MÉTODOS DE ATAQUES Y PREVENCIÓN DE LA INGENIERÍA SOCIAL EN LAS ALCALDÍAS DEL HUILA EN COLOMBIA

FABIO ALEXANDER VEGA SÁNCHEZ
WILSON SUÁREZ LIZCANO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
NEIVA
2018

MÉTODOS DE ATAQUES Y PREVENCIÓN DE LA INGENIERÍA SOCIAL EN LAS ALCALDÍAS DEL HUILA EN COLOMBIA

FABIO ALEXANDER VEGA SÁNCHEZ
WILSON SUÁREZ LIZCANO

Proyecto para optar por el título de Especialistas en Seguridad Informática

Director de Proyecto
MARTÍN CAMILO CANCELADO RUIZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
NEIVA
2018

Nota de aceptación:

_____

_____

_____

_____

Firma del presidente del jurado

_____

Firma del jurado

_____

Firma del jurado

Neiva, mayo de 2018

DEDICATORIA

Dedicamos este proyecto a Dios quien declaramos nuestro señor y creador, a la Universidad Nacional Abierta y a Distancia - UNAD quien nos ha dado la posibilidad de formarnos como mejores profesionales, a nuestras familias por su apoyo incondicional, a nuestros amigos y personas que nos acompañaron firmemente en el cumplimiento de este proyecto innovador.

AGRADECIMIENTOS

Agradecemos a la Universidad Abierta y a Distancia - UNAD por permitirnos formarnos como mejores profesionales de una manera adaptable a las condiciones laborales, por disponer de un método eficaz de aprendizaje y por mejorar cada vez más la educación en nuestro país. A Dios, quien declaramos nuestro creador, padre y salvador, a familiares y amigos por brindarnos su fiel acompañamiento en todo el proceso de formación.

TABLA DE CONTENIDO

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

INTRODUCCIÓN

El presente trabajo es una investigación descriptiva en donde se va a desarrollar el tema de la Ingeniería Social, sus métodos de ataque, las principales maneras y herramientas para su prevención en el ámbito de las alcaldías del Huila en Colombia.

Como se sabe del tema, no es nuevo y ya lleva mucho tiempo hablándose del mismo, aun así, las personas siguen cometiendo errores que permiten que se realicen estos delitos, pues la Ingeniería Social es usada con el objetivo de engañar a las víctimas para acceder a información y lograr obtener algún tipo de provecho ya sea social, económico, político o personal.

La información es un activo que es de gran importancia y valor para toda organización, de ahí la importancia de garantizar su integridad, disponibilidad y confidencialidad. Por medio de esta investigación se pretende exponer las vulnerabilidades más comunes en los entornos públicos en este sector del país, y poder generar las recomendaciones necesarias para reducir los riesgos a esta amenaza.

TITULO DEL PROYECTO

MÉTODOS DE ATAQUES Y PREVENCIÓN DE LA INGENIERÍA SOCIAL EN LAS ALCALDÍAS DEL HUILA EN COLOMBIA

1 PROBLEMA DE INVESTIGACIÓN

1.1 DESCRIPCIÓN DEL PROBLEMA

Los humanos por naturaleza son ingenuos, generalmente con buenos motivos y como sociedad necesitan ser capaces de poder confiar en su prójimo. Sin embargo, existen personas que se aprovechan de esta ingenuidad para el beneficio personal, que pueden llegar a manipular psicológicamente a las personas con el fin de obtener información suficiente para para realizar fraudes o tener accesos ilegítimos a sistemas de información, utilizando un amplio repertorio de vectores de ataque, como el phishing, vishing, baiting o mediante la comunicación directa, por mencionar unos pocos. Debido a que las entidades públicas cómo las alcaldías municipales de Colombia están categorizadas por conservar información pública y muchas de carácter confidencial, pueden ser un objeto claro de ataques por la ingeniería social. Los procedimientos para defender o mitigar este tipo de ataques pueden llegar a ser difíciles de implementar, pero son importantes y se deben realizar para evitar nefastas consecuencias que pueden traer pérdidas económicas y de información pública, ya que estas entidades son las que se encargan de administrar los procesos y recursos de los municipios de Colombia. La ingeniería social actualmente se encuentra reconocida como uno de los ataques más peligrosos y silenciosos de la informática, y por ello es necesario que los funcionarios públicos tengan los conocimientos previos y necesarios para mitigar este tipo de ataques contra la información, ya sea desde la parte de la ingeniería de la informática, como de las políticas del gobierno como lo es por ejemplo la estrategia de Gobierno en Línea, que actualmente se está migrando a lo que se denominará “Gobierno Digital” , que incluye unos lineamientos y componentes como el de la “seguridad y privacidad” que define unas políticas modernizadas para garantizar la seguridad de la información dentro de las entidades públicas del estado colombiano.

1.2 FORMULACIÓN DEL PROBLEMA

¿Cómo funciona la Ingeniería Social, cuáles son los métodos comunes más efectivos que se presentan en la actualidad y cómo puede una entidad pública cómo las alcaldías del Huila defenderse contra la misma?

2 OBJETIVOS DEL PROYECTO

2.1 OBJETIVO GENERAL

Investigar los métodos más comunes y eficaces que se practican en la Ingeniería Social, con el fin de dar a conocer a las alcaldías del Huila los métodos apropiados para contrarrestar la amenaza en sus sistemas de Información.

2.2 OBJETIVOS ESPECÍFICOS

- Reconocer la terminología y conceptos relacionados de la ingeniería social.
- Investigar acerca de los antecedentes y hechos relacionados con la Ingeniería Social en Colombia y el mundo.
- Determinar los métodos de la Ingeniería Social y su funcionamiento, especificando los más comunes y efectivos que se utilizan en la actualidad en las alcaldías del Huila.
- Diseñar una serie de métodos funcionales que permita sensibilizar y mitigar el impacto de los ataques de la ingeniería social en las alcaldías del Huila.

3 JUSTIFICACIÓN

La Ingeniería Social aprovecha el aspecto humano de las falencias encontradas en la seguridad de la información para aprovecharse en un sistema. En algunas organizaciones estas cuentan con profesionales altamente capacitados en TI que conforman el equipo técnico para proteger a los sistemas de los ataques a los usuarios finales, los cuales estos no tienen mayores conocimientos sobre los riesgos. En las entidades públicas colombianas generalmente reconocen a las amenazas informáticas como asuntos lógicos en los sistemas informáticos y físicos en la conservación del hardware informático, sin embargo, existe una vulnerabilidad aún con mayores riesgos que proviene principalmente del factor psicológico de las personas, la ingeniería social es una de las amenazas más peligrosas en la informática, partiendo desde el punto de que cualquier persona sin tener los mayores conocimientos en informática, puede realizar ataques que pueden llegar hasta grandes escalas en una organización y ocasionar pérdidas tanto financieras como de información vital.

Desafortunadamente muchas de las entidades colombianas, entre ellas las alcaldías, han descuidado este ámbito de vulnerabilidad y como consecuencia vienen siendo afectadas por esta creciente amenaza que, en el mayor de los casos, no fue improvista o detectada, y que últimamente ha causado alrededor del planeta. Lo que hace aún más preocupante esta amenaza, es que no sólo puede provenir desde el territorio nacional, sino también desde fuentes externas en cualquier parte del mundo. Para la protección contra esta amenaza es necesario implementar las normas y políticas de seguridad dadas en la ingeniería y por el gobierno nacional, lo que es un dato preocupante, ya que según la última medición anual realizada por el gobierno (2016)[1] en cuanto a la implementación de la estrategia de Gobierno en Línea, se encontró que componente de seguridad y privacidad de la información sólo se está cumpliendo el 22% a nivel nacional y 17% a nivel departamental (Huila), lo que revela un muy bajo índice en la implementación de las políticas de seguridad dadas por el Ministerio de las Tecnologías de la Información y las Comunicaciones (MinTIC), quien es el ente superior encargado de las soluciones TIC en el estado colombiano.

El principio fundamental del proyecto es sensibilizar a las entidades públicas especialmente las alcaldías municipales del Huila, a conocer los métodos de ataque y protección actuales de la ingeniería social, para mejorar seguridad de la información dentro de los sistemas de información de las entidades públicas.

[1] Basado en la lectura de: Índice de Gobierno Digital - Nivel Territorial. Disponible en: http://estrategia.gobiernoenli nea.gov.co/623/w3-propertyvalu e-14714.html

4 DELIMITACIÓN Y ALCANCE

En los sistemas de información se distinguen una gran tipología de amenazas informáticas; en el presente proyecto se cubrirán el estudio de las amenazas internas, donde el personal laboral de las alcaldías del Huila estarán directamente involucrados en los ataques ocasionados por la ingeniería social, no se cubrirán las amenazas o riesgos fuera del perímetro de estas entidades y que no tienen como objetivo principal la seguridad interna.

5 METODOLOGÍA DE INVESTIGACIÓN

Lo que se pretende al realizar este proyecto es identificar efectivamente el rol de las alcaldías del Huila frente a la conciencia del complejo entorno de la seguridad informática y la importancia de estos, con el fin de reducir la eficacia de los ataques de ingeniería social y aumentar la seguridad en general en las alcaldías del Huila, por tanto, se enmarca dentro de una investigación descriptiva.

Esta investigación se hará realizando un procedimiento secuencial, usando encuestas, obteniendo la información basados tanto en la revisión de la investigación actual sobre la ingeniería social y amenazas informáticas, como en la observación del comportamiento humano, cuyo objetivo será identificar las vulnerabilidades, consecuencia de las debilidades del comportamiento de los usuarios en las alcaldías del Huila a la hora de tomar decisiones en el uso de la información y contacto directo con su entorno de trabajo, para reducir la posibilidad de que se den ataques de ingeniería social.

5.1 TIPO DE INVESTIGACIÓN

El proyecto se basa en una investigación descriptiva, el cual se enfoca en encontrar y analizar las causas y consecuencias que traen la aparición de la ingeniería social en las alcaldías del Huila, para así mismo determinar los controles y acciones necesarias para mitigar el impacto que éstas han producido en dichas entidades.

Para la aplicación de esta investigación, se utiliza el método causal, un método que comprende el comportamiento, variables e influencias de las causas y efectos de la ingeniería social dentro de las alcaldías del Huila, y que finalmente se utilizará como base principal para establecer métodos de prevención que contribuyan a reducir los riesgos que la ingeniería social puede producir dentro de dichas entidades.

5.2 POBLACIÓN MUESTRA

5.2.1 Población. El proyecto se relacionará y aplicará sobre el sector público específicamente en algunas alcaldías del departamento del Huila, enfocándose principalmente en el área de sistemas y empleados de estas entidades.

5.2.2 Muestra. Para obtener resultados más precisos sobre el estado actual e influencia de la ingeniería social dentro de las alcaldías municipales del Huila, se seleccionarán diez (10) alcaldías de acuerdo a su disposición, y se aplicarán dos (2) encuestas por entidad al personal laboral que incluye contratistas, de plata y/o de carrera administrativa, teniendo en cuenta las dependencias y cargos más cercanos a las áreas de las TIC, sistemas e informática.

Teniendo en cuenta la cantidad de alcaldías seleccionadas y las encuestas a realizar, se obtiene un total de veinte (20) muestras de la siguiente manera.

(10) alcaldías x (2) encuestas = (20) muestras.

Adicionalmente, se tomará un registro fotográfico autorizado sobre las fortalezas y debilidades de la ingeniería social dentro de las entidades.

5.3 TÉCNICAS DE ANÁLISIS Y PROCESAMIENTO DE DATOS

Acorde a la metodología de investigación, se emplearán las siguientes técnicas:
Directas o interactivas: observación y entrevistas cualitativas, utilizando cuestionarios, listas de chequeo, entrevistas personales.
Observación discreta y observación abierta.
Indirectas o no interactivas: pruebas en equipos de cómputo, documentación, procedimientos y procesos.
Con los datos obtenidos para su análisis se hará tabulando y mostrando gráficamente los resultados

5.4 METODOLOGÍA DE DESARROLLO

Para el desarrollo del proyecto y con el fin de lograr alcanzar los objetivos propuestos se ha propuesto una serie de actividades a desarrollar.

Tabla 1. Metodología de desarrollo.

Objetivos	Actividades
• Reconocer la terminología y conceptos relacionados de la ingeniería social.	- Recolectar información de diversas fuentes documentales y por Internet acerca de la Ingeniería Social.
• Investigar acerca de los antecedentes y hechos relacionados con la Ingeniería Social en Colombia y el mundo.	- Indagar en Internet acerca de los hechos que se han presentado más relevantes en Colombia y el mundo de Ingeniería Social.
• Determinar los métodos de la Ingeniería Social y su funcionamiento, especificando los más comunes y efectivos que se utilizan en la actualidad en las alcaldías del Huila.	- Investigar en diversas fuentes documentales e Internet acerca de los diversos tipos de ataques que usa la Ingeniería Social y verificar en las alcaldías del Huila por medio de la realización de encuestas cuáles podrían y se han presentado hasta el momento.
• Diseñar una serie de métodos funcionales que permita sensibilizar y mitigar el impacto de los ataques de la ingeniería social en las alcaldías del Huila.	- Generar un documento que señale los distintos controles que se recomiendan implementar en las alcaldías del Huila y que podrían mitigar los riesgos por ataques de Ingeniería Social.

Fuente: el autor.

6 MARCO REFERENCIAL

6.1 ESTADO DEL ARTE

En años anteriores, los ataques informáticos eran ataques individuales de gran penetración y en tantos sistemas como fuera posible y causar el mayor daño posible, no tenían objetivos específicos, pero en los últimos años los ataques se han vuelto complejos y contra usuarios específicos, estos ataques utilizan varias técnicas de ataque diferentes para evitar ser detectados por los actuales sistemas de protección. Las organizaciones que utilizan sistemas de protección están en riesgo de ser atacadas por métodos modernos de *malware*.

El código malicioso utilizado en los ataques modernos tiene consecuencias más devastadoras que las que se tenían con gusanos y virus de la década anterior. Muchos sistemas de protección existentes están inadecuadamente preparados para detener nuevas formas de código malicioso. Los *hackers* reconocieron la debilidad de una defensa con vulnerabilidades nuevas y comenzaron a desarrollar un nuevo ataque.

Uno de los primeros autores que hablan acerca de la Ingeniería Social fue *Harl's* (1997), quien plantea situaciones, métodos, persuasión e implicaciones de esta nueva forma utilizada por los hackers en esa época.[2]

Una característica importante de los ataques modernos es que se centran en el eslabón más débil en la cadena de seguridad, los seres humanos. Como sugieren los autores *K. Mitnick* y *W. Simon* "*Los ataques de Ingeniería Social pueden tener éxito cuando la gente es estúpida o, más comúnmente, simplemente ignorante acerca de las buenas prácticas de seguridad*"[3]. Tal vez este libro y lo que sus autores abordan sea difícil pasar por alto el enorme impacto que han tenido en este tema, y poco se escribe que no esté en cierta medida mencionado en este libro, aunque hoy en día se pueden encontrar miles de fuentes de información sobre la Ingeniería Social[4].

Los ataques de los ingenieros sociales están dirigidos principalmente a las personas por esto la psicología tiene mucho que ver en la forma como se pueden

[2] Harl 1997. People Hacking: The Psychology of Social Engineering.
[3] Tomado textualmente de: Mitnick, Kevin D., Simon, William L. The Art of Deception: Controlling the Human Element of Security. John Wiley & Sons, 2002.
[4] Basado en la lectura de: Nohlberg, Marcus. Securing Information Assets: Understanding, Measuring and Protecting against Social Engineering Attacks.2008.

persuadir a los usuarios de sistemas informáticos, el autor *Robert B. Cialdini* escribió un libro que investiga acerca de estos comportamientos[5].

Otros autores como *Markus Huber* (2008) presentan una investigación de la ingeniería social evaluando la comprensión, medición y protección. Se enfoca en saber más acerca de lo que es la ingeniería social, y cómo funciona, a través del estudio de los anteriores trabajos de seguridad de la información[6].

Daniel Siegel (2009) hace un estudio sobre las nuevas vulnerabilidades de las redes sociales, que pueden ser explotadas por la ingeniería social. Las redes sociales están muy extendidas para uso privado, así como se utilizan a menudo en cualquier entorno empresarial. Dado que la naturaleza de dicha red social es la distribución de los datos, inevitablemente, plantea la cuestión de si pueden ser objeto de ataque de este tipo[7].

Un libro que toca el tema de la herramienta de auditoria en la ingeniería social y como reducir las vulnerabilidades es *Advances in Communications, Computing, Networks and Security* de los autores *Paul Dowland, Steven Furnell* (2009), ellos hicieron varios experimentos y plantean puntos a tener en cuenta en las auditorias acerca de este tipo de ataque.[8]

El phishing ha sido una de las principales tácticas de ingeniería social empleadas para obtener información personal a través de correo electrónico. De acuerdo con *Dean* (2010), el *phishing* es "*una práctica en la que una persona intenta recopilar información de acceso o autenticación haciéndose pasar por alguien que necesita esa información*"[9].

Más recientemente los autores *Christopher Hadnagy, Michele Fincher* (2015) se refieren al *phishing* desde el punto de vista de la toma de decisiones humanas y el impacto de la influencia deliberada y manipulación en el receptor. Dan una idea del espionaje financiero corporativo y los objetivos de robo de identidad de los atacantes[10].

Otra autora *Sharon Conheady* (2014) se ha centrado en la planificación de pruebas, el reconocimiento y desarrollo de escenarios y los resultados obtenidos

[5] Basado en la lectura de: Cialdini, Robert. Influence, the psychology of persuasion. 2001
[6] Huber, Markus. Measuring Readiness against Automated Social Engineering. 2008.
[7] Siegel, Daniel. On the New Threats of Social Engineering Exploiting Social Networks. 2009.
[8] Paul Dowland, Steven Furnell. Advances in Communications, Computing, Networks and Security. Lulu.com, 2009.
[9] Copiado textualmente de: Tamara, Dean. Network+ Guide to Networks.2009 P. 621.
[10] Hadnagy, Christopher. Fincher, Michele. Phishing Dark Waters: The Offensive and Defensive Sides of Malicious Emails.2015.

de ataques de Ingeniería Social. Todo esto con el fin de proponer algunas medidas que pueden tomarse para defenderse de este tipo de ataques. Igualmente aborda el impacto de las tecnologías nuevas y emergentes sobre las tendencias futuras de la Ingeniería Social[11].

En el contexto latinoamericano también se han hecho diversas investigaciones y estudios acerca de la Ingeniería Social.

Sergio Arcos Sebastián (2011) en su tesis para la Universidad Politécnica de Catalunya presenta varios ejemplos de ataque a sistemas informáticos y concientizar a las personas sobre los diferentes riesgos que se presentan[12].

Diego *González Juárez* y *José Peña Enríquez* de la Universidad Nacional Autónoma de México, indagan acerca del *Phishing* y el panorama que se tenía en ese momento, así como las leyes de protección de datos de su país[13].

Hay una tesis muy interesante de los autores *Geovanna Hernández Flores y José Urrutia Franco*, quienes analizan el conocimiento que tienen en la facultad de ciencias administrativas de la universidad de Guayaquil, frente al posible uso de técnicas de ataques utilizando la Ingeniería social[14].

Ahora bien, en Colombia el tema de la Ingeniería social no es ajeno a las empresas ni a los usuarios domésticos. En varios medios de comunicación se viene hablando del tema desde hace algunos años.

Édgar Medina de la sección Tecnósfera publicó un artículo referente a la Ingeniería Social, y expone acerca de los delincuentes que se enfocan usando técnicas y métodos para cometer delitos en nuestro país[15].

En cuanto a algunos trabajos y tesis se tiene a las autoras *Natalia Salazar y Marcela González* (2007) quienes se enfocan en el *Phishing* y como ha afectado a usuarios de entidades financieras, esto lo hacen abordando los distintos ataques

[11] Conheady, Sharon. Social Engineering in IT Security: Tools, Tactics, and Techniques: Testing Tools, Tactics & Techniques. McGraw Hill Professional, 2014.
[12] Sergio Arcos Sebastián. Ingeniería social: Psicología aplicada a la seguridad informática.2011
[13] Diego Dante González Juárez, José Antonio Peña Enríquez. Estudio del impacto de la Ingeniería Social – Phishing. 2012
[14] Hernández Flores Geovanna Belén, Urrutia Franco José Gregorio. Ingeniería Social a través de medios informáticos, análisis de las posibles amenazas existentes en la facultad de ciencias administrativas de la Universidad de Guayaquil. 2015.
[15] MEDINA, Edgar. Ingeniería social, la razón del éxito de los ladrones digitales. 29 de junio de 2015. Articulo disponible en: http://www.eltiempo.com/archivo/documento/CMS-16020156

que se han presentado con algunas entidades financieras del país y como se efectuó el mismo, al final producen algunas recomendaciones para no ser víctimas de los mismos[16].

