de investigación pretendemos obtener el buen uso de las redes sociales para llevar a cabo un gran objetivo planteado dentro de la institución, y así mismo realizando énfasis en las estrategias de ataque perteneciente de la ingeniería social y poder determinar las vulnerabilidades y riesgos existentes en la Universidad del Valle, con el fin de deducir recomendaciones en pro de la seguridad de la información y poder garantizar su disponibilidad, confidencialidad e integridad.

El presente proyecto hace referencia al tema de seguridad social y el impacto que se tienen los delitos informáticos y el porque hoy en día son muchas las personas que se comunican, en la parte específica sobre el uso de las redes sociales . Su objetivo es de engañar a los usuarios para obtener su información, con el fin de conseguir algún tipo de beneficio, poder ser económico, político o religioso.

Actualmente se logró poder identificar que la principal causa de las vulnerabilidades a la información son las grandes empresas, públicas o privadas, que era el recurso humano y no los recursos tecnológicos, como se pensó en su momento. Actualmente las empresas en el mundo no son ajenas a las fallas de seguridad por lo tanto sus empleados pueden causar, lo que se condensa en una falta de cultura alrededor de la información. Para ello se debe tener en cuenta lo mas importante que es 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.

Los resultados de esta información pueden ser útiles para que en el futuro cercano se logre implementar y puedan dar apoyo a la población seleccionada, y puedan ayudar a resolver algunos de los problemas de ingeniería social que presenten en las universidades.

Mostrando el avance acerca del pasado en el desarrollo de la seguridad de la información, “se dice que es el primer ataque informático en la historia y la cuál se produjo un día viernes 13 del año de 1989. Este proceso se visualizó en una revista especializada donde regalaba disquetes promocionales, los cuales resultaron infectados por aquel virus que afectó a decenas de las empresas y particulares” . Al tiempo, se visualiza el nombre llamado “nace el virus "Dark avenger" que es causado por un daño lento en el sistema operativo, y que a su vez en ese mismo año, la IBM comercializa el primer programa antivirus” por el cual es distribuido en el mercado, y lo que se puso en una perspectiva de un panorama que prometía generar grandes ganancias. El de la protección de la información.

La ingeniería social ha adquirió relevante importancia a pesar de que su existencia es desde hace muchísimo tiempo atrás. Es una conversación tan trivial y tan simple en el echo de sacar la información a una amistad (edad y fecha del cumpleaños por ejemplo) o a un profesor las posibles preguntas de una examen final son formas "básicas" que se de hacer ingeniería social. Por qué el único objetivo es obtener

información valiosa, el ingeniero social realiza esta técnica para obtener la información de las personas sin que se dé cuenta que ha sido una victima de un delito informático.

El activo es una parte más importante en las organizaciones empresariales son la información, en la cual es donde se toman todas las precauciones necesarias, para mantener y preservar esta dicha información, y sus políticas de seguridad que han venido desarrollando y evolucionando con su modelo de seguridad de la información la cual es soportada en tres pilares fundamentales que son confidencialidad, integridad y disponibilidad; teniendo en cuenta las buenas prácticas en cuanto al tipo de gestión y administración en las Tecnologías de la Información.

Una buena política de seguridad se debe en el aseguramiento que se tiene en cuanto al acceso a la información sólo pueda realizarse por aquellos que tengan permiso de acceso a los datos, y contar con unas buenas herramientas de control para los mismos y poseer la identificación correspondiente.

La mejor herramienta para protegerse de los ataques de ingeniería social es el sentido común.

El ser humano es 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 se basan en su funcionamiento u objetivo comercial en sus trabajadores, es un factor que a su vez es el de mayor abandono o rezago frente a los temas de seguridad informática.

El tipo de proceso en el cual se obtiene en el desarrollo de las leyes y las normativas legales que son aquellas que se tipifiquen y penalicen los delitos informáticos como una de las actividades que ha venido creciendo en países tales como Colombia en Latinoamérica. La ley del Código Penal colombiano tiene como el Título denominado "De la Protección de la información y de los datos" esto es relacionado como la cual se divide en dos capítulos, a saber: “De los atentados contra la confidencialidad, la integridad, la disponibilidad de los datos y de los sistemas informáticos” y “De los atentados informáticos y otras infracciones”.

En Colombia, también se relaciona solo hasta el 2009 la cualmse viene a tratar con la rigurosidad en el tema de la seguridad de la información con el nacimiento de la Ley 1273 de 2009, "Por este medio se modifica el Código Penal, y 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 son utilizados dentro de las tecnologías de la información y de las comunicaciones, entre otras disposiciones.

5.Metodología

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, y cuya temática es la Auditoria de Sistemas. A través de esta investigación se pretende determinar cuáles son las vulnerabilidades 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. 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 las redes sociales. Para esto se realizara una estadística de las encuestas acerca de la ingeniería social para la Universidad.

En función de los objetivos definidos en el presente estudio, donde se plantea el estudio de la ingeniería social en el uso de las redes sociales de las personas en la sede de la universidad del valle, se emplearon como técnica común y característica de este nivel de investigación, la encuesta, el cual será orientado de manera esencial para alcanzar los fines propuestos en el presente trabajo de investigación.

6.Conclusiones

Con el desarrollo de esta labor investigativa se logró visibilizar las vulnerabilidades encontradas, no solo a través de la observación y la experiencia, sino también, con los resultados de la encuesta, para sus respectivas estadísticas.

La Universidad se ingresa fácilmente a los distintas áreas y de igualmente a las oficinas de cada edificio y pasan por las zonas restringidas dentro de ellas. Muchas de las dependencias tiene fallas de diseño y organización, la cual permite que los usuarios tengan alcance a documentos y equipos de cómputo.

La universidad no cuenta con controles estrictos que administren el contenido en internet.