6.2 MARCO TEÓRICO

La ingeniería social (*Social Engineering SE*) a lo largo del tiempo ha dado lugar a diversas opiniones acerca de lo que significa y la manera cómo esta técnica funciona. No se trata sólo del hecho de simplemente mentir para estafar o cometer un fraude, también se refiere a las herramientas utilizadas por los delincuentes para cometer estos actos delictivos. Esta es una ciencia algo más compleja, cuyas teorías se pueden dividir en partes o ecuaciones para poder ser estudiadas.

La ingeniería social es utilizada todos los días por casi todas las personas en situaciones cotidianas. Por ejemplo, un empleado que no se siente bien pago y que busca un aumento está utilizando la ingeniería social, la manera en que los niños hacen que sus padres cedan a sus caprichos, la manera en que los maestros interactúan con sus estudiantes, en la forma en que médicos, abogados o psicólogos obtienen información de sus pacientes o clientes. Definitivamente se utiliza en muchas interacciones humanas, la mayoría de las veces sin fines delincuenciales.

La ingeniería social por supuesto también se da en otros ambientes cómo en el gobierno, el comercio, en la grande y pequeña empresa. Desafortunadamente, también está presente cuando los delincuentes, estafadores y similares engañan a las personas para que les den información que las haga vulnerables a los crímenes. Como cualquier herramienta, la ingeniería social se puede decir que no es buena ni mala, simplemente es una herramienta que tiene usos diferentes.

Se tienen dos palabras ingeniería que significa "*Arte y técnica de aplicar los conocimientos científicos a la invención, diseño, perfeccionamiento y manejo de nuevos procedimientos en la industria y otros campos de aplicación científicos*". Y social "*Que está relacionado con las actividades que se llevan a cabo como miembros de la sociedad*".[17] Combinando esas dos definiciones se puede observar que la ingeniería social es entonces, el arte o la ciencia cuya principal habilidad consiste en manipular a los seres humanos para que actúen de alguna manera en algún aspecto de sus vidas o trabajos.

[16] Natalia Salazar, Marcela González. "Phishing": La Automatización de la Ingeniería Social. Octubre de 2007.
[17] Tomado textualmente de: https://es.oxforddictionaries.com/definicion

Ahora bien, en términos informáticos la ingeniería social es el método utilizado por una persona externa a una organización para robar información por ejemplo el engaño a empleados, generalmente el atacante pretende ser una persona legítima con algún tipo de autoridad para solicitar la información. El atacante de ingeniería social usualmente usa esta información de privilegios para acceder a un sistema informático o base de datos para modificar, alterar o robar información confidencial.

Un ingeniero social, básicamente, utiliza medios cómo el teléfono o Internet para engañar a la gente y hacer que estos revelen información sensible quebrantando las políticas de seguridad. Usando este método, los ingenieros sociales aprovechan la tendencia humana de confiar en la gente. El principio usado por la ingeniería social es basarse en aprovecharse del eslabón más débil en los mecanismos de seguridad, los seres humanos.

Un ejemplo de un ataque de ingeniería social que se presenta en la actualidad es mediante archivos adjuntos de tipo malicioso en correos electrónicos, a pesar que existen recomendaciones y los usuarios ya tienen conocimiento al respecto, abren estos adjuntos sin detenerse a analizar el riesgo que se está corriendo. Estos archivos podrían iniciar ataques de correos electrónicos masivos de spam o instalar código malicioso en los equipos y propagarse por la red corporativa.

Cuando se habla de ataques el más sencillo y que ocurre comúnmente que consiste en engañar a un usuario haciéndole creer que el atacante es por ejemplo es el administrador del sistema y que por medio del comunicado le solicita la contraseña al usuario para un determinado suceso de índole técnico. Igualmente se presentan casos a menudo donde por medio de correos electrónicos solicitan contraseñas de tarjetas de crédito para para un procedimiento como activar una cuenta existente porque fue bloqueada y debe realizar este desbloqueo facilitando estos datos.

Los usuarios deben tener claro que tanto los administradores de sistemas como las entidades financieras raramente o nunca requieren información confidencial, como las contraseñas, para realizar procedimientos técnicos.

Debido a todas estas vulnerabilidades la mejor opción que tienen las organizaciones para mejorar y reducir este tipo de riesgos es capacitar a los empleados y usuarios acerca de los diferentes métodos de ataques que utilizan los cibercriminales usando la Ingeniería Social, y logren proteger mejor su privacidad y su información, mejorando y aplicando las políticas de seguridad.

Uno de los ingenieros sociales más famosos es *Kevin Mitnick*, según él, "*La ingeniería social se basa en la falsedad y la ingenuidad de los usuarios comunes*"[18]. Definitivamente realizar un ataque mediante la Ingeniería Social es mucho más económico y efectivo, pues explota a las personas, que son susceptibles a engaños, sobornos e ingenuidad y no a los medios tecnológicos que son más difíciles de atacar.

6.2.1 Antecedentes de la Ingeniería Social en el mundo. En el mundo hay muchos ejemplos de este tipo de ingeniería social llevada a cabo incluso hace más de un siglo. El caballo de Troya parece ser la historia que todos saben y aún memorable, tanto así que los troyanos hoy en día, fueron llamados así por su similitud de ataque.

También es recordado *Victor Lustig* quien es conocido por haber "vendido" la torre *Eiffel* dos veces haciéndole creer a los comerciantes de chatarra de la época que iba a ser desmantelada.

George Parker otro estafador que logró vender en *New York*, el *Madison Square Garden*, la Estatua de la Libertad y el puente de *Brooklin*, a incautos que supuestamente iban a ganar fortunas con ellos.

Hacia el año de 1920 *Charles Ponzi*, se hizo famoso por estafar a muchas personas con el llamado esquema de *Ponzi*, que no es más que las conocidas pirámides, dónde el captaba recursos de la gente prometiendo ganancias. *Bernie Madoff* utilizó en el año 2009 este mismo esquema, estafando a las personas alrededor de $65.000 millones de dólares.

El mayor robo de bancos conocido en la historia hasta ese momento de los Estados Unidos fue cometido utilizando la Ingeniería Social, *Stanley Mark Rifkin* en el año de 1978, siendo técnico en informática y contratista de un banco de California, logró memorizar los códigos que los empleados usaban para realizar transferencias, luego con una llamada haciéndose pasar por empleado logró transferir $10 millones de dólares.

El hacker más conocido y que ayudó a popularizar la ingeniería social como un término de seguridad de la información, *Kevin David Mitnick*, hacía 1990 había pasado ya 5 años en la cárcel tras utilizar contraseñas y códigos adquiridos a través de la ingeniería social en delitos relacionados con la piratería informática, incluyendo comprometer las computadoras de correo de voz de *Pacific Bell* y

[18] Disponible en: https://nohlberg.files.wordpress.com/2007/03/nohlberg_thesis_smaller.pdf

copiar software propietario de varias compañías de teléfonos celulares y computadoras. Hoy en día hacker de sombrero blanco.

En cuanto a los ataques más reconocidos en los últimos años tenemos:

Estafas BEC (*Business Email Compromise*), en este ataque los estafadores se dirigen al personal de organizaciones medianas y grandes mediante llamadas o mail, pretendiendo ser otro empleado, pero de un nivel más alto.

Brecha de Bit9 el grupo de ciber-espionaje "*Hidden Lynx*" año 2012 en China, accedieron a la infraestructura de Bit9 para firmar ficheros, para que pudieran firmar malware y hacer que éste pareciera legítimo. Luego lo utilizaron para atacar a clientes y organizaciones con Bit9.

Secuestro de *Twitter* de *AP Associated Press*, este ataque comenzó con un correo electrónico de *phishing* que llevó a un empleado inadvertidamente a ceder el acceso a la cuenta de *Twitter* de la agencia de noticias. Los atacantes usaron la cuenta comprometida para mediante un *tweet* informar que había habido explosiones en la Casa Blanca. El ataque tuvo un gran impacto en el mercado de valores, haciendo que el *Dow Jones* cayera 150 puntos.

6.2.2 Antecedentes de la Ingeniería Social en Colombia. En nuestro país al igual que el resto del planeta los casos de ataques mediante ingeniería social abundan y en todos los sectores, políticos, sociales, empresariales, etc. Además, los usuarios de nuestro país, a pesar de estar advertidos y haber asistido a capacitaciones, muchas veces no tiene presente este tipo de ataque como una amenaza real.

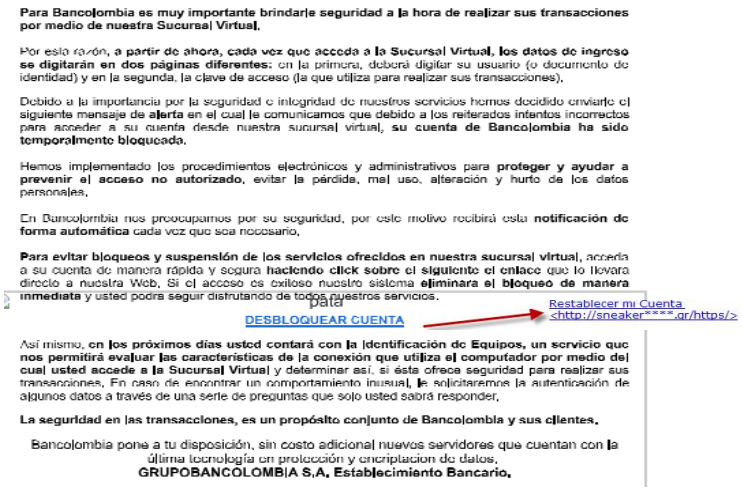
Tal vez un caso muy sonado fue el de la operación JAQUE, que logró la liberación de varios secuestrados entre ellos la excandidata presidencial Ingrid Betancur, el éxito de la operación fue el uso de la Ingeniería social usada por la inteligencia de las fuerzas armadas, quienes lograron interceptar y determinar el modo cómo se comunicaban los guerrilleros, para poder llevar a cabo una suplantación de identidad. Figura 1.

Figura 1. Operación JAQUE.

Fuente: http://www.eltiempo.com/politica/proceso-de-paz/asi-fue-la-operacion-jaque-34151

Los antecedentes de los últimos años parecen tener una tendencia elevada en cuanto a que los atacantes que usan la Ingeniería Social, pues prefieren medios como el correo electrónico para cometer los delitos. El *phishing* en Colombia está dentro de los delitos más recurrentes, los criminales están pendientes de noticias de última hora, como desastres naturales, para lanzar estos ataques logrando que las victimas presten atención e ingresen a *links* que los llevan a sitios que en realidad solo pretenden robar información confidencial, como la financiera.

Figura 2. Email fraudulento Bancolombia.



Para Bancolombia es muy importante brindarle seguridad a la hora de realizar sus transacciones por medio de nuestra Sucursal Virtual.

Por esta razón, **a partir de ahora, cada vez que acceda a la Sucursal Virtual, los datos de ingreso se digitarán en dos páginas diferentes:** en la primera, deberá digitar su usuario (o documento de identidad) y en la segunda, la clave de acceso (la que utiliza para realizar sus transacciones).

Debido a la importancia por la seguridad e integridad de nuestros servicios hemos decidido enviarle el siguiente mensaje de **alerta** en el cual le comunicamos que debido a los reiterados intentos incorrectos para acceder a su cuenta desde nuestra sucursal virtual, **su cuenta de Bancolombia ha sido temporalmente bloqueada.**

Hemos implementado los procedimientos electrónicos y administrativos para **proteger y ayudar a prevenir el acceso no autorizado**, evitar la pérdida, mal uso, alteración y hurto de los datos personales.

En Bancolombia nos preocupamos por su seguridad, por este motivo recibirá esta **notificación de forma automática** cada vez que sea necesario.

Para evitar bloqueos y suspensión de los servicios ofrecidos en nuestra sucursal virtual, acceda a su cuenta de manera rápida y segura **haciendo click sobre el siguiente el enlace** que lo llevara directo a nuestra Web. Si el acceso es exitoso nuestro sistema **eliminara el bloqueo de manera inmediata** y usted podrá seguir disfrutando de todos nuestros servicios.

patel

DESBLOQUEAR CUENTA

Restablecer mi Cuenta
<http://sneaker****.gr/https/>

Así mismo, **en los próximos días usted contará con la identificación de Equipos, un servicio que nos permitirá evaluar las caracteristicas de la conexión que utiliza el computador por medio del cual usted accede a la Sucursal Virtual** y determinar así, si ésta ofrece seguridad para realizar sus transacciones. En caso de encontrar un comportamiento inusual, le solicitaremos la autenticación de algunos datos a través de una serie de preguntas que solo usted sabrá responder.

La seguridad en las transacciones, es un propósito conjunto de Bancolombia y sus clientes.

Bancolombia pone a tu disposición, sin costo adicional nuevos servidores que cuentan con la última tecnología en protección y encriptacion de datos.
GRUPOBANCOLOMBIA S.A. Establecimiento Bancario.

Fuente: mail.yahoo.com

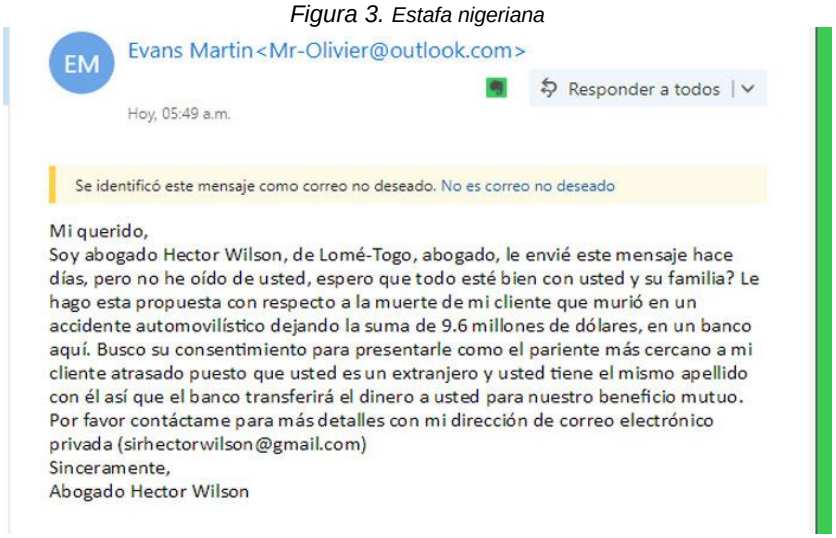
Hace unos meses mediante *phishing*, desde la cuenta *informacion@bancolombia.com.co,* Figura 2. varios usuarios de esa entidad fueron víctimas de fraude pues pensaban que el correo era legítimo, este contenía un link que llevaba a una página del banco que fue muy bien clonada, la cual pedía ingresar los datos para desbloquear la cuenta en una página falsa y de esta manera obtener los datos de los incautos. En este año ya ha habido casos de ataques de Ingeniería social utilizando grabaciones muy parecidas a las que se oyen cuando se llaman a los bancos, este engaño ha permitido a los delincuentes cometer fraudes con los datos obtenidos de sus víctimas.

Entre los casos más sonados también se encuentra el de las pirámides como DMG dónde mucha gente perdió grandes sumas de dinero y sin importar estrato social ni perfiles específicos todos perdieron, su creador David Murcia que desde el año 2005 logró que las personas en la Hormiga, Putumayo confiaran en él, entregando sus ahorros a cambio de excelentes ganancias o bienes. Producto de la Ingeniería Social David Murcia logra captar tanto dinero que se extiende rápidamente por todo el país e incluso otros países vecinos.

En los últimos años con el proceso de paz en la Habana y las elecciones presidenciales también dio mucha controversia el *hacker Andrés Sepúlveda*, quien mediante la Ingeniería Social y usando perfiles falsos logró obtener información de los guerrilleros que negociaban el proceso de paz, con el fin de influenciar sobre los resultados de la campaña política.

Hay otros como el caso de la estafa nigeriana, consiste en un correo que informa que la persona ha sido seleccionada ya sea por el gobierno africano o una empresa petrolera o una lotería e incluso un difunto millonario, para recibir una suma millonaria pero que requieren un número de cuenta y que, al pagar una suma de dinero sustanciosa por comisión, podrá obtener un giro millonario. Figura 3.

Figura 3. Estafa nigeriana



Fuente: https://elruinaversal.com/2017/10/05/el-ruinaversal-se-reune-con-el-abogado-wilson-para-recibir-la-millonaria-herencia-que-le-dejo-un-familiar-desconocido/

Igualmente se han utilizado las redes sociales para difundir noticias como la muerte de artistas famosos y otro tipo de desastres que han causado que las personas incluso no duerman en sus casas por temor a un temblor que podría ocurrir, pero también se usan este tipo de acontecimientos para llevar a las personas a hacer clic a enlaces de páginas dónde se captura información confidencial. De la misma manera estas páginas pueden solicitar el ingreso usando las credenciales de la misma red social, esto hace que el atacante obtenga más información de la víctima y dirigir mejor su ataque.

Desafortunadamente no sólo se prestan las redes sociales para este tipo de delitos también cuando las víctimas son menores de edad y la otra persona finge también ser menor de edad para obtener información o incluso fotos sexuales que después usan para extorsionar a la víctima.

6.3 MARCO CONCEPTUAL

- **Seguridad informática**: es la parte del campo de la informática la cual se encarga de proteger o salvaguardar la información o datos de los usuarios almacenados en un sistema (informático), pero para lograr esta seguridad en necesario seguir unas normas, leyes estándares y así minimizar el riesgo, además de esto hay dos clases de seguridad ya sea seguridad de software y seguridad de hardware, todo esto siempre con el propósito de salvaguardar la información datos del usuario.

- **Seguridad de la información**: son un grupo de normas o leyes que se utilizan para custodiar la información manteniéndola en secreto no solo en el campo informático sino en cualquier campo ya que la información no solo está disponible en este medio.

- **Seguridad física**: consiste en crear obstáculos físicos como medidas de prevención y protección contra amenazas que afecten la integridad de la información o cualquier recurso del sistema.

- **Seguridad tecnológica**: son el conjunto de normas y leyes establecidas que nos conceden proteger o salvaguardar la información o datos en un sistema, además de esto se deben utilizar una serie de software o programas para mejorar esta seguridad.

- **Integridad**: Es tener la certeza que la información es veraz, segura y confiable, garantizando que este completa, que tenga todas sus partes tal y como fue guardada inicialmente, sin ninguna clase de modificación o alteración sin permisos autorizados.

- **Confidencialidad**: garantiza que la información sea segura que no sea vista o utilizada por terceros no autorizados para no correr el riesgo que la información sea divulgada o utilizada para fines ajenos a nuestra voluntad.

- **Disponibilidad**: garantiza que puede acceder a la información cuando la necesiten los usuarios, a través de los canales adecuados siguiendo los procesos correctos[19].

- **Spyware**: Son aplicaciones informáticas que recopilan información mediante el seguimiento de las preferencias y comportamientos de los usuarios durante la navegación en Internet. Estos datos se envían posteriormente a desarrolladores de software de terceros para diferentes propósitos legítimos o ilegítimos.

- **Phishing**: puede ser descrito como un intento de adquirir fraudulentamente Información personal, como información de la tarjeta de crédito o contraseñas pretendiendo ser un empleado legítimo o una persona de más rango o autoridad. El ataque mediante phishing es generalmente iniciado a través de correo electrónico, llamadas telefónicas (*vishing*) o mensajería instantánea.

[19] Basado en la lectura de: Seguridad y privacidad de la información. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G3_Procedimiento_de_Seguridad.pdf

- **Spam**: es el correo no deseado, enviado por el atacante que pretende lograr el colapso de servicios, además pueden contener código malicioso para hacer un ataque tipo phishing o virus informático.

- **Hackers:** son personas apasionadas por el conocimiento de la tecnología, por ejemplo, expertas en electrónica, sistemas operativos, lenguajes de programación y arquitecturas de red que utilizan sus habilidades y capacidades de descubrir vulnerabilidades en las redes y sistemas de información, planteándose metas y retos para lograr un objetivo que es violar la seguridad impuesta en cualquier sistema.

- **Crackers**: sus intenciones son en sí las de acceder y dañar los sistemas informáticos hurtando modificando o robando la información. Tienen motivaciones las cuales van desde las económicas hasta las políticas.

- **Phreakers**: son atacantes, que orientan sus acciones más hacia las comunicaciones telefónicas, para lograr llamadas gratis o para ir superando sus mejores intrusiones.

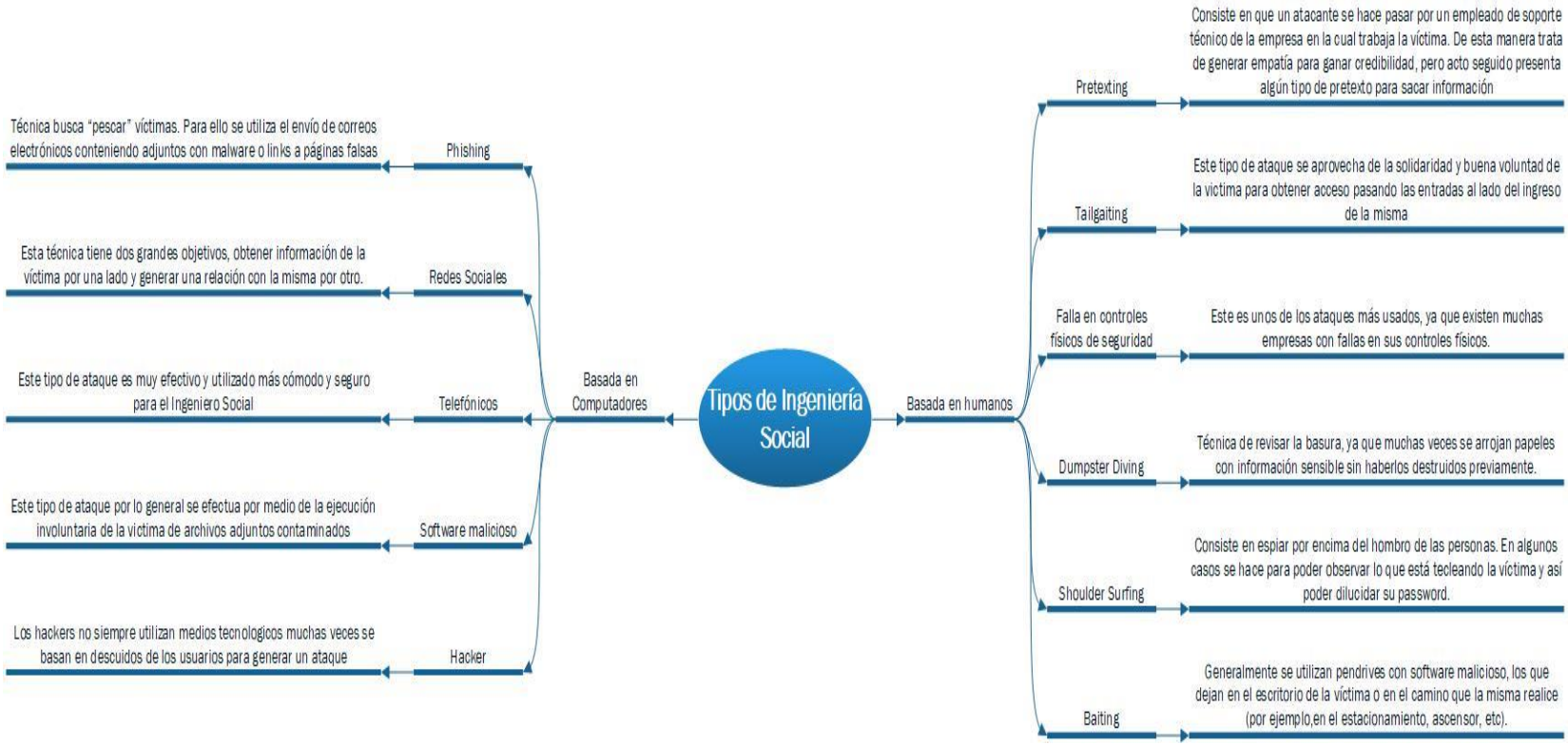
- **Espías**: son expertos en la aplicación de la Ingeniería Social, asumen diferentes roles con suficiente credibilidad para poder engañar a sus víctimas.

- **Ingeniero Social**: Este es el perfil de atacante que es de mayor interés para esta investigación, al tipificar las diferentes conductas que pueden ejecutar durante un ataque de Ingeniería Social.

- **Tipos de ingeniería social**: en la figura 4 se presenta un esquema de cada tipo de ingeniería social y su definición.[20]

[20] Las definiciones se basaron en la lectura de: Glossary of cyber security terms. Disponible en: https://www.bsigroup.com/en-GB/Cyber-Security/Cyber-security-for-SMEs/Glossary-of-cyber-security-terms/

Figura 4. Tipos de Ingeniería Social.



Fuente: el autor.

- **Pentesters**: son *hackers* que usan sus conocimientos y habilidades al ejecutar pruebas de penetración a los sistemas de organizaciones que los contratan y los supervisan, mediante el uso de herramientas para hallar las vulnerabilidades y brindar una solución.

- **Ladrones de identidad**: se basan en la suplantación de identidades para poder realizar transacciones comerciales y en la personificación usando ropa o uniformes para lograr ingresar a diferentes sitios. Utilizan técnicas como buscar en la basura para obtener ilegalmente información personal de sus víctimas, para luego hacer uso indebido de la misma.

- **Empleados descontentos**: suelen pasar desapercibidos pues manejan un bajo perfil, para no demostrar sus intenciones y no perder su trabajo, hasta lograr sus cometidos, entonces se convierten en ingenieros sociales para poder cometer delitos como robo de información, suplantación, espionaje y venta de información sensible de la organización donde se encuentran a la competencia.

- **Estafadores**: estos delincuentes engañan a las personas con el fin de sacar un beneficio económico aprovechándose de las necesidades de las personas y también de organizaciones. A diario en Colombia se conocen noticias como el caso de InterBolsa o las famosas pirámides.

- **Reclutadores**: se valen de técnicas basadas en engaños para persuadir a sus víctimas, a fin de apoderarse de ellos.

- **Vendedores**: Obtienen la información de diferentes fuentes con el fin de brindar soluciones a las necesidades de los posibles consumidores y lograr de esta manera la confianza de los mismos.

- **Gobierno**: los representantes de los gobiernos y los políticos tienen cualidades de un ingeniero social; carismáticos, seguros, asertivos que tienen el poder para desviar la atención como el de crear cortinas de humo sobre temas importantes.

- **Doctores, psicólogos y abogados**: estos profesionales utilizan muchas técnicas de Ingeniería Social para lograr persuadir a sus clientes, aunque en el caso de los médicos, sus recomendaciones son en pro de la salud de sus

pacientes. Pero también existen los que se dedican a cometer actos ilícitos como prestarse para estafas por tierras y otras estafas[21].

6.4 MARCO NORMATIVO

En Colombia en el año 2009 la Ley 1273 introdujo y tipificó más exactamente los delitos informáticos, abarcando todos los aspectos en cuanto a lo relacionado con la protección de la información y además brindando los mecanismos y soportes jurídicos para que las empresas, organizaciones y personas puedan proteger mejor su información, y servir de herramienta para poder denunciar lo cual es muy importante pues fue un gran paso en la lucha que hasta hoy día se sigue en contra de estos actos y sus autores.

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*"[22].

Otras leyes en la legislación colombiana sobre delitos informáticos:

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"[23].

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"[24].

---

[21] Basado en la lectura de: Social Engineering: The Art of Human Hacking. Disponible en: https://www.pdf-archive.com/2014/06/02/social-engineering-the-art-of-human-hacking/

[22] Tomado textualmente de: Ley 1273 de 2009. Disponible en: http://www.mintic.gov.co/portal/604/w3-article-3705.html

[23] Tomado textualmente de: Ley estatutaria 1266 del 31 de diciembre de 2008. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1266_2008.html

[24] Tomado textualmente de: Ley 1341 del 30 de julio de 2009. Disponible en: http://www.mintic.gov.co/portal/604/w3-article-3707.html

7 PRODUCTO A ENTREGAR

El resultado final del proyecto, será un análisis y estudio profundo de la ingeniería social presente en las alcaldías del Huila, con el fin de concientizar principalmente a este tipo de entidades públicas, acerca de los métodos de ataques actuales que se practican y que afectan tanto a entidades públicas como privadas, conocer el impacto y riesgo que pueden provocar y proponer una serie de controles que permitan prevenir o mitigar el impacto de los ataques provenientes de la ingeniería social en las alcaldías del Huila.

8 PLANIFICACIÓN DEL PROYECTO

El presente proyecto planea abarcar diferentes aspectos y áreas determinantes para establecer criterios importantes en su desarrollo, vinculando todos los entornos que se relacionan con la ingeniería social, y abarcando campos que vienen desde la parte tecnológica e informática hasta la parte social y económica, enfocando esencialmente el área pública del departamento del Huila, específicamente en las alcaldías. En el inicio del proyecto se buscarán las bases teóricas e históricas de la ingeniería social, para poder identificar bien las amenazas que ayudaran a realizar esta investigación. Se buscará encontrar y detallar los nuevos métodos de ataques que se han desarrollado y evolucionado en los últimos años, hasta llegar a convertirse en una gran amenaza que ha llegado a afectar no solo a personas, sino también a entidades públicas y privadas. Una vez sean identificados los factores de riesgo y amenazas, se describirán los respectivos controles y métodos de prevención para mitigar el impacto que podría producir un ataque de ingeniería social en las alcaldías del Huila, con el propósito de aumentar la seguridad en los entornos informáticos que allí se encuentran.

Igualmente, durante el desarrollo del proyecto, se describirán los detalles relevantes encontrados, en cuanto a falencias de seguridad, que serán respectivamente soportados, a fin de que la información sea totalmente real y verificable, además de no sólo llegar a datos teóricos, sino también a los prácticos, que se realizarán en dichas entidades. El proyecto se desarrollará de forma organizada, teniendo en cuenta el cronograma de actividades para el control del tiempo y desarrollo de cada uno de los componentes del presente proyecto.

9 RECURSOS NECESARIOS PARA EL DESARROLLO

Utilizando recursos como el software libre, visitas a empresas, uso de computares personales, búsqueda de información en bibliotecas públicas e internet, y demás recursos gratuitos disponibles, que estén dentro del marco legal y que no requieran de mayores inversiones. Los recursos que se necesitarán para el desarrollo del proyecto se detallan a continuación.

Tabla 2. Recursos necesarios.

RECURSO	DESCRIPCIÓN	PRESUPUESTO
Equipo Humano	Estudiantes del proyecto. No se requiere personal adicional	Cero Pesos ($ 0)
Equipos	No se requiere compra de equipos nuevos.	Cero Pesos ($ 0)
Software	Se utilizará software libre.	Cero Pesos ($ 0)
Viajes	Transporte para las visitas a algunas alcaldías del Huila	Trescientos Mil Pesos ($ 300.000)
Salidas de Campo	Viáticos para gastos indispensables.	Trescientos Mil Pesos ($ 300.000)
Materiales	Papelería en general, dispositivos de almacenamiento USB.	Doscientos Mil Cero Pesos ($ 300.000)
TOTAL	**Quinientos Mil Pesos ($ 900.000)**	

Fuente: el autor.

10 CRONOGRAMA DE ACTIVIDADES

Fecha de inicio: 27 de agosto de 2017
Fecha de finalización: 30 de noviembre de 2017
Tutor: Ing. Salomón González

Tabla 3. Cronograma de actividades.

Tarea	Días	Inicio	Fin	Ag	Septiembre				Octubre					Noviembre		
				S1	S2	S3	S4	S5	S6	S7	S8	S9	S10	S11	S12	S13
Asesoría	96	27/08/2017	30/11/2017	■	■	■	■	■	■	■	■	■	■	■	■	■
Definición del tipo de proyecto	3	27/08/2017	29/08/2017	■												
Definición del tema de investigación	5	30/08/2017	03/09/2017	■	■											
Definición de objetivos	4	04/09/2017	07/09/2017		■											
Definición de alcance	3	08/09/2017	10/09/2017			■										
Justificación	3	11/09/2017	13/09/2017			■										
Fuentes bibliográficas	12	14/09/2017	25/09/2017			■	■	■								
Metodología	7	26/09/2017	02/10/2017					■	■							
Marco referencial	5	03/10/2017	07/10/2017						■							
Diseño de encuestas	9	08/10/2017	16/10/2017							■	■					
Aplicación de encuestas	10	17/10/2017	26/10/2017								■	■				
Análisis de resultados	8	27/10/2017	03/11/2017									■	■			
Entrevistas	8	04/11/2017	11/11/2017										■	■		
Análisis de entrevistas	7	12/11/2017	18/11/2017											■	■	
Elaboración del documento	10	19/11/2017	28/11/2017												■	■
Entrega del proyecto final	2	29/11/2017	30/11/2017													■

Fuente: el autor.

11 DISEÑO DE ENCUESTAS

La encuesta constará de 30 preguntas clasificadas en 6 fases (identificación, conocimiento, vulnerabilidades, amenazas, impacto y controles) teniendo en cuenta componentes de la metodología MAGERIT, para tener una mayor organización de la información. Todas las peguntas serán de modo selección múltiple y las respuestas tomadas en valores cuantitativos (de 1 a 5), y otras en valores cualitativos predefinidos, con el fin de obtener datos de una forma más clara y precisa, y facilitar la calificación y cuantificación de los resultados estadísticos obtenidos.

Tabla 4. Diseño de encuestas.

Fase	Número	Pregunta	Respuesta	Tipo
Fase 1: Identificación	1	¿Nombre del cargo que posee?	Única	Cualitativa
	2	¿A qué dependencia pertenece su cargo?	Única	Cualitativa
	3	¿Cuántas personas están a cargo del área de sistemas?	Única	Cuantitativa
	4	¿Cuántas personas más tiene acceso al área de sistemas?	Única	Cuantitativa
	5	¿Cuáles son los activos más importantes de la entidad?	Múltiple	Cualitativa
Fase 2: Conocimiento	6	¿Sabe que es la ingeniería social?	Única	Cuantitativa
	7	¿Tienen los demás empleados conocimiento acerca de la ingeniería social?	Única	Cuantitativa
	8	¿Conoce los métodos o controles de seguridad para mitigar la ingeniería social?	Única	Cuantitativa
	9	¿Sabe cómo atender un caso de ingeniería social?	Única	Cuantitativa
	10	¿Sabe cómo realizar un estudio de vulnerabilidades, amenazas, riesgos y controles informáticos?	Única	Cuantitativa
Fase 3: Vulnerabilidades	11	¿Se ha realizado alguna evaluación de vulnerabilidades?	Única	Cualitativa
	12	¿Conoce el estado actual de vulnerabilidades?	Única	Cuantitativa
	13	¿En qué grado de vulnerabilidad cree que se encuentre la entidad?	Única	Cuantitativa
	14	¿Se han capacitado a los empleados en cuanto a la seguridad informática?	Única	Cuantitativa
	15	¿Qué grado de vulnerabilidad cree que estaría un empleado si fuese atacado por ingeniería social?	Única	Cuantitativa

Tabla 4. Diseño de encuestas (continuación).

Fase	Número	Pregunta	Respuesta	Tipo
Fase 4: Amenazas	16	¿Se ha realizado alguna evaluación de amenazas?	Única	Cualitativa
	17	¿Qué amenazas puede identificar dentro de su entidad?	Múltiple	Cualitativa
	18	¿Qué amenazas ha sido víctima la entidad?	Múltiple	Cualitativa
	19	¿Cuáles cree que son los motivos que tendría un ingeniero social para atacar la entidad?	Múltiple	Cualitativa
	20	¿Cuáles cree que serían los activos más importantes que un ingeniero social atacaría?	Múltiple	Cualitativa
Fase 5: Probabilidad e Impacto	21	¿Qué tan presente puede estar la ingeniería social en su entidad?	Única	Cuantitativa
	22	¿Qué tan frecuente se presentan las amenazas informáticas en su entidad?	Múltiple	Cuantitativa
	23	¿Cuál es el impacto de las amenazas informáticas en su entidad?	Múltiple	Cuantitativa
	24	¿Qué probabilidad de éxito cree que tendría un ataque de ingeniería social?	Única	Cuantitativa
	25	¿Cuáles serían los activos más afectados por la ingeniería social?	Múltiple	Cualitativa
Fase 6: Controles	26	¿Se ha realizado alguna evaluación de controles en la entidad?	Única	Cualitativa
	27	¿Qué tipo de controles se realizan para proteger los activos informáticos?	Múltiple	Cualitativa
	28	¿Cree que los controles actuales son suficientes para mitigar la ingeniería social?	Única	Cuantitativa
	29	¿La entidad posee políticas de seguridad?	Única	Cualitativa
	30	¿Se aplicarán nuevos controles de seguridad de los activos en un futuro próximo?	Única	Cualitativa

Fuente: el autor.

La siguiente es una tabla que muestra el tipo de respuesta, que tendrá cada una de las preguntas según su categoría.

Tabla 5. Tipos de respuesta de la encuesta.

Tipos de respuesta	Cuantitativa	Cualitativa
Múltiple	Términos predefinidos calificables de 1 a 5	Términos predefinidos
Única	1 a 5	Término definido

Fuente: el autor.

12 RESULTADO DE ENCUESTAS

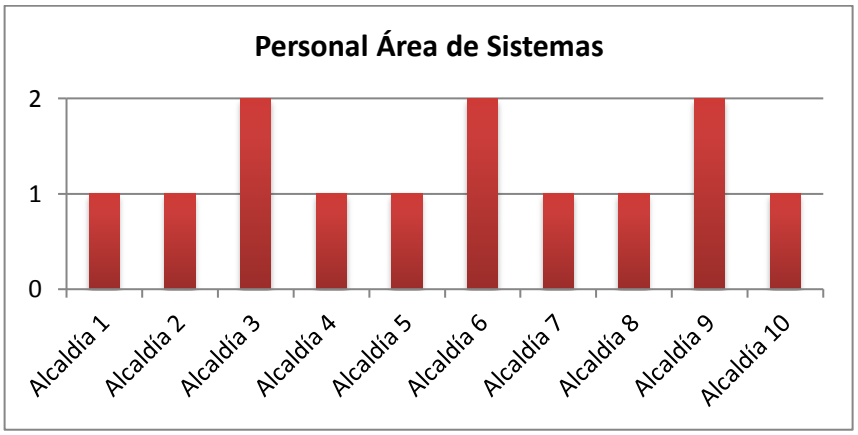
La encuesta se realizó satisfactoriamente escogiendo a diez (10) de las alcaldías huilenses tomadas al azar, conservando la integridad de la entidad y reservando el derecho de su identidad por motivos de seguridad. La mayoría de las encuestas se realizó telefónicamente, al personal directo encargado del área sistemática que cuyos cargos se relacionan con la informática y el apoyo a las TIC de su municipio.

A continuación, se exponen los resultados de las encuestas en fases, donde se demuestran datos muy relevantes en cuanto al estado actual de la seguridad informática de las entidades públicas.

12.1 FASE 1: IDENTIFICACIÓN.

Esta fase comprende la identificación de algunos datos necesarios tanto de la entidad pública como del encuestado.
Uno de los datos positivos que se obtuvieron en esta fase, es que todas las entidades poseen un personal adecuado encargado del área de sistemas, figura 5, con una profesión u ocupación relacionada con las TIC. Sus cargos en su mayoría pertenecientes a las dependencias de Secretaría General y Secretaría de Planeación.

Figura 5. Personal área de sistemas.

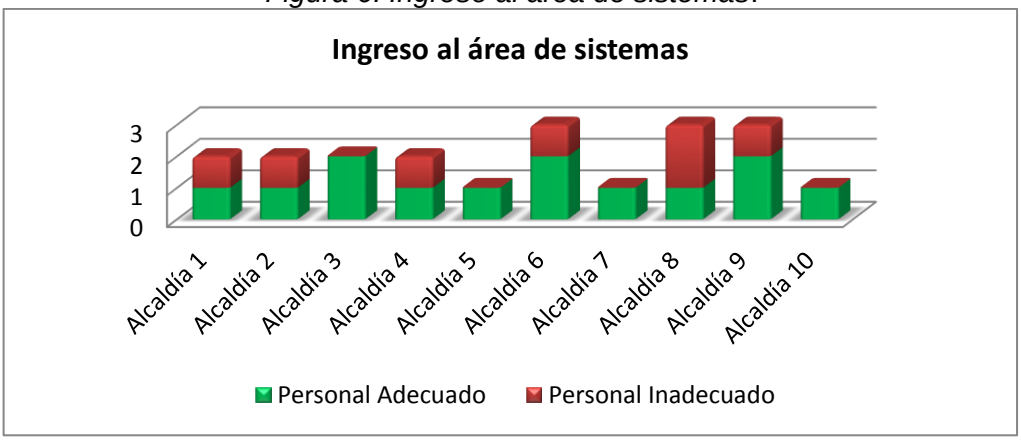


Fuente: el autor.

Las personas a cargo del área de sistemas no superan el número de tres (3) personas, siendo un promedio de una (1) o dos (2) personas a cargo por entidad.

Ahora bien, unos de los datos que si hay que preocuparse, es el control de acceso de otras personas al área de sistemas, tales como asiadoras, contratistas u otras personas que pueden tanto desconfigurar el sistema o causar otro tipo de daño. Figura 6. Se puede notar que son muy pocas las entidades que sólo se permite el acceso al personal autorizado.