La universidad no se encuentra preparada para enfrentar la materialización de alguna de las amenazas encontradas.

Elaborado por:	Harol Méndez Collo y Claudia Florez
Revisado por:	

Fecha de elaboración del Resumen:	24	05	2017

ANEXO E DIVULGACIÓN DEL PROYECTO.

PROCESOS DE ANÁLISIS DE DIVULGACIÓN DEL PROYECTO

COMPROMISO DE LAS DIRECTIVAS

Facilitar la divulgación de un manual para todos los funcionarios de la entidad.

POLÍTICA DE ESTRUCTURA ORGANIZACIONAL DE SEGURIDAD DE LA INFORMACION

Las Directivas son aquellas que se encargan de facilitar la divulgación en el proceso de las Políticas de Seguridad y de dicha Información de todos los funcionarios de una entidad y de todo el personal provisto por terceras partes.

LA UTILIZACIÓN DE LAS NORMAS PARA USO DE DISPOSITIVOS MÓVILES

Esta Dirección Tecnologica es aquella en la cual se debe configurar la opción de borrado remoto la cual permite que la información en los dispositivos móviles institucionales, desarrollen con el fin de eliminar los datos de dichos dispositivos y restaurarlos de la mejor forma dentro de los valores de fábrica, ya sea de forma remota, para así mismo poder evitar dicha divulgación que no sea autorizada de información en caso de pérdida o hurto. [121]

[121] INSTITUTO COLOMBIANO DE CRÉDITO EDUCATIVO Y ESTUDIOS TÉCNICOS EN EL EXTERIOR. MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN. Bogotá. ICETEX, 2014.

LAS NORMAS PARA LA CLASIFICACIÓN Y MANEJO DE LA INFORMACIÓN

Todo tipo de usuarios se deben acatar los procesos de lineamientos de una guía de clasificación de la Información para llevar acabo el proceso del acceso, divulgación, almacenamiento, copia, transmisión, etiquetado y eliminación de la información que hacen parte del contenido de los recursos tecnológicos, así como de la información física de la institución.

Los diferentes tipos de usuarios deben llevar a cabo un proceso de consideraciones para llevar a cabo cuando se trata de lo que se impriman, escaneen, saquen copias y envíe fases tales como verificar las áreas adyacentes a impresoras, los escáneres, las fotocopiadoras y el tipo de máquinas de fax para asegurarse que no quedaron documentos de tipo relacionados o adicionales; para asi mismo, recoger las impresiones inmediatamente y los documentos confidenciales para evitar su divulgación no autorizada.

LAS POLÍTICA DE PROTECCIÓN FRENTE A SOFTWARE MALICIOSO

Tenemos que proporcionar los mecanismos necesarios para garantizar este tipo de protección de la información y de los recursos de la plataforma tecnológica en la cual se procesa y almacena, adoptando los controles necesarios para poder evitar este tipo de la divulgación, modificación o daño permanente que son ocasionados por el contagio y de aquel software malicioso. Además, proporcionará los mecanismos para generar un tipo de cultura dentro de la seguridad entre sus funcionarios y el personal provisto por terceras partes frente a los ataques de software malicioso

LAS NORMAS DE INTERCAMBIO DE INFORMACIÓN

El Grupo de Contratación es aquel que se hace parte donde se debe establecer en los tipos de contratos donde se establezcan con terceras partes, los Acuerdos de Confidencialidad o Acuerdos de intercambio dejando explícitas las responsabilidades y obligaciones legales asignadas a dichos terceros por la divulgación no autorizada de dicha información en beneficiarios del instituto o de los que han sido entregados en razón del cumplimiento de los objetivos misionales en la institución

Los propietarios de los activos de esta información se deben velar porque este tipo de información dentro de sus beneficiarios sera protegida por la divulgación no autorizada que es parte de los terceros a quienes se entrega en esta dicha información, verificando el cumplimiento de las clausulas relacionadas en los tipos de contratos, Acuerdos de confidencialidad o Acuerdos de intercambio establecidos

El proceso de la Coordinación de correspondencia es la que se debe acoger el procedimiento para el intercambio, de dicha información tales como son: (medios de almacenamiento y documentos) con terceras partes y la adopción de los tipos de controles a fin de proteger diche información sensible contra divulgación, pérdida o modificaciones.

El proceso de la Dirección de Tecnología se debe ofrecer servicios o herramientas de intercambio de la información, así como adoptar controles como el cifrado de dicha información, la cual permiten el cumplimiento dentro del procedimiento para el intercambio de dicha información tales como (digital o medio magnético), con el fin de proteger dicha información contra divulgación o modificaciones no autorizadas.

LA POLÍTICA DE INCLUSION DE CONDICIONES DE SEGURIDAD EN LA RELACIÓN CON TERCERAS PARTES

Los funcionarios son aquellos responsables de la realización y/o firma de este tipo de contratos o convenios con terceras que foman parte de lo que se aseguran del tipo de divulgación de las políticas, normas y procedimientos de seguridad de la información a dichas partes.

LAS NORMAS PARA EL REPORTE Y TRATAMIENTO DE INCIDENTES DE SEGURIDAD

En el caso de conocer la pérdida o divulgación no autorizada de dicha información clasificada es desarrollada como el uso interno, reservado o restringido, de los funcionarios en la cual se deben notificarlo a la Oficina de Riesgo para que se registre y se le dé el trámite necesario para cada proceso.

La Dirección de Tecnología se debe implantar con dichos controles necesarios para llevar a cabo una protección de dicha información personal de los beneficiarios, funcionarios, proveedores u otras terceras partes almacenada dentro de las bases de datos o cualquier tipo de repositorio y así mismo poder evitar su divulgación, alteración o eliminación sin la autorización requerida.