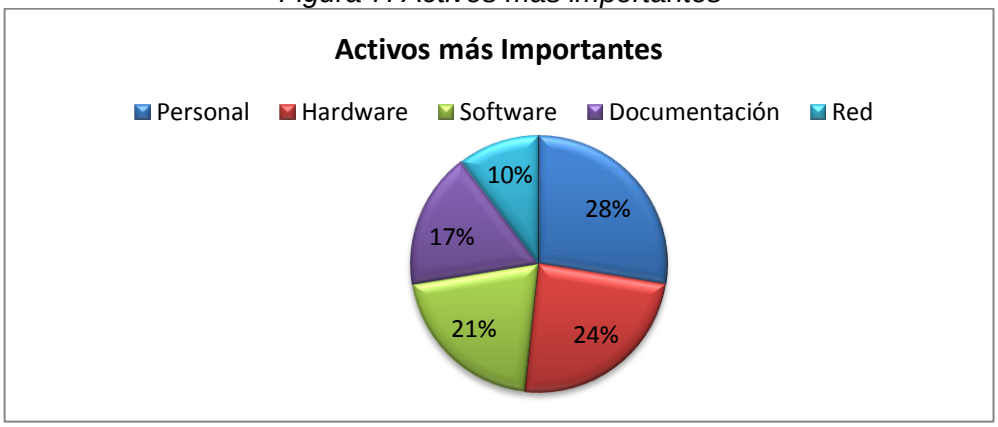
Figura 6. Ingreso al área de sistemas.



Fuente: el autor

A continuación en la figura 7, se puede identificar cuáles son los tipos de activos más importantes en las entidades públicas, con el siguiente orden de prioridad: Personal, Hardware, Software, Documentación y por último la Red.

Figura 7. Activos más importantes

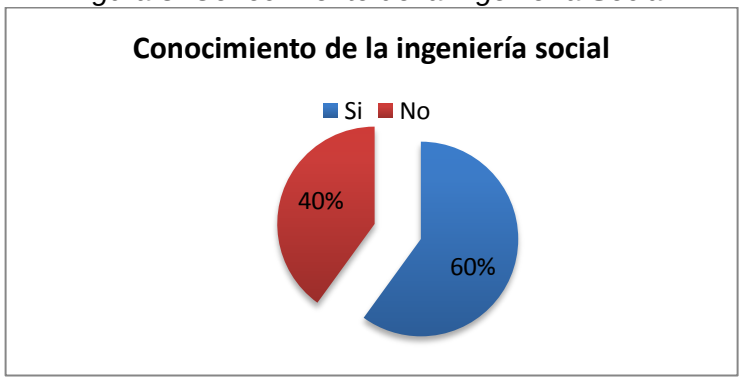


Fuente: el autor

12.2 FASE 2: CONOCIMIENTO.

Esta fase comprende el nivel del conocimiento y capacidades que tiene la entidad y su personal a cargo frente a temas relacionados con la ingeniería social.
Como primera medida, es importante reconocer el nivel de conocimiento acerca de la ingeniería social que tienen las personas a cargo de los sistemas de información. Figura 8.

Figura 8. Conocimiento de la Ingeniería Social.

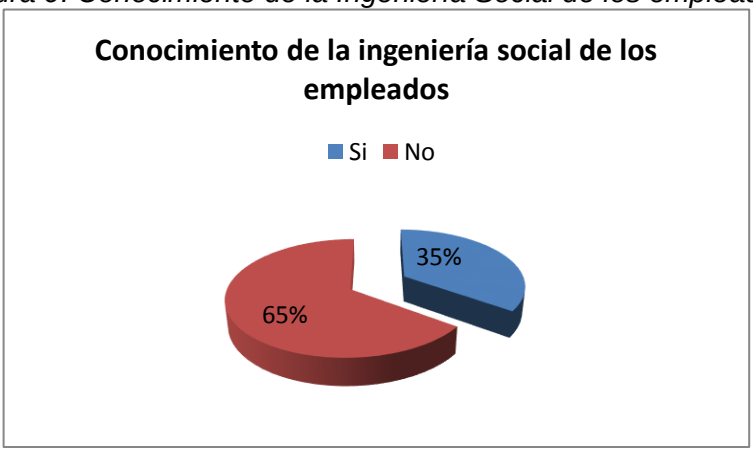


Fuente: el autor.

Aunque más de la mitad del personal tiene conocimientos previos acerca de la ingeniería social (60%), no es un nivel suficiente para asegurar una mayor atención y protección a los activos informáticos en las entidades frente a esta amenaza. Como uno de los propósitos del desarrollo de la encuesta, también es concientizar a los empleados para que fortalezcan sus conocimientos de la ingeniería social.

En base a lo anterior mencionado, el dato más preocupante está en los demás empleados, puesto a ellos también son puntos directos de ataque de la ingeniería social, y ellos también deben tener al menos una base de conocimiento sobre esta amenaza. Figura 9.

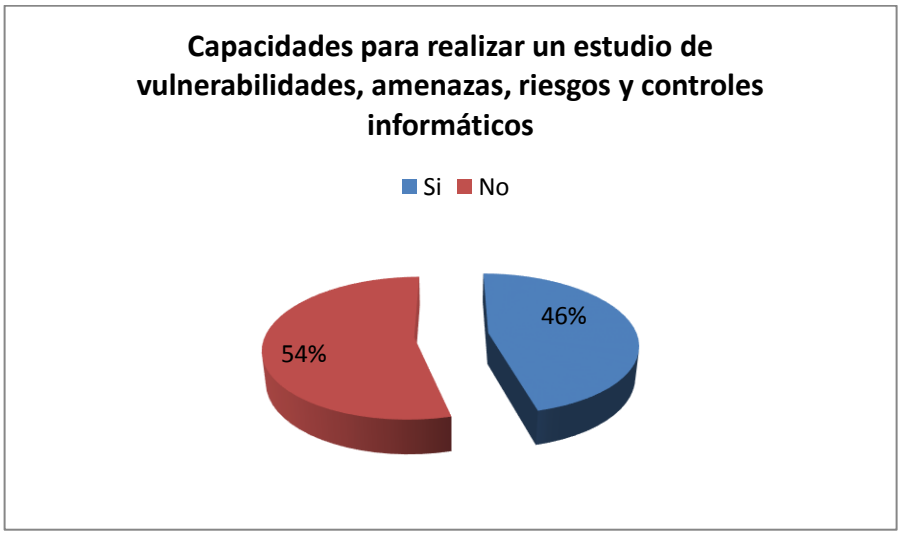
Figura 9. Conocimiento de la Ingeniería Social de los empleados.



Fuente: el autor.

Como en el caso del nivel de conocimiento acerca de la ingeniería social, las entidades a penas se encuentran en un nivel aceptable para poder realizar un estudio de la seguridad de sus activos, como es el de vulnerabilidades, amenazas, riesgos y sus controles respectivamente. Figura 10.

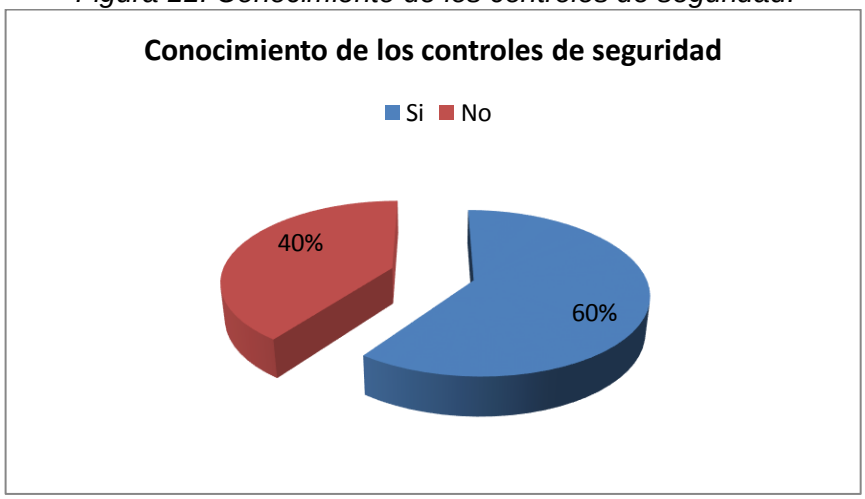
Figura 10. Capacidades para realizar un estudio de vulnerabilidades, riesgos, amenazas y controles informáticos.



Fuente: el autor

Cuando la ingeniería social es una amenaza activa, es importante reconocer y aplicar los controles o métodos de seguridad mínimos cuanto antes, para mitigar el impacto de esta. En las alcaldías municipales encuestadas, más de la mitad tiene conciencia para aplicar algunos controles suficientes para contrarrestar esta amenaza. Figura 11.

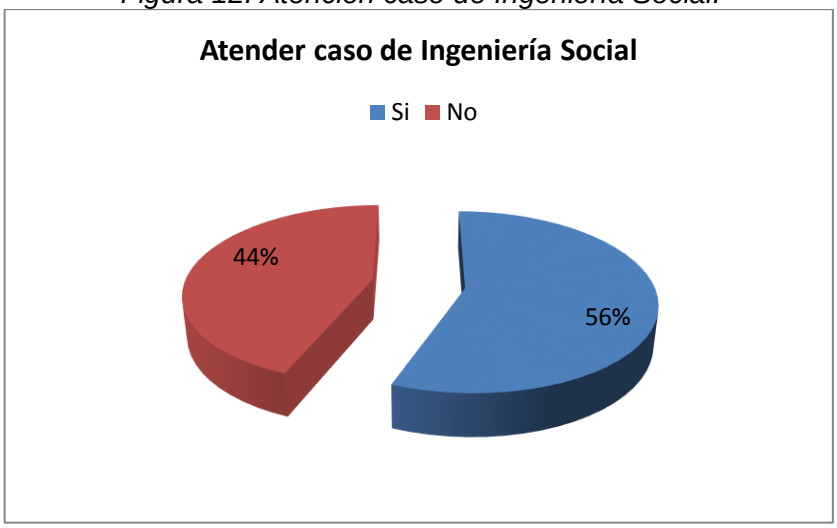
Figura 11. Conocimiento de los controles de seguridad.



Fuente: el autor.

Del 60% de las entidades que poseen unas bases para aplicar los controles, en su mayoría (56%) pueden atender un caso de ingeniería social, es decir, que solo el 4% restante más el 40% que no poseen las capacidades, para un total de 44%, no tienen las capacidades necesarias para atender un caso de ingeniería social. Figura 12.

Figura 12. Atención caso de Ingeniería Social.



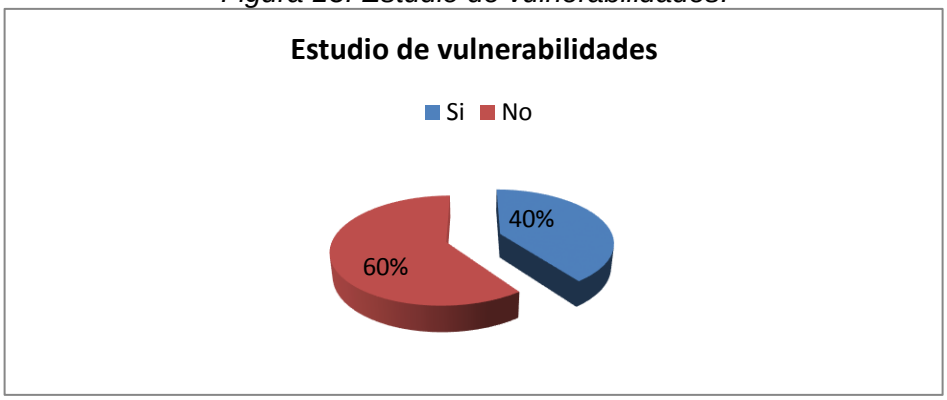
Fuente: el autor.

12.3 FASE 3: VULNERABILIDADES.

Esta fase se encarga de revelar un estudio aproximado del nivel de vulnerabilidad o debilidades en que se encuentran las alcaldías municipales.

Dentro de la encuesta realizada, se indagó acerca del estudio de vulnerabilidades dentro de sus entidades, dato que no incluía específicamente la mención de las vulnerabilidades sino del estudio realizado en sí, y se encontró que menos de la mitad han realizado un estudio acerca de las vulnerabilidades presentes en sus entidades. Figura 13.

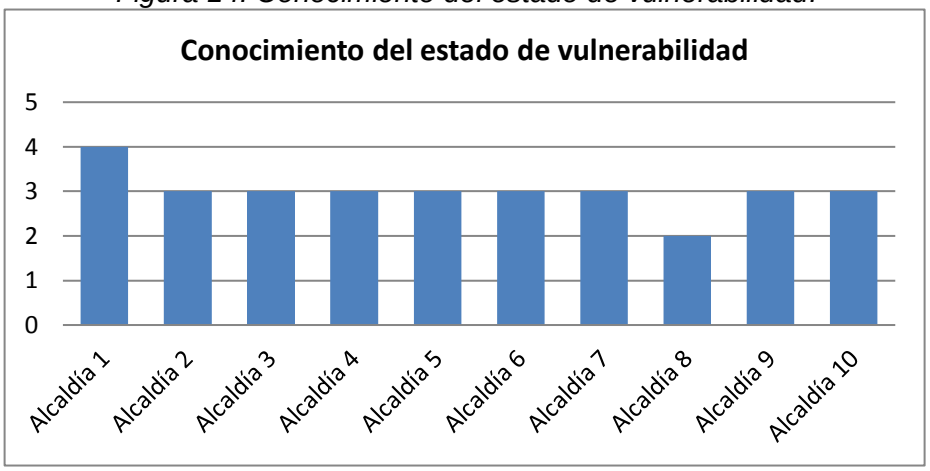
Figura 13. Estudio de vulnerabilidades.



Fuente: el autor.

Un dato preocupante, ya que si incialmente no se tiene un estudio realizado acerca de las vulnerabilidades presentes en sus entidades, es difìcil determinar el estado o certeza del estado real de vulnerabilidad o afectaciones que podría sufrir los sistemas de información dentro de sus entidades. Figura 14.

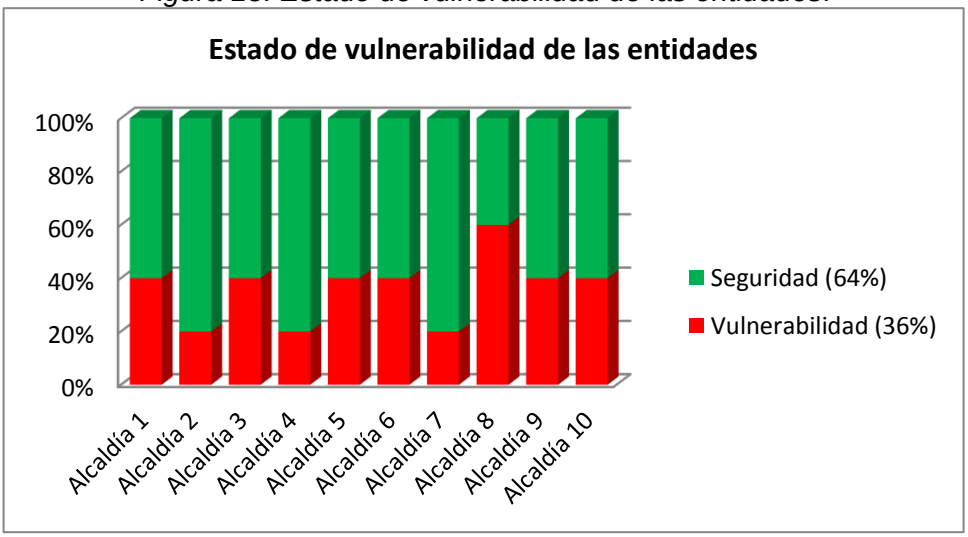
Figura 14. Conocimiento del estado de vulnerabilidad.



Fuente: el autor.

Realizando un reconocimiento acerca del estado actual de vulnerabilidad, figura 15, se obtiene que 64% de las entidades cuentan con un grado de seguridad, el resto (36%), podrían ser puntos débiles desconocidos que pueden dar lugar a vulnerabilidades, objeto que debe de ser analizado minuciosamente para controlar los puntos ciegos de las alcaldías.

Figura 15. Estado de vulnerabilidad de las entidades.

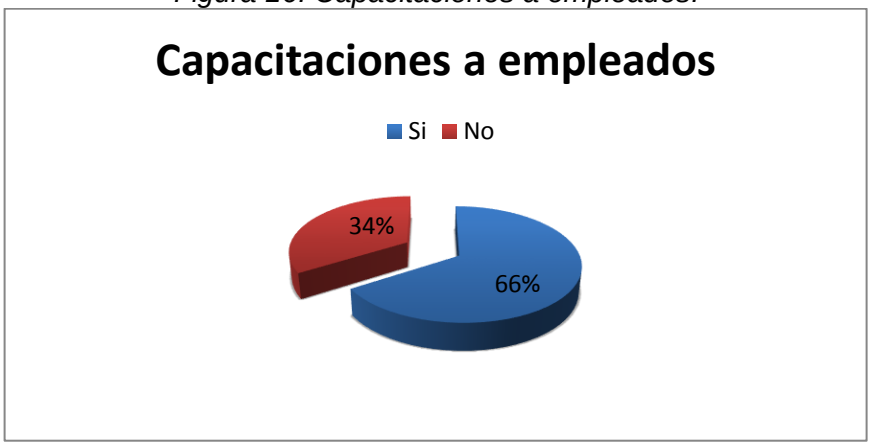


Fuente: el autor.

Otro punto a favor, es que en la mayoría de las entidades (66%), han concientizado a sus empleados en cuanto a la seguridad informática de sus

puestos de trabajo, un gran punto a favor, ya que generalmente todos los empleados utilizan sistemas informáticos para desarrollar sus labores.

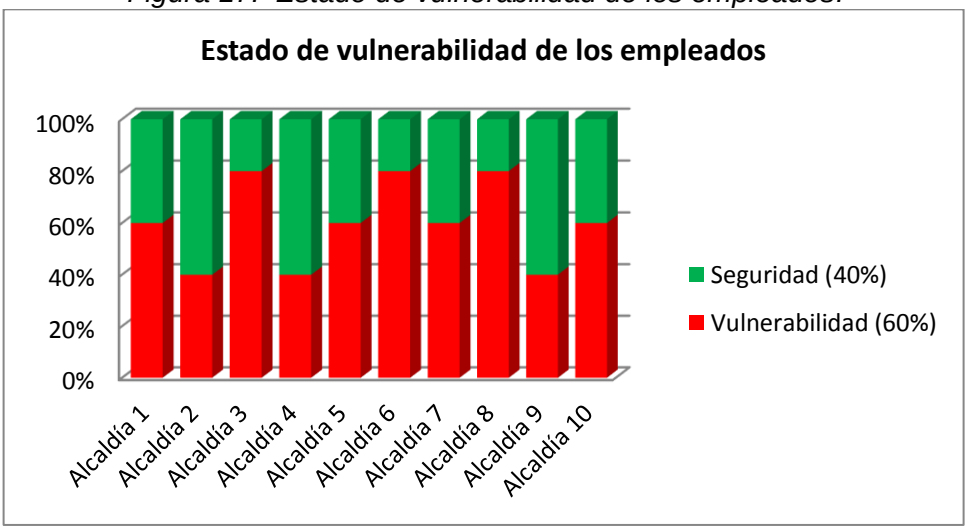
Figura 16. Capacitaciones a empleados.



Fuente: el autor.

Pero diseñando nuevamente un paralelo frente a la vulnerabilidad y seguridad de los empleados, a pesar de las capacitaciones recibidas, figura 16, este no es un proceso suficiente para graduar positivamente el nivel de seguridad de los empleados, puesto a que actualmente, el 60% de ellos aún se encuentran en condiciones vulnerables. Figura 17.

Figura 17. Estado de vulnerabilidad de los empleados.



Fuente: el autor.

12.4 FASE 4: AMENAZAS.

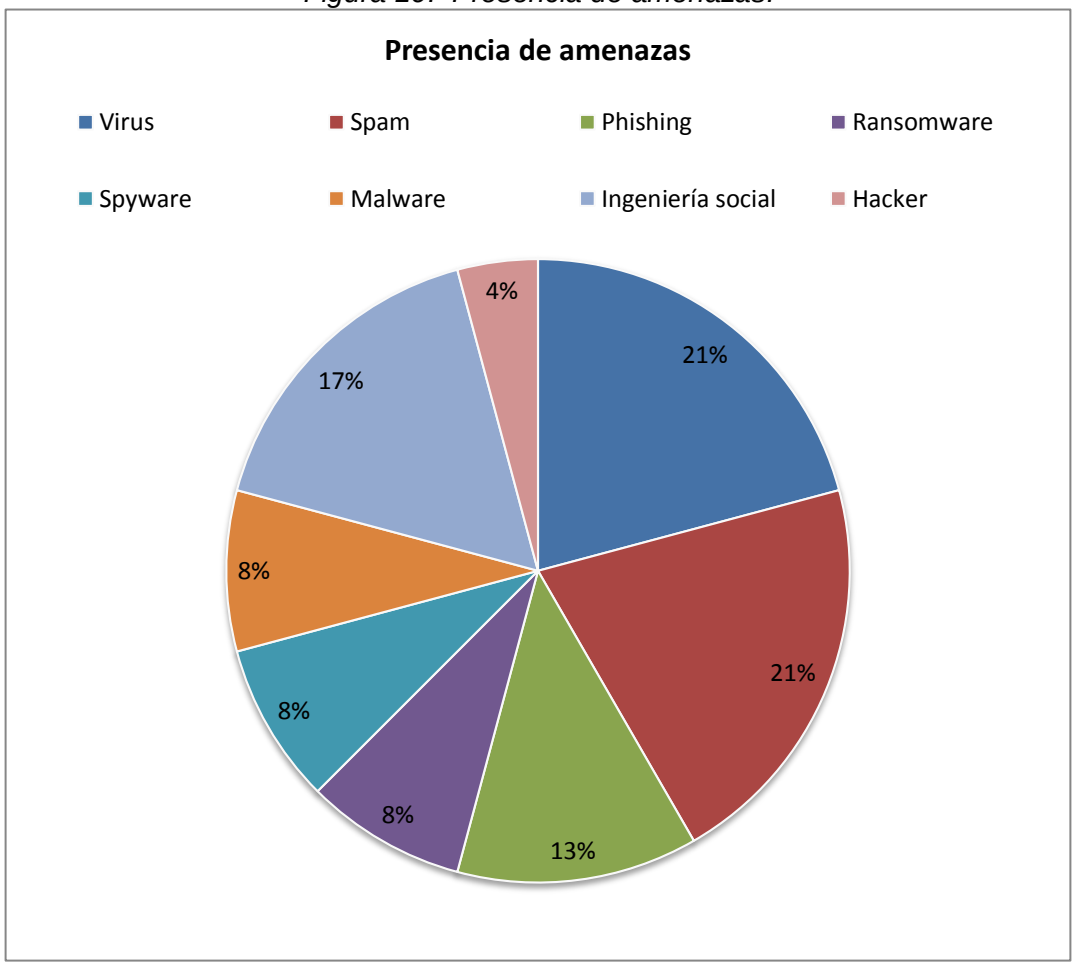
Esta fase analiza el nivel y los factores de amenazas relacionados tanto con la ingeniería social como de las demás amenazas presentes en las alcaldías municipales.
Acerca del estudio interno de amenazas en las entidades públicas, se obtiene que la mitad de las entidades han realizado un estudio, figura 18. El resto se defiende con su propia experiencia.

Figura 18. Estudio de amenazas.

Fuente: el autor.

Uno de los datos obtenidos más importantes, es el nivel de las amenazas presentes en las alcaldías municipales, figura 19. Un dato muy favorable para tomar las medidas necesarias frente a ellas.

Figura 19. Presencia de amenazas.

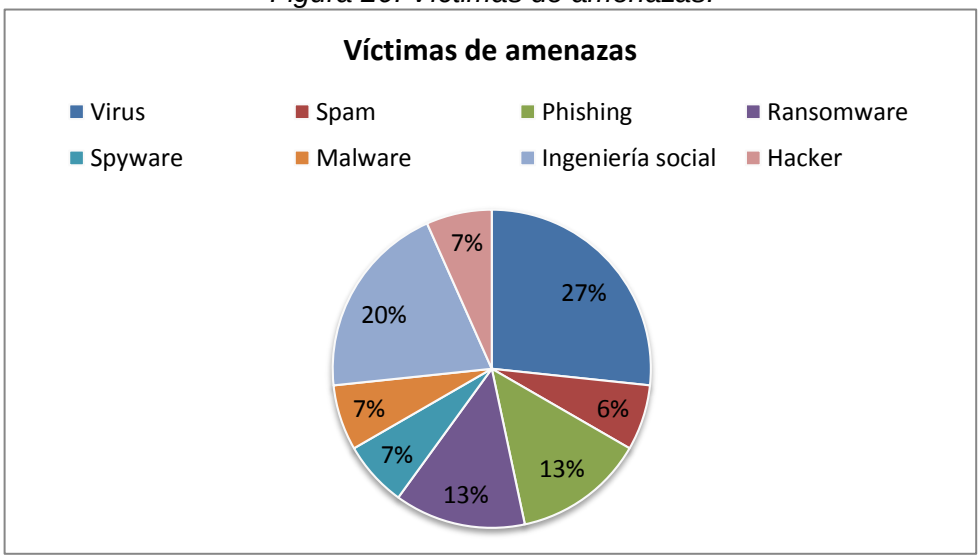


Fuente: el autor.

Como se puede observar, el virus informático que incluye los gusanos, troyanos, bombas lógicas y sus derivados relacionados, son la principal amenaza dentro de las entidades, junto con el spam, que es el correo no deseado, en donde se asegura, que diariamente se reciben correos no deseados de diferentes direcciones. Las siguientes amenazas más presentes son la ingeniería social y el phishing, con un grado más elevado de riesgo, y por último tenemos al *malware*, *spyware*, el *ransomware* y el *hacking*, siendo estos últimos una amenaza con menos presencia, pero con un grado muy alto de impacto.

Siguiendo la referencia de la presencia de amenazas en las entidades, se obtiene también un dato relacionado muy relevante acerca del nivel de ataques obtenidos.

Figura 20. Víctimas de amenazas.

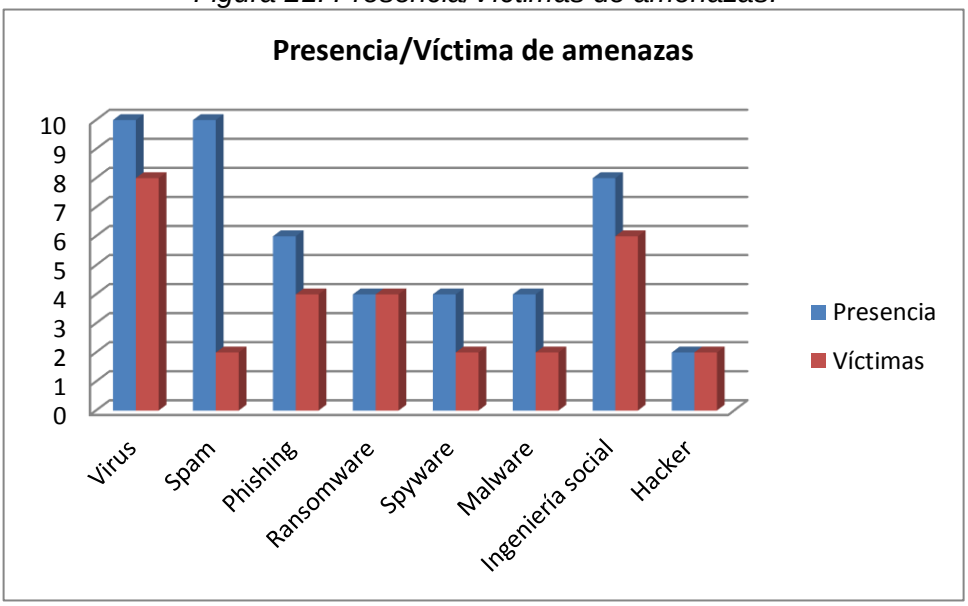


Fuente: el autor.

Como se presencia en la figura 20, a pesar de ser una de las amenazas más comunes, el virus informático a través de su mayor presencia, ha logrado obtener los números más altos en ataques informáticos dentro de las entidades, seguido de la Ingeniería Social, cuya amenaza puede involucrar a la mayor parte de los activos incluyendo el personal, seguidamente tenemos el *Phishing*, *Spam*, y el *Ransomware*, después le sigue el *Malware* y el *Spyware*, y por último y no menos riesgoso, el *hacker*.

Con los dos anteriores datos propuestos, se puede realizar un paralelo entre la presencia de amenazas y sus víctimas, obtenidas por los ataques dentro de las entidades públicas, generando así un valor aproximado de su eficiencia de ataque.

Figura 21. Presencia/Víctimas de amenazas.

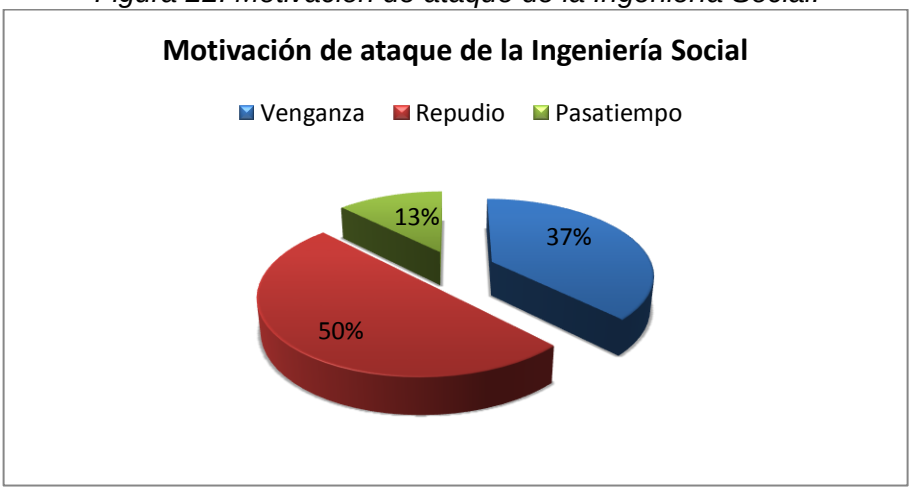


Fuente: el autor.

Como se puede apreciar en la figura 21, el virus informático tiene una gran presencia dentro de las entidades públicas, siendo este uno de los más presentes y amenazas más riesgosas dentro de los equipos informáticos. El *Spam*, a pesar de su gran presencia, su nivel de víctimas es muy bajo, siendo así una amenaza de riesgo muy baja. El *Phishing* por su parte, presenta un nivel de amenaza medio, tanto en su presencia como en su nivel de víctimas. El *ransomware*, a pesar de no tener un gran nivel de presencia, su efectividad de riesgo es casi segura durante el ataque, siendo así una de las amenazas más peligrosas. El *Spyware* y el *Malware* no poseen niveles altos de presencia ni de víctimas, por lo que no se consideran amenazas tan peligrosas. Por otra parte, la ingeniería social si tiene presencia media-alta en las entidades, y su nivel de víctimas también es muy considerable, posicionándose así también como una amenaza peligrosa. Finalmente tenemos al *hacker*, esta amenaza generalmente no se puede presenciar, debido a que en su mayoría no se implementan sistemas de detección, por lo que posiblemente es la respuesta a la cual esta amenaza se muestre como “poco probable”, pero que, en sí, se debe considerar que, a pesar de ello, puede causar grandes riesgos.

A continuación, en la figura 22, se muestra una de las posibles causas o motivaciones principales por las que se realizaría ingeniería social en una alcaldía municipal.

Figura 22. Motivación de ataque de la Ingeniería Social.

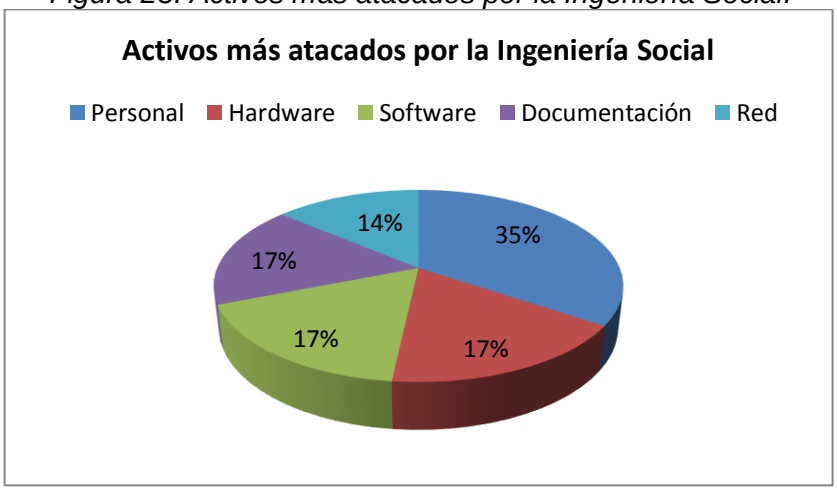


Fuente: el autor.

La mayor de las causas es debido al repudio, seguido de la venganza, puesto a que, en Colombia, no se tiene un gran aprecio por la política y sus personajes, siendo una alcaldía municipal parte de ello. Por último, se encuentra el pasatiempo, que se reconoce como gente aficionada que por su ficción intentan realizar este tipo de ataques.

Otro factor del que se debe tener en cuenta, es la víctima final, el artefacto o activo que el ingeniero social preside atacar. A continuación, en la figura 23, se muestran los activos más atacados por la ingeniería social.

Figura 23. Activos más atacados por la Ingeniería Social.



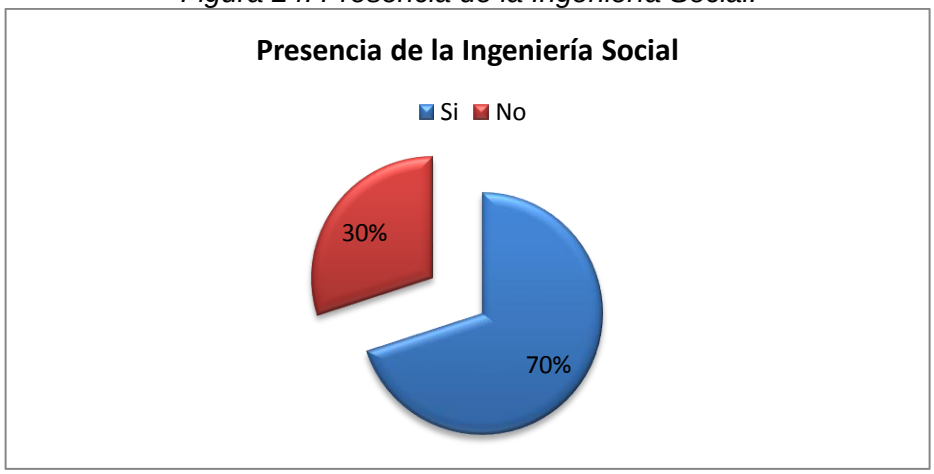
Fuente: el autor.

En primer lugar, tenemos a las personas como la principal víctima de la ingeniería social, debido a que esta precisamente se encarga de confundir o engañar psicológicamente a una persona. Les sigue el software, hardware y la documentación que son activos que pueden reservar información importante, y por último teneos a la red, considerada la menos atacada por la ingeniería social.

12.5 FASE 5: PROBABILIDAD E IMPACTO

Esta fase se encarga de estudiar y medir el nivel de ocurrencia e impacto que podría tener la ingeniería social y demás amenazas, para así calcular un valor aproximado del riesgo que puede estar presente en las alcaldías municipales.
Anteriormente se había mencionado acerca de la presencia de distintas amenazas, en esta ocasión, se puede apreciar exclusivamente la ingeniería social. Figura 24.

Figura 24. Presencia de la Ingeniería Social.

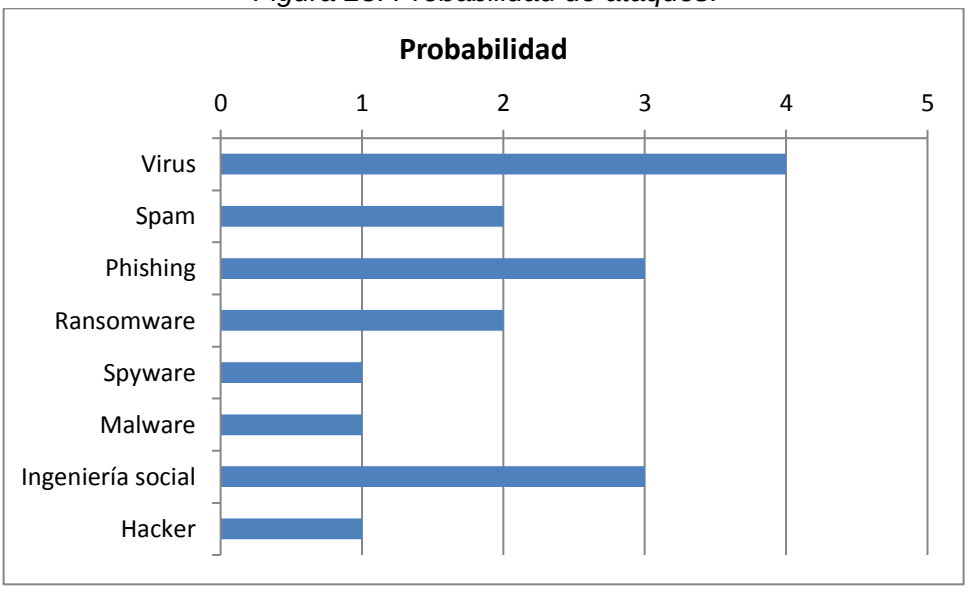


Fuente: el autor.

En el 70% de las entidades aseguran tener casos de ingeniería social, mientras el 30% restante, no presencian esta amenaza.

Uno de los propósitos más grandes de la encuesta realizada, es obtener información relevante y más precisa de los niveles de la situación actual frente a las amenazas informáticas hoy en día. Para ello se recurrió a realizar una medición simple de la probabilidad y el impacto que podría tener cada una de ellas. Figura 25.

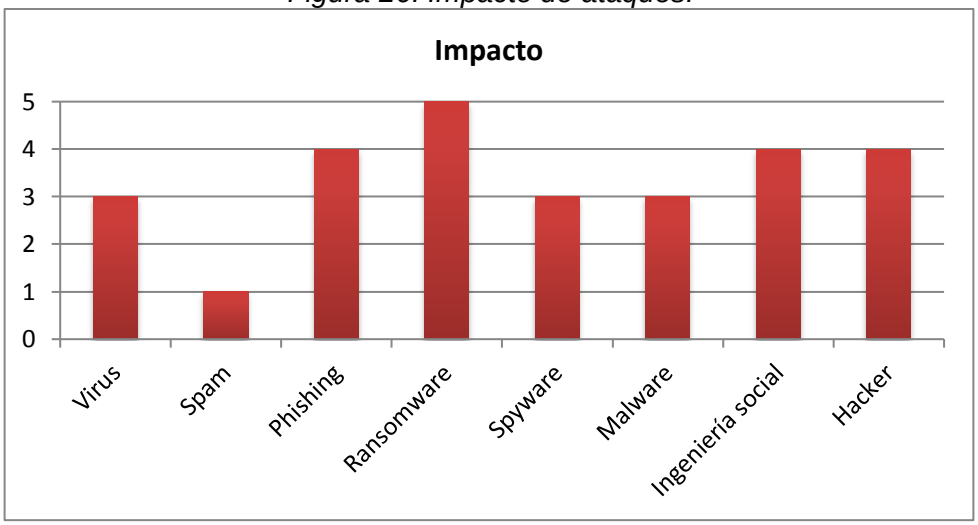
Figura 25. Probabilidad de ataques.



Fuente: el autor.

Como en los anteriores casos, el Virus Informático es el más propenso y presente entre las amenazas informáticas, seguido del *Phishing*, *Spam*, la Ingeniería Social y el *Ransomware*, y en los puestos finales, el *Spyware*, *Malware* y el *Hacker*.
El siguiente proceso fue el de obtener y calcular el nivel de impacto promedio que causaría cada una de las amenazas dentro de sus entidades.

Figura 26. Impacto de ataques.



Fuente: el autor.

Según los resultados, figura 26. Se obtuvo que el *Ransomware* es una de las amenazas más peligrosas de acuerdo a su impacto, esto debido a que una vez tenga efecto en su víctima, el daño generalmente es irreversible, causando grandes pérdidas de información importante. Seguidamente tenemos al *Phishing*, la *Ingeniería Social* y el *Hacker* como las siguientes amenazas más peligrosas; después tenemos al *Virus*, el *Spyware* y el *Malware* como las siguientes amenazas de menor impacto, y finalmente tenemos al Spam, considerada como la amenaza menos peligrosa.
Con los anteriores datos mencionados, se puede calcular un promedio del riesgo informático, tomando las bases de la metodología *MAGERIT*, hallando el riesgo obtenido de la multiplicación del nivel de probabilidad por el nivel de impacto, a través de la siguiente tabla.

Tabla 6. Estimación del riesgo.

Riesgo		**Impacto**				
		1	**2**	**3**	**4**	**5**
Probabilidad	**5**	**5**	**10**	**15**	**20**	**25**
	4	**4**	**8**	**12**	**16**	**20**
	3	**3**	**6**	**9**	**12**	**15**
	2	**2**	**4**	**5**	**8**	**10**
	1	**1**	**2**	**3**	**4**	**5**

Fuente: el autor.

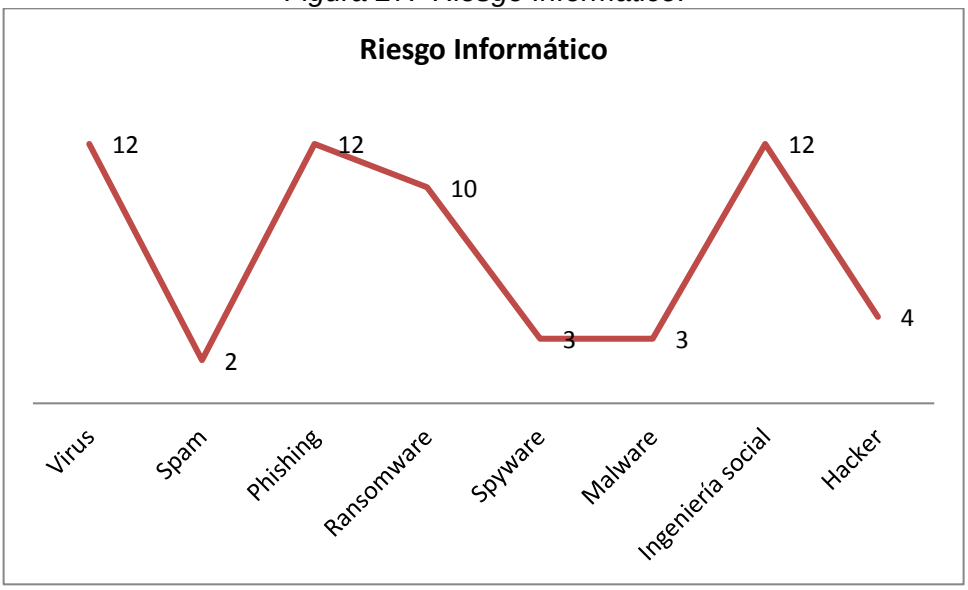
Tabla 7. Estimación para cada amenaza.

	Probabilidad	**Impacto**	**Riesgo**
Virus	4	3	12
Spam	2	1	2
Phishing	3	4	12
Ransomware	2	5	10
Spyware	1	3	3
Malware	1	3	3
Ingeniería social	3	4	12
Hacker	1	3	3

Fuente: el autor.

De acuerdo a estas medidas, la Ingeniería Social, junto con el Virus y el *Phishing* son consideradas las amenazas de más riesgo en las alcaldías municipales, figura 27. Seguido del *ransomware*, el *hacking*, *Spyware*, *Malware* y en último lugar, el *Spam*.

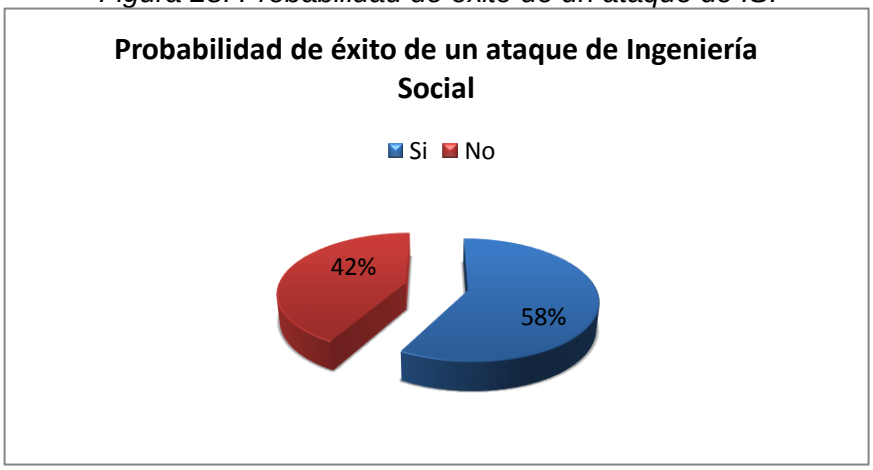
Figura 27. Riesgo Informático.



Fuente: el autor.

Siguiendo las medidas de probabilidad, a continuación, se mide el nivel de éxito que podría tener la ingeniería social dentro de la entidad. Figura 28.

Figura 28. Probabilidad de éxito de un ataque de IS.

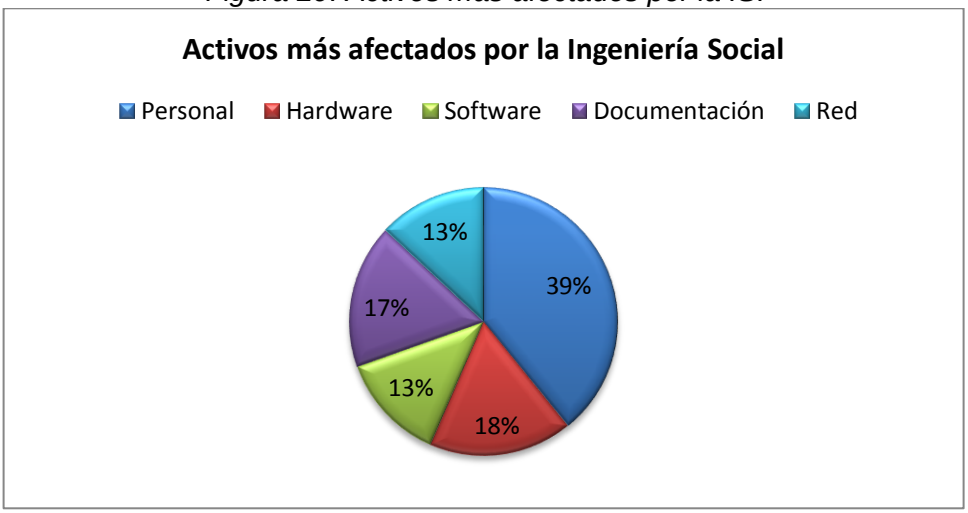


Fuente: el autor.

Según los resultados, la probabilidad de éxito sería de un 58%, un resultado no favorable para las alcaldías municipales. Este dato es preocupante, ya que, según esto, existe una mayor probabilidad de que se pueda realizar la ingeniería socia dentro de la entidad.

Como los recursos más afectados, se tiene principalmente al personal como la principal víctima de la ingeniería social, considerando sea este uno de los puntos más débiles, seguidamente del hardware, documentación, el software y la red. Figura 29.

Figura 29. Activos más afectados por la IS.

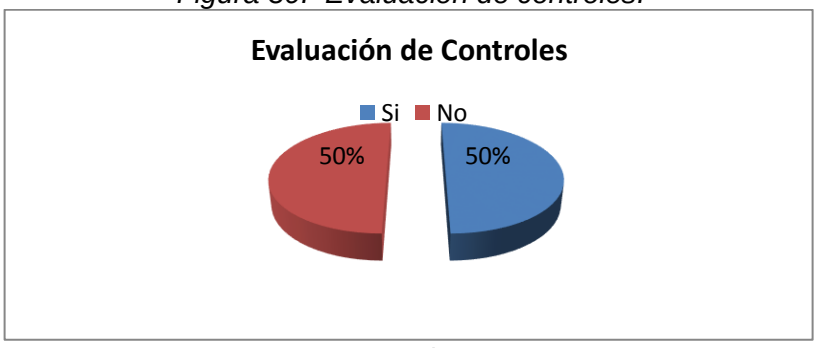


Fuente: el autor.

12.6 FASE 6: CONTROLES.

Esta fase corresponde al estudio y nivel de implementación de los métodos y controles de seguridad que se implementan dentro de las alcaldías municipales.
La figura 30 nos muestra el porcentaje de evaluación de controles de seguridad realizadas en las entidades públicas, sólo la mitad de ellas lo han realizado.

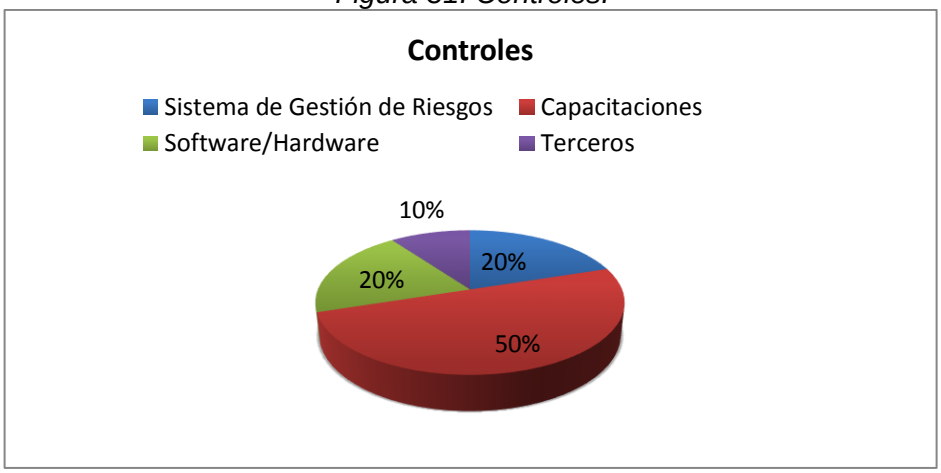
Figura 30. Evaluación de controles.



Fuente: el autor.

Generalizando los controles que se utilizan, tenemos la siguiente información, figura 31.

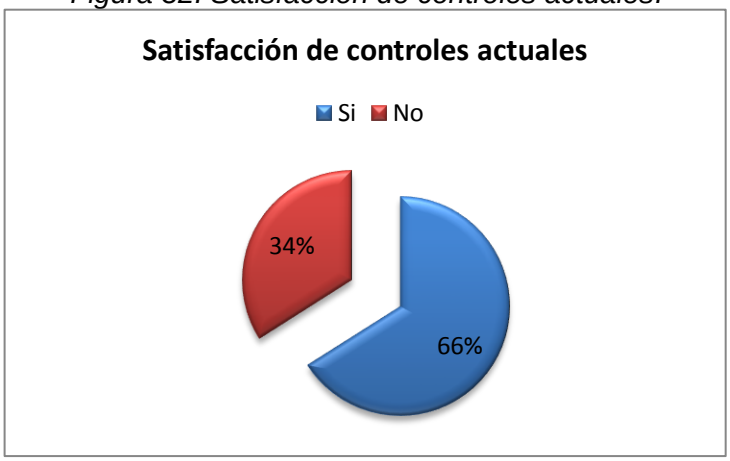
Figura 31. Controles.



Fuente: el autor.

El control de seguridad más utilizado, son las capacitaciones, un factor muy favorable, ya que como anteriormente se mencionó, el factor humano depende mucho de la seguridad de los demás activos. El siguiente control a utilizar es el del Software y SGR, aunque el SGR es un mecanismo muy útil para maximizar la seguridad de la información, no es el método más implementado en las alcaldías. Finalmente se tienen a los terceros, como última medida de control, ya la mayoría de las entidades prefieren reservar los activos y su información.
Otro punto a considerar, es el nivel de satisfacción actual que tienen con sus controles implementados. Figura 32.

Figura 32. Satisfacción de controles actuales.



Fuente: el autor.

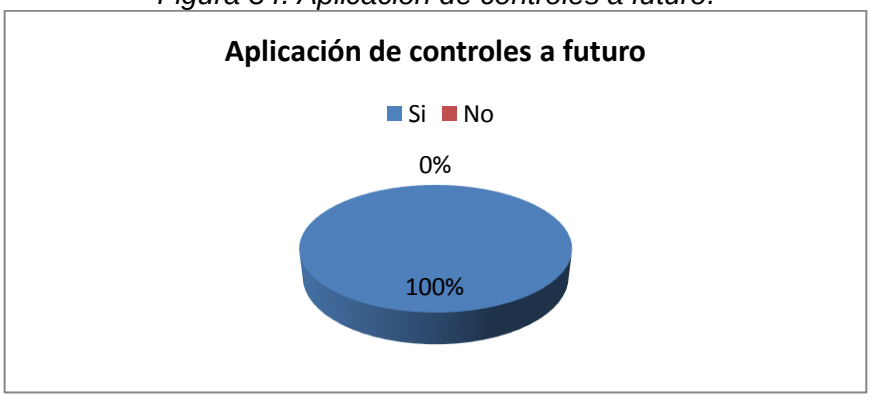
Según el análisis, el 66% de las entidades se encuentran satisfechas, y el 34% consideran que no son suficientes para tener una seguridad plena de sus activos.
En las entidades públicas existe un documento que es de obligatorio diseño, cumplimiento y publicación, llamado políticas de seguridad, en donde casi todas las alcaldías lo poseen y aseguran tenerlo en cumplimiento. Figura 33.

Figura 33. Políticas de seguridad.

Fuente: el autor.

Finalmente, es importante revelar si las entidades desean y pretenden implementar nuevos controles de seguridad en las alcaldías en un futuro. Figura 34.

Figura 34. Aplicación de controles a futuro.



Fuente: el autor.

La respuesta a este interrogante fue muy positiva. De acuerdo a esta información hace que documentos como el presente sean muy factibles de realizar, que servirán de guía y modelo para mejorar la seguridad de la información en las entidades públicas.

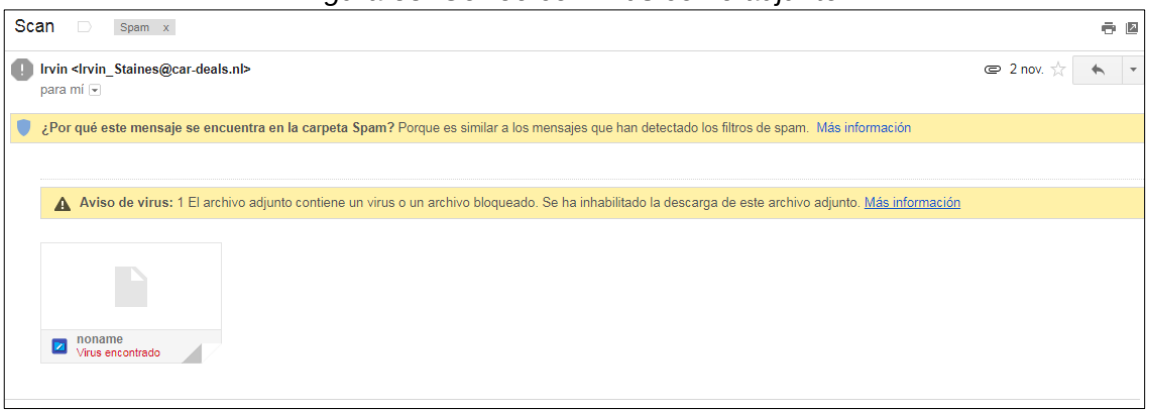
13 FUNCIONAMIENTO DE LAS AMENAZAS ENCONTRADAS EN LAS ALCALDÍAS MUNICIPALES

Lo que se pudo determinar por medio de las encuestas, en lo dialogado y encontrado mediante la observación física y lógica, permite evidenciar las diferentes formas en que la Ingeniería Social puede llegar a ser amenazas importantes en este tipo de entidades, ya que, como entidades públicas, manejan una gran cantidad de información muy importante de sus municipios.
A continuación, se presentan diferentes amenazas con evidencias reales que se presentan en las alcaldías del Huila, reservando sus identidades por motivos de seguridad.

13.1 VIRUS

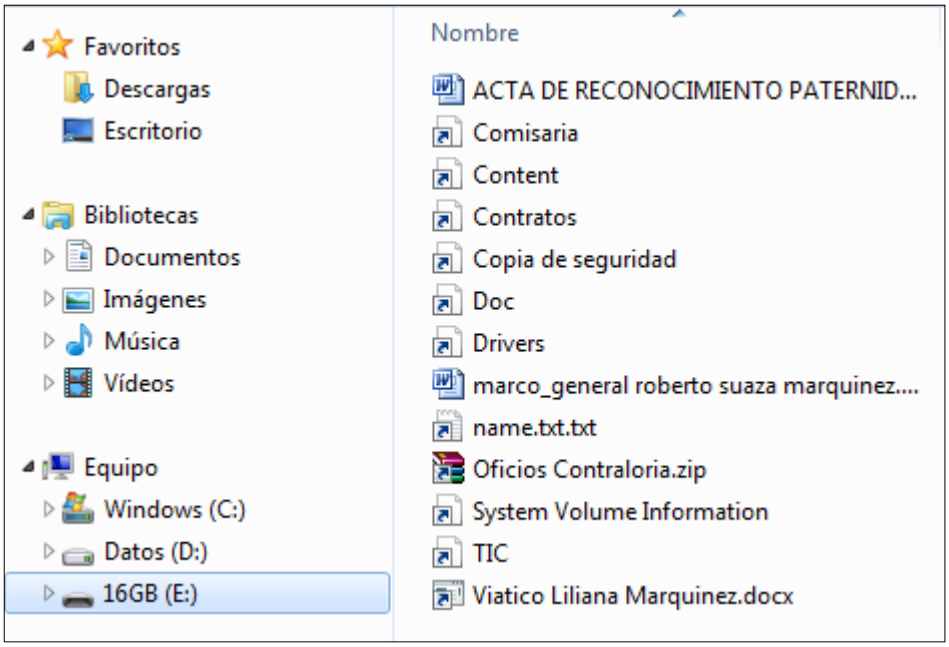
Prácticamente todos los usuarios saben que un virus puede afectar los equipos que tienen a cargo y, de hecho, han tenido que solicitar ayuda técnica para eliminarlos, pero la mayoría de ellos no son capaces de identificar un archivo infectado. Entonces se tiene que un usuario, aunque esté capacitado muchas veces, no tiene el cuidado necesario ni el hábito de actualizar el antivirus instalado en el equipo, de evitar insertar dispositivos como *USB* que pueden contener virus, figura 36, ni tampoco de realizar un análisis con el antivirus, esto generalmente debido al tiempo que se toma del escaneo cada vez que se inserta un dispositivo de almacenamiento *USB*. Los virus informáticos pueden provenir desde medios locales y externos, como por ejemplo en el correo electrónico, figura 35, que gracias a los servicios de escaneo de virus en línea se pueden lograr evitar o advertir al usuario de posibles amenazas.

Figura 35. Correo con virus como adjunto.



Fuente: el autor.

Figura 36. Memoria USB con virus informático.



Fuente: el autor.

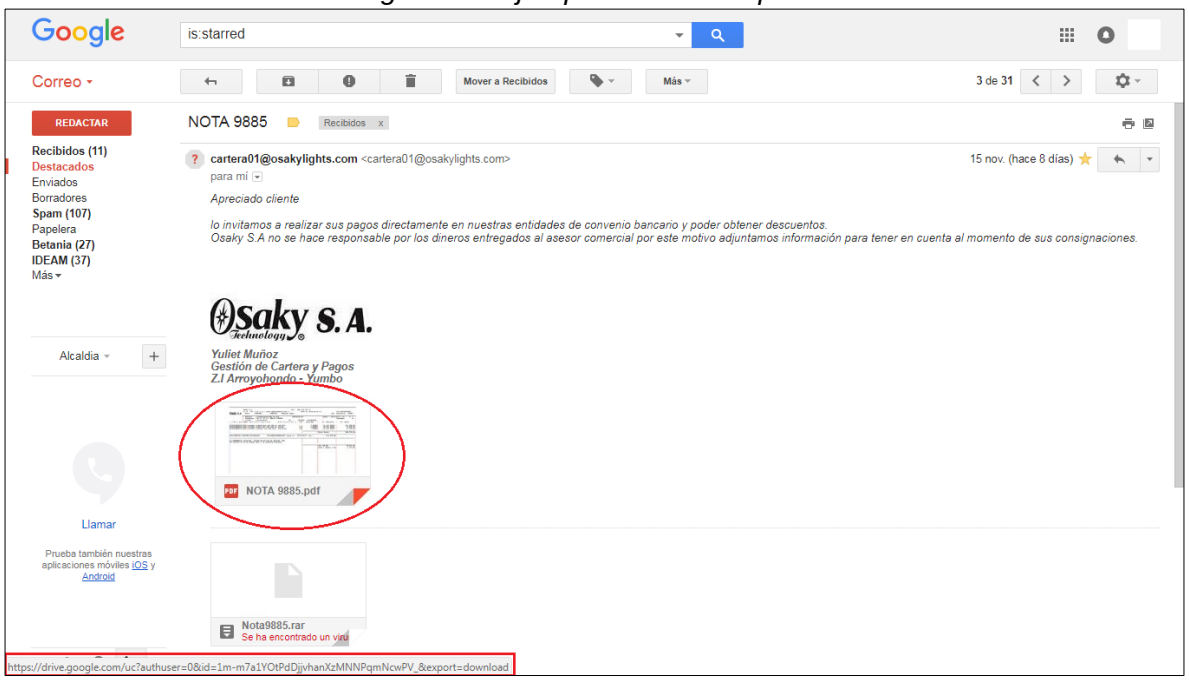
13.2 SPAM

El spam o correo no deseado, llega a través de correo electrónico, los usuarios en las diferentes alcaldías indican que el correo deseado, en su mayoría se filtra a la carpeta de *Spam*, en este caso del servicio de correo electrónico ofrecido por *Google*, que cuentan con correos institucionales con la siguiente estructura: dependencia@municipio-huila.gov.co, cada alcaldía cuenta con una cantidad promedio entre 5 a 20 correos corporativos. Los usuarios aseguran que a diario reciben aproximadamente entre 3 a 5 correos en el spam figura 37. El problema se presenta esencialmente cuando los empleados no logran identificar los correos spam que logran sobrepasar los filtros de seguridad y llegan directamente a la bandeja de entrada figura 38, estos contienen virus, enlaces, o adjuntos archivos adjuntos sospechosos que pueden comprometer la seguridad de la información y del equipo.

Figura 37. Correo spam de un mes.

Fuente: correo institucional de la alcaldía.

Figura 38. Ejemplo de correo spam.



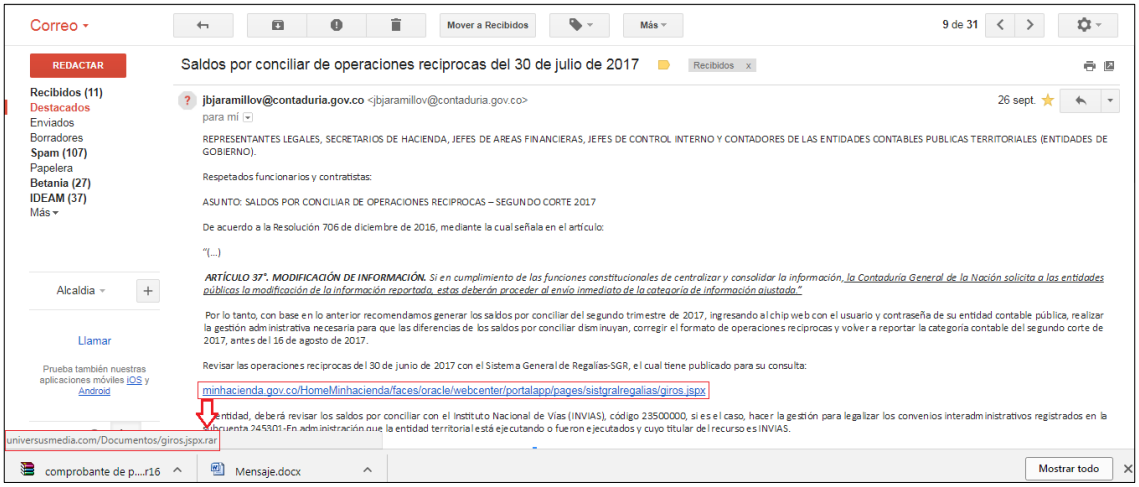
Fuente: el autor.

13.3 PHISHING

Este tipo de amenaza, se presenta generalmente a través del correo electrónico que incluye enlaces que redirigen al usuario a un sitio web falso figura 39. Allí, se les requiere ingresar sus credenciales de inicio de sesión o algún tipo de información, muchas veces un archivo de descarga que contiene códigos maliciosos. Al igual que en los casos anteriores, aunque existen capacitaciones los usuarios no prestan la suficiente atención a las mismas, desconocen muchas veces la manera de identificar los correos legítimos, esto a su vez, otorgaría acceso a los atacantes a las cuentas del usuario. Además, el *phishing* también puede realizarse por medio del teléfono, algo que la mayoría de usuarios indicó no

tener el suficiente cuidado, pues confían en la persona y brindan ayuda cuando se les requiere. Otro aspecto es que la mayoría de los empleados acceden a las redes sociales, habilitando otro campo donde se puede presentar este tipo de amenazas.

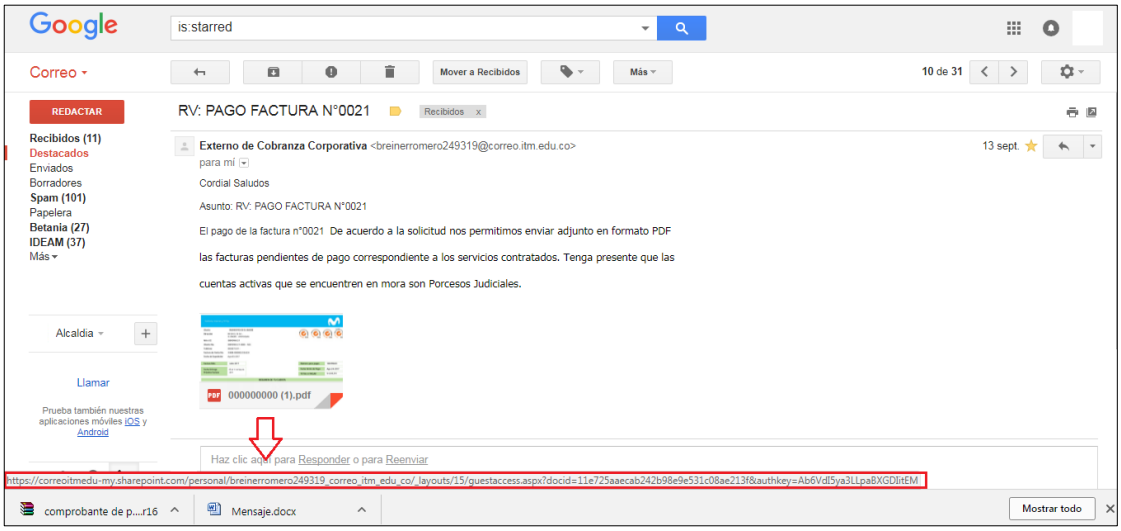
Figura 39. Ejemplo phishing 1.



Fuente: el autor.

Tal como se puede apreciar en la Figura. *39*, casos de *phishing* pueden llegar con información falsa, que contienen enlaces engañosos, donde exponen una URL de una fuente segura en el texto del correo, pero su hipervínculo redirige al usuario a otra página web diferente e insegura, esto con el fin de que el usuario sea engañado y acceda al enlace sospechoso.

Figura 40. Ejemplo phishing 2.



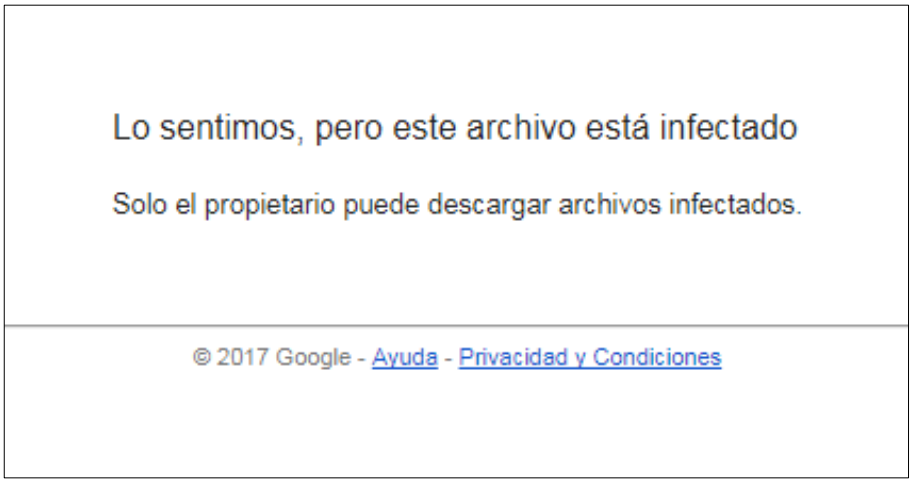
Fuente: el autor.

Otros casos de phishing, pueden presentarse con los adjuntos, en donde el atacante diseña una imagen o estilo similar a un archivo adjunto dentro del correo electrónico, haciendo creer al usuario de ser realmente un archivo adjunto del correo, pero que realmente es una imagen con un enlace que lo redirige a un sitio web falso o la descarga de archivos maliciosos figura 40.

13.4 RANSOMWARE

Los príncipes nigerianos ya no son las únicas amenazas que acechan en la bandeja de entrada de los empleados. Para las organizaciones gubernamentales y muchas empresas, los ataques de *ransomware* entregado a través de correos electrónicos de *spear phishing*, que pueden secuestrar valiosos activos de datos y exigen un rescate para liberarlos figura 41, son una amenaza de seguridad en rápido crecimiento, aunque hasta el momento no se han presentado casos a gran escala en estas entidades, los usuarios afirman desconocer cómo identificar este tipo de amenaza.

Figura 41. Ransomware.



Fuente: el autor.

13.5 SPYWARE

Los empleados de las alcaldías del Huila tienen acceso a Internet sin un control de privilegios o accesos, como para descargar archivos de uso personal, los usuarios no son conscientes del daño que su uso de *P2P*, instalación de programas desconocidos y de mensajería instantánea, que atraen la instalación de software malicioso figura 42, y que, si no se cuenta un buen antivirus actualizado, este podría traer graves consecuencias sobre la información de la entidad que se resguarda en el equipo.

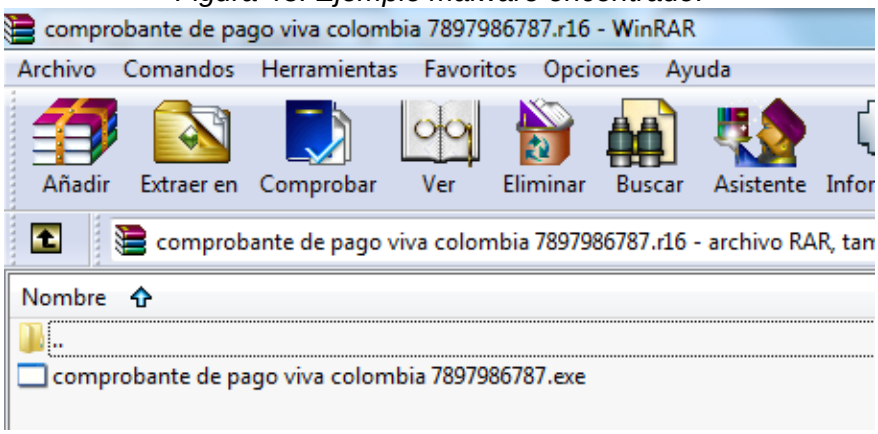
Figura 42. Spyware en archivo adjunto.

Fuente: el autor.

13.6 MALWARE

Al consultar a los usuarios acerca de los archivos adjuntos en los correos electrónicos o programas descargados figura 43, aunque la mayoría sabe que puede ser dañino, muchas veces logran ser descargarlos, ignorando las señales de advertencia, hecho como este es el que da lugar a momentos cuando el equipo empieza a presentar una lentitud en su rendimiento, también debido a la publicidad en los navegadores.

Figura 43. Ejemplo malware encontrado.



Fuente: el autor.

13.7 HACKER

Los ataques por hacker en lo que se conoce, no se han presentado hasta el momento, y respecto a estos, los administradores de los sistemas y las políticas de seguridad de las entidades ya han implementado el uso de contraseñas seguras, además como una medida de seguridad, las contraseñas se cambian varias veces durante el año en la mayoría de las plataformas y software. Igualmente, las redes cuentan con seguridad de encriptación y sistemas como *firewall*.

13.8 ACCESO FÍSICO

En la ingeniería social, se podría aprovechar circunstancias como las que se evidencian a continuación figura 44:

Figura 44. Documentos importantes sobre los escritorios.

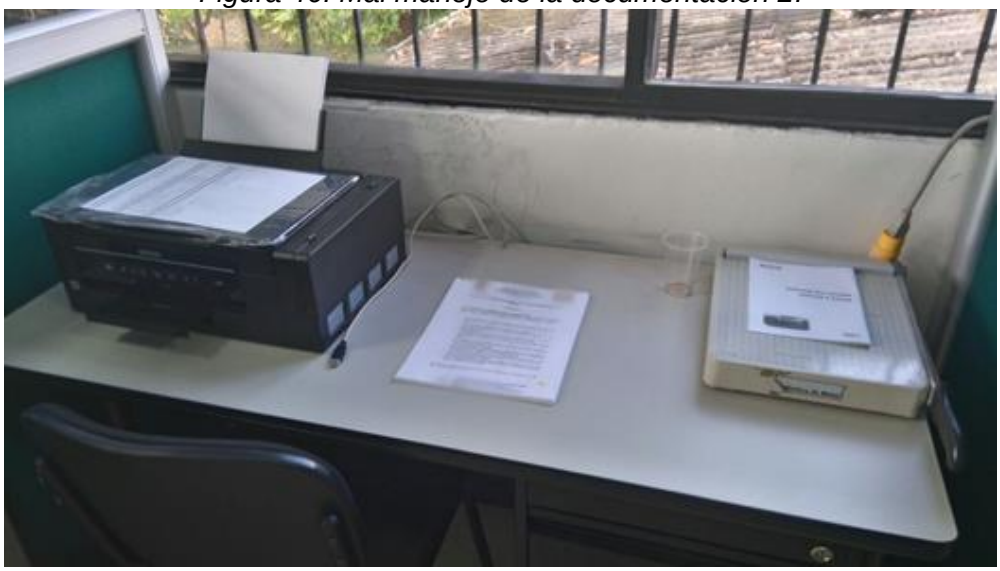
Fuente: el autor.

Este hecho permite que otras personas tengan fácil acceso a documentos que podrían ser algo muy importantes para la entidad. Si existen robos dentro de almacenes y otros lugares que cuentan con personal de seguridad, como no lo lograrían personas que podrían pasarse por un ciudadano corriente y logra acceder o tomar documentación que está muy accesible, figura 45 y figura 46.

Figura 45. Mal manejo de la documentación.

Fuente: el autor.

Figura 46. Mal manejo de la documentación 2.



Fuente: el autor.

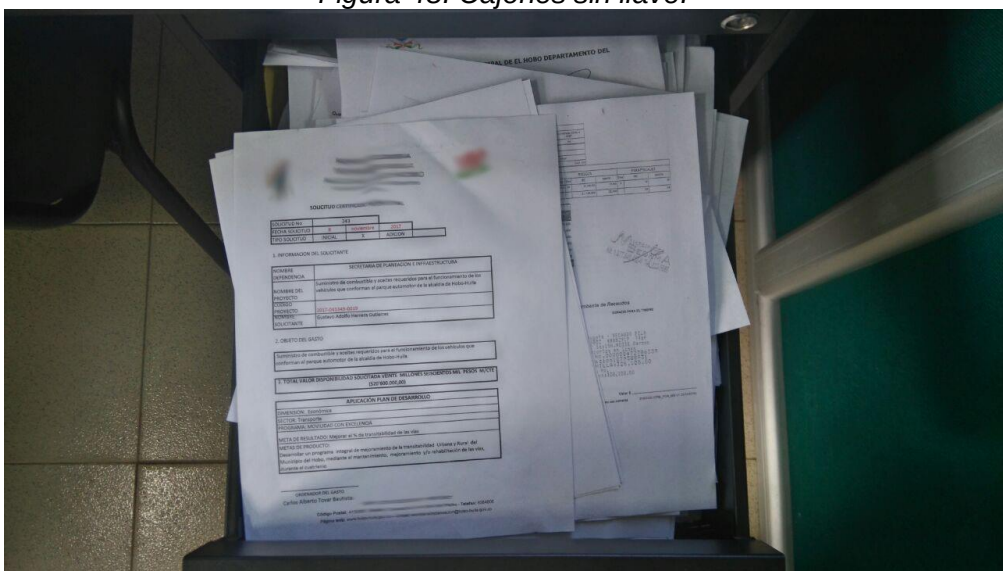
Otro hecho de los que pueden presentarse, es que, si no realiza un control adecuado a los accesos a las oficinas, personas externas fácilmente podría extraer, destruir o copiar con fotografías, información que podría ser confidencial de la entidad, figura 47.

Figura 47. Fáciles accesos físicos.

Fuente: el autor

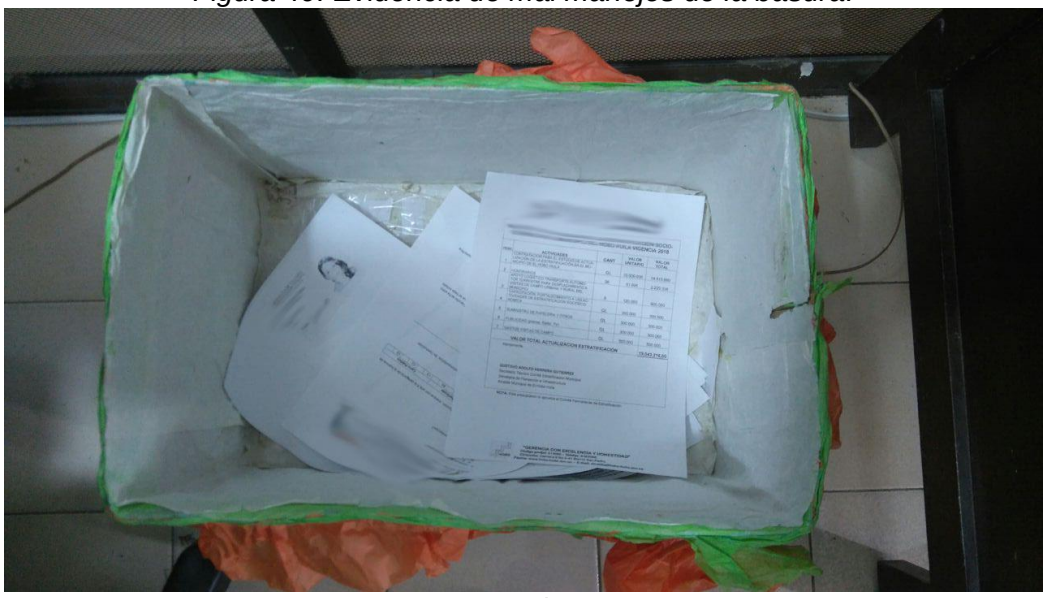
Los escritorios carecen de cerraduras que permitan poner bajo llave documentación importante, figura 48. Y además los sitios de almacenamiento de los mismos no son adecuados figura 49.

Figura 48. Cajones sin llave.



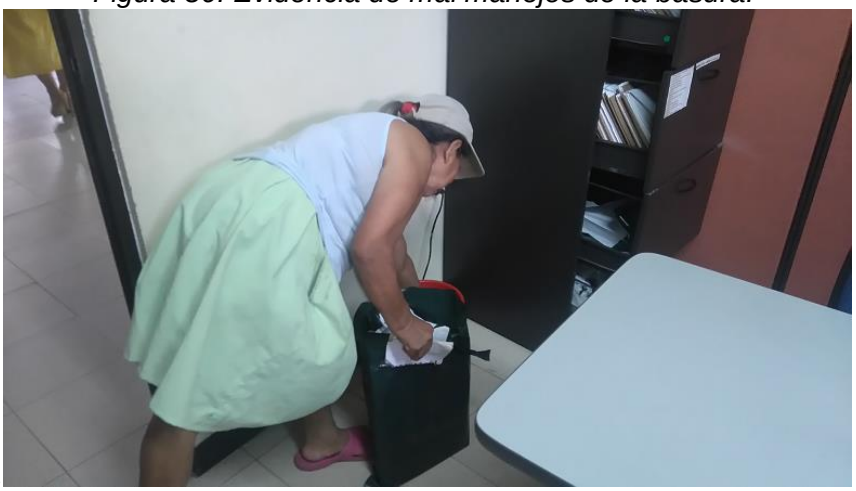
Fuente: el autor.

Figura 49. Evidencia de mal manejos de la basura.



Fuente: el autor.

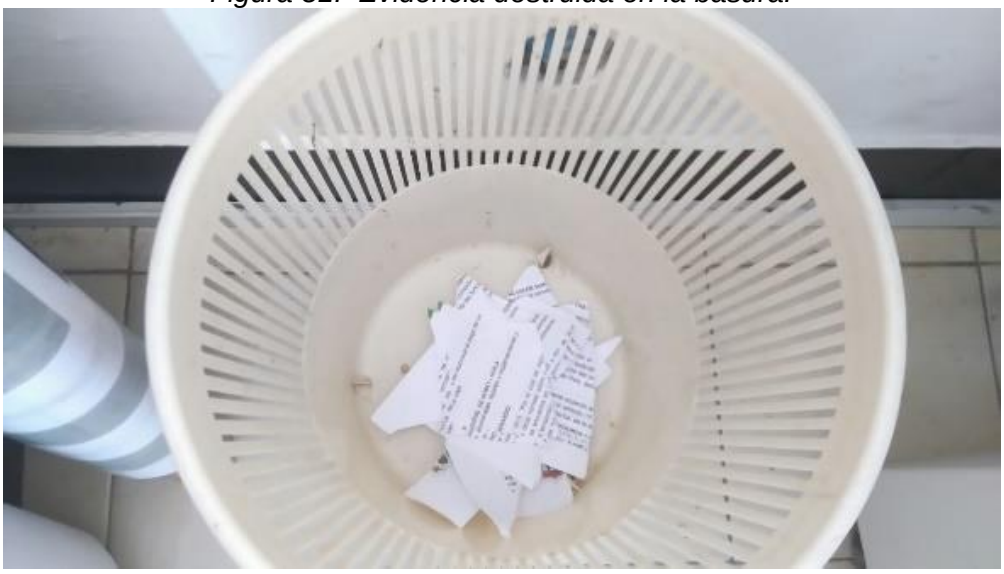
Figura 50. Evidencia de mal manejos de la basura.



Fuente: el autor.

Dentro del aspecto residual, figura 50, se ha encontrado una vulnerabilidad que permite a hasta personas externas, acceder a cierta parte de información de la entidad. Aunque a pesar de que la entidad es púbica, no toda la información puede ser revelada, y una parte de la documentación residual (basura) figura 51, logra salir de las instalaciones sin ser por lo menos destruida para quedar ilegible, esto con el fin de asegurar información reservada no caiga en manos de personas que pueden estar recolectando información en este mecanismo de desecho.

Figura 51. Evidencia destruida en la basura.



Fuente: el autor.

14 MÉTODOS FUNCIONALES QUE PERMITAN REDUCIR ATAQUES DE INGENIERÍA SOCIAL EN LAS ALCALDÍAS DEL HUILA

Dentro de los hallazgos encontrados, para mejorar las prácticas de seguridad dentro de las alcaldías del Huila se tienen:

14.1 GOBIERNO DIGITAL

En primera instancia, es de gran importancia comenzar por las recomendaciones o políticas establecidas por el gobierno nacional, que ha fundado estrategias para mejorar la eficiencia y seguridad TI dentro de las entidades públicas, una de estas es la que se conocía como Gobierno en Línea y que ahora comienza a llamarse Gobierno Digital, debido a una actualización entre sus componentes y lineamientos que se empezará a implementar durante el año 2018.

Figura 52. Logos de Gobierno en Línea y Gobierno Digital.

Fuente: Gobierno Digital.

La estrategia emprende una serie de políticas destinadas a mejorar la calidad TI en todos sus aspectos, entre ellos el de la seguridad de la información. En la tabla 8 y 9 se pueden observar los cambios en la estructura de Gobierno en Línea y Gobierno Digital.

Tabla 8. Componentes de Gobierno en Línea.

	Componentes
GOBIERNO EN LÍNEA	TIC para Gobierno Abierto
	TIC para Servicios
	TIC para la Gestión
	Seguridad y Privacidad de la Información

Fuente: Manual Estrategia de Gobierno en línea.

Tabla 9. *Componentes de Gobierno en Línea.*

GOBIERNO DIGITAL	***Componentes***
	TIC para el Estado
	TIC para la Sociedad
	Habilitadores Transversales
	Arquitectura
	Seguridad y Privacidad
	Servicios Ciudadanos Digitales

Fuente: Manual de Gobierno Digital.

Como puede notarse, el componente de la seguridad y privacidad de la información, pasó a ser uno de los habilitadores transversales de Gobierno Digital, que tendrá la misma responsabilidad de conservar la confidencialidad, integridad y disponibilidad de los activos de información de las entidades del estado, garantizando su buen uso y la privacidad de los datos[25].

En la Tabla 10 podemos encontrar los subcomponentes y criterios de la seguridad y privacidad de la información, que en conjunto con los sistemas de protección que se mencionarán más adelante, pueden forjar un gran mecanismo de seguridad eficiente contra la ingeniería social y las demás amenazas de la información.

Tabla 10. Subcomponentes y criterios de la Seguridad y Privacidad.

	Subcomponentes	***Criterios***
SEGURIDAD Y PRIVACIDAD	Definición del marco de seguridad y privacidad de la información y de los sistemas de información	Diagnóstico de Seguridad y Privacidad
		Plan de Seguridad y Privacidad de la Información
	Implementación del plan de seguridad y privacidad de la información y de los sistemas de información	Gestión de riesgos de seguridad y privacidad de la información
	Monitoreo y mejoramiento continuo	Evaluación del desempeño

Fuente: Manual Estrategia de Gobierno en línea.

[25] Basado en la lectura de: Manual de Gobierno Digital. Disponible en: http://mintic.gov.co/portal/604/articles-61775_recurso_2.pdf

14.2 CAPACITACIONES

El primer y más importante método que se debe implementar es la capacitación y educación de los usuarios, si los usuarios desconocen en su gran mayoría los tipos de ataques a los que pueden estar expuestos, entonces no podrán evitarlos. Dentro de la recomendación más importante a impartirles es que no deben dar información sin antes contar con la autorización de la persona que lo puede facultar. Dentro de las capacitaciones hay que ser lo más claro posibles con los usuarios demostrándoles que los correos electrónicos con una apariencia y presentación muy profesional, pueden incluir direcciones de correo electrónico falsas de empresas legítimas o presentaciones aparentemente inocentes.

14.3 POLÍTICAS DE SEGURIDAD

Aunque la mayoría de las entidades poseen una estructura de políticas de seguridad básica, se debe añadir a la política de seguridad otros parámetros más específicos como la prohibición del uso de las redes sociales en los equipos de las alcaldías, además de concientizar a las personas de establecer seguridad en sus perfiles para que no todo el mundo tenga acceso a su información personal.

14.4 TOKENS

Se recomienda reforzar la seguridad el manejo de dinero que se mueve por las cuentas de las alcaldías en las dependencias de secretaría de hacienda o tesorería municipal, solicitando a las entidades bancarias el uso de tokens, dispositivos de seguridad y el reporte de transacciones, pues en otras alcaldías del país se han presentado robos millonarios mediante el robo de contraseñas de las cuentas de los responsables de las mismas.

14.5 ACTUALIZACIÓN

Para poder llevar acciones preventivas, tanto aplicaciones de software como los mismos administradores de los sistemas, deben actualizase. El personal administrativo debe capacitarse por lo menos una vez cada 6 meses acerca de nuevas alertas de amenazas, así como reconocer las acciones preventivas y correctivas cuando se presente un caso. Se recomienda mejorar las estrategias de seguridad, enfocándose en acciones como las actualizaciones continuas de los

servidores, los programas antivirus, los detectores de intrusos y la implementación de herramientas de control de la red.

14.6 SOFTWARE DE SEGURIDAD

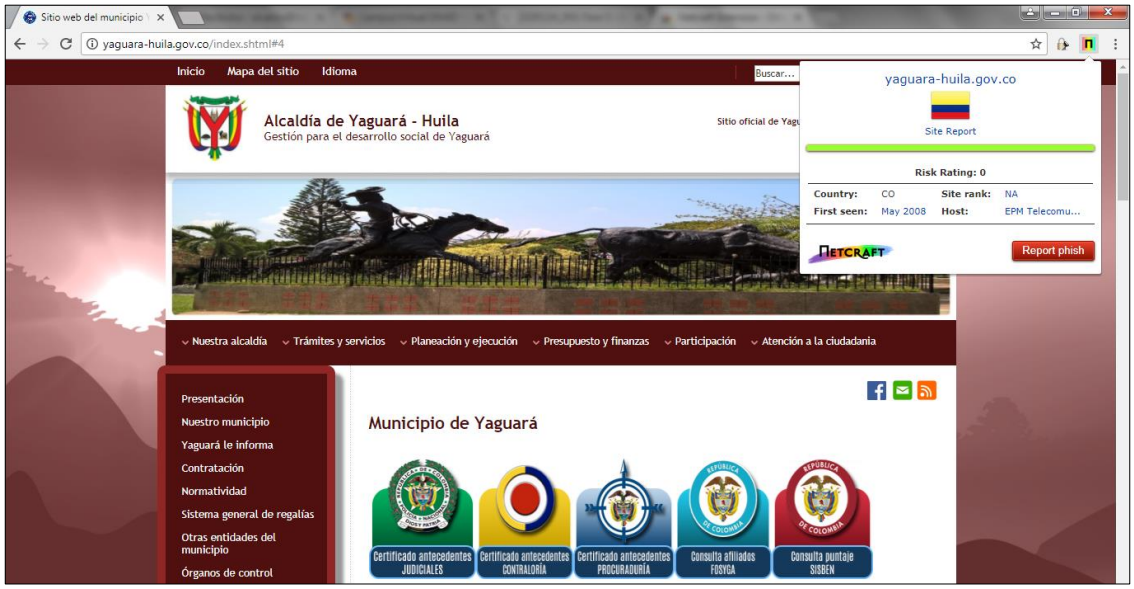
Para poder proteger completamente contra los nuevos ataques y amenazas en la red un programa antivirus no es suficiente. Se recomienda realizar una valoración para lograr escoger e implementar un paquete de seguridad que pueda ofrecer protección contra ataques de Ingeniería Social y que también detengan el *malware*, *spyware*, *spam*, y *phishing*, sin que este logre llegar a los equipos de los usuarios, que brinden control a dispositivos *USB*, detección de amenazas basado en la nube, que muestre un riesgo vs reputación de las aplicaciones, y evite que *plugins* se descarguen o ejecuten.

Existen herramientas que además pueden ayudar en este sentido y lograr prevenir ataques por phishing en estas entidades.

14.7 NETCRAFT

Se puede descargar como una extensión tanto de *Chrome* como *Mozilla*, http://toolbar.netcraft.com/, funciona mediante alertas realizadas por la comunidad mundial de usuarios y verificadas por *Netcraft*, acerca de direcciones y correos fraudulentos de esta manera al acceder a una *URL* reportada o recibir un correo, esta extensión podrá verificar si es phishing al hacer clic en el icono al lado derecho de la barra de direcciones. Figura 52.

Figura 53. Netcraft.



Fuente: el autor.

Se debe entonces, capacitar a los empleados en el uso de esta herramienta, así podrán identificar de una manera más concreta si las direcciones a las que entran son legítimas. Además, es una herramienta libre y sin costo alguno.

14.8 COPIAS DE SEGURIDAD

Implementar sistemas para prevenir pérdida de datos, como copias de seguridad en dispositivos de almacenamiento extraíbles seguros y en la nube, donde se identifique la información sensible, la proteja de pérdidas y además pueda controlar su uso. Revisar semanalmente que los sistemas de respaldo estén funcionando correctamente y que la información respaldada cumpla con la integridad. Igualmente, esta copia de respaldo de información debe encontrarse alojada en un sistema diferente, pues si algunos tipos de ransomware pueden encriptar las copias de seguridad.

14.9 SYMANTEC DATA LOSS PREVENTION

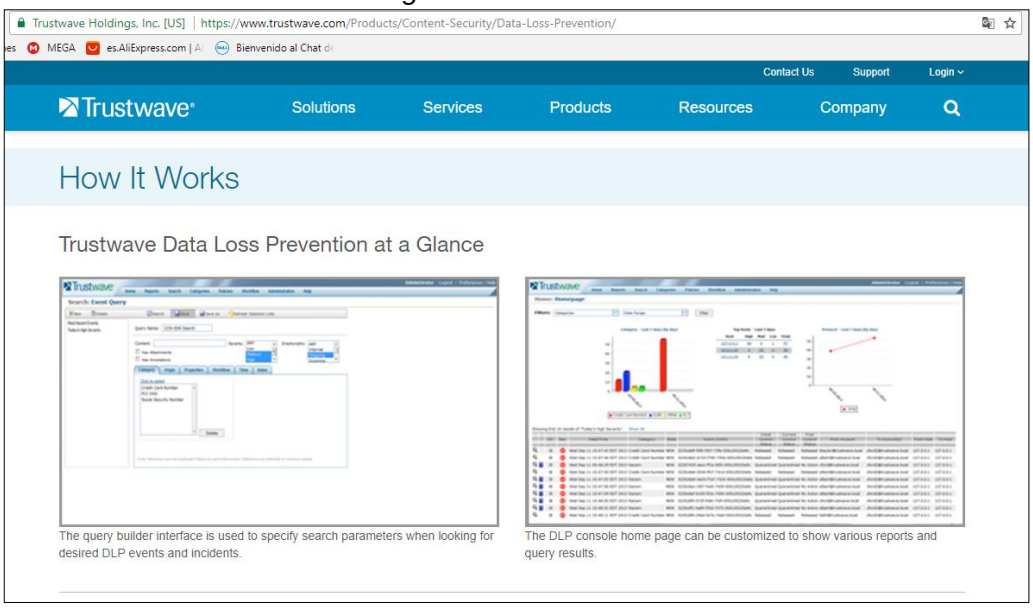
Symantec DLP utiliza una combinación de tecnologías avanzadas para detectar con precisión datos confidenciales, ya sea en reposo o en movimiento, e incluye una variedad de políticas listas para usar para ayudar a habilitar el cumplimiento de las mismas. Además, cuenta con una función de clasificación de datos que

identifica los archivos etiquetados como sensibles por los usuarios a través de *Symantec Information Centric Tagging*, para evitar su pérdida por cualquier motivo. La desventaja es su costo.

14.10 TRUSTWAVE DATA LOSS PREVENTION

Proporciona a las organizaciones las herramientas que necesitan para descubrir, controlar y proteger los datos mientras cumplen con las regulaciones internas y externas. El análisis juega un papel importante en esta plataforma. *Trustwave* supervisará todos los documentos y anexos basados en la web que ingresen a las alcaldías, incluidos correos electrónicos, *blogs* y publicaciones en redes sociales, figura 53. Se analizan para detectar violaciones de las políticas de seguridad. El sistema bloqueará automáticamente cualquier violación, manteniendo los datos seguros.
La ventaja es que tiene una versión demo para probar y comprobar si se adapta a las necesidades para después adquirir la licencia.
https://www.trustwave.com/Products/Content-Security/Data-Loss-Prevention/

Figura 54. Trustwave.



Fuente: el autor.

14.11 DISPOSITIVOS EXTRAÍBLES

Establecer normas en las políticas de seguridad, que tomen las medidas necesarias con el buen uso de los medios extraíbles, como su análisis, restricción de copias a información confidencial y mediante *logs* monitorear las acciones que se realizan con los mismos.

14.12 CONTRASEÑAS

Aplicar la política del uso correcto de las contraseñas, están deben ser seguras contener de 8 a 10 caracteres alfanuméricos y símbolos, prohibir su intercambio, el cambio cada 6 meses, y que no se apunten en papel o elementos de fácil acceso para otros. Crear y difundir una política de seguridad en específica que promueva el buen uso de contraseñas.

14.13 CÁMARAS DE SEGURIDAD

Aunque actualmente es un recurso opcional para las entidades, es recomendado utilizar un sistema de vigilancia por cámaras de seguridad, que servirá para esclarecer algún hecho o incidente que haya ocurrido. Además, puede significar un tanto en la decisión de un ingeniero social, ya que, al ver las cámaras de seguridad, lo pensará dos veces antes de realizar algún acto.

14.14 SEGURIDAD EN ACCESOS FÍSICOS

Ya sea por una persona contratada para vigilar y controlar los accesos a oficinas, o un sistema de acceso como el biométrico, es necesario implementar reglas y controles de acceso para restringir y controlar los espacios que ingenieros sociales podrían aprovechar.

15 CONCLUSIONES

Mediante la realización de esta monografía se logró investigar los métodos más comunes y eficaces que se practican en la Ingeniería Social, dándose a conocer a los funcionarios de las alcaldías del Huila, las maneras apropiadas para contrarrestar estas amenazas en los sistemas de información.

Se pudo indagar diferentes fuentes bibliográficas y de esta manera lograr reconocer la terminología y conceptos relacionados de la ingeniería social, estableciendo también algunos antecedentes y hechos relacionados en Colombia y el mundo.

Por medio de encuestas, observación directa, evidencia fotográfica e indagación en diferentes alcaldías del Huila, se pudo determinar los métodos más frecuentes de la Ingeniería Social y la manera como se han presentado, destacando los más comunes y que han tenido incidencia afectando a estas entidades.

Igualmente se estableció que uno de los problemas más evidentes aparte de la capacitación es el tema de seguridad, pues ninguna alcaldía cuanta con un control de acceso físico estricto a las instalaciones. Es de notar que también muchas de las oficinas no se encuentran bien diseñadas lo que puede permitir ataques de Ingeniería social como escuchar sobre el hombro, o detrás las divisiones o puertas. También se encuentra que hay un mal manejo con respecto a las basuras pues no se destruye de manera adecuada.

Con base en la información obtenida y teniendo en cuenta los métodos que existen en la actualidad para lograr minimizar el riesgo de un ataque por Ingeniería Social, se establecieron una serie de métodos funcionales que van a permitir sensibilizar y concientizar a los funcionarios en las diferentes alcaldías del Huila, de la importancia de la capacitación y buen uso de los activos que tienen a su cargo.

Las alcaldías visitadas no se encuentran lo suficientemente preparadas para enfrentar la materialización de un ataque por Ingeniería Social de gran consecuencia, como ha ocurrido en otras partes del país, donde han logrado robar gran cantidad de recursos utilizando estos métodos. Esto tendría grandes consecuencias legales, de ahí la importancia de la aplicación de los métodos sugeridos.

16 DIVULGACIÓN

La divulgación de esta monografía se llevará a cabo una vez se dé la aprobación de los jurados de la Especialización de Seguridad Informática de la UNAD, y se hayan completado las correcciones pertinentes.

Se deberá socializar en la alcaldía del municipio priorizado donde se realizaron las pruebas, para una vez aprobada, pueda presentarse a las demás alcaldías.

De igual manera se subirá al repositorio de la UNAD en donde la monografía podrá ser consultada y revisada por la comunidad académica y al público en general.

17 BIBLIOGRAFÍA

CONHEADY, Sharon. Social Engineering in IT Security: Tools, Tactics, and Techniques: Testing Tools, Tactics & Techniques. Ed. McGraw Hill Professional, 2014. Pg. 272. ISBN 0071818472.

HADNAGY, Christopher. Social Engineering: The Art of Human Hacking. Ed. Illustrated, Publisher John Wiley & Sons, 2010. Pg. 416. ISBN 1118029712, 9781118029718.

LONG, Johnny. No Tech Hacking: A Guide to Social Engineering, Dumpster Diving, and Shoulder Surfing. Ed. Syngress, 2011. Pg. 384. ISBN 0080558755.

MANN, Lan. Hacking the Human: Social Engineering Techniques and Security Countermeasures. Ed. Gower Publishing, Ltd., 2012. Pg. 266. ISBN 1409458288.

MITNICK, Kevin D. SIMON, William L. The Art of Deception: Controlling the Human Element of Security. John Wiley & Sons, 2011. P. 368. ISBN 076453839X, 9780764538391.

SINGH PATEL, Rahul. Kali Linux Social Engineering. Ed. Packt Publishing Ltd, 2013. Pg 84. ISBN 1783283289, 9781783283286.

WATSON, Gavin. MASON, Andrew. ACKROYD, Richard. Social Engineering Penetration Testing: Executing Social Engineering Pen Tests, Assessments and Defense. Ed. Syngress, 2014. Pg. 390. ISBN 0124201822.

ZORZ, Mirko. The life of a social engineer: Hacking the human [en línea], 19 de Mayo de 2016. Disponible en Internet: https://www.helpnetsecurity.com/2016/05/19/social-engineer/

EDITOR. WeLiveSecurity. Cinco cosas que debes saber sobre la Ingeniería Socia [en línea], 06 de junio de 2016. Disponible en Internet: https://www.welivesecurity.com/la-es/2016/01/06/5-cosas-sobre-ingenieria-social/

LONDOÑO, César Jaramillo. La Ingeniería Social: Un Desafío Investigativo [en línea], 01 de octubre de 2012. Disponible en Internet: http://publicaciones.eafit.edu.co/index.php/revista-universidad-eafit/article/viewFile/1175/1062

GONZÁLEZ JUÁREZ, Diego Dante. PEÑA ENRÍQUEZ, José Antonio. Estudio del impacto de la Ingeniería Social – Phishing [en línea], 2012. Disponible en Internet: http://www.ptolomeo.unam.mx:8080/xmlui/bitstream/handle/132.248.52.100/2730/Tesis.pdf?sequence=1

TIWARI, Aditya. Fossbytes. What Is Social Engineering? What Are Different Types Of Social Engineering Attacks? [en línea], 28 de febrero de 2017. Disponible en Internet: https://fossbytes.com/what-is-social-engineering-types-techniques/

FLORES, Hernández. BELÉN URRUTIA, Geovanna. GREGORIO, Franco José. Ingeniería Social a través de medios informáticos, análisis de las posibles amenazas existentes en la facultad de ciencias administrativas de la Universidad de Guayaquil [en línea], diciembre de 2015. Disponible en Internet: http://repositorio.ug.edu.ec/bitstream/redug/10741/1/tesis_Ingenieria%20social%20a%20traves%20de%20medios%20informaticos%2C%20analisis%20de%20las%20posibles%20amenazas%20existe.pdf

KEREKI GUERRERO, Inés Friss. Modelo para la Creación de Entornos de Aprendizaje basados en técnicas de Gestión del Conocimiento [en línea], diciembre de 2003. Disponible en Internet: http://www.ort.edu.uy/fi/pdf/Tesis.pdf

MORALES, José André. Ingeniería Social [en línea], 2014. Disponible en: https://cybercamp.es/cybercamp2014/attachments/multimedia/CyberCamp_IngenieriaSocial.pdf

SÁNCHEZ 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 [en línea], Julio de 2011. Disponible en: http://dspace.ups.edu.ec/bitstream/123456789/3349/1/UPS-CT002088.pdf

COLOMBIA, Ministerio de Tecnologías de la Información y Comunicaciones. 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" [en línea], 04 de enero de 2017. Disponible en Internet: http://www.mintic.gov.co/portal/604/w3-article-3705.html

COLOMBIA, Ministerio de Tecnologías de la Información y Comunicaciones. Ley 1273 de 2009. Ley 1341 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 del Espectro y se dictan otras disposiciones" [en línea], 03 de mayo de 2017. Disponible en Internet: http://www.mintic.gov.co/portal/604/w3-article-3707.html

COLOMBIA, Congreso de la República. Ley estatutaria 1266 de 2008 [en línea], 31 de diciembre de 2008 [revisado 11 de septiembre de 2017]. Disponible en Internet: http://www.secretariasenado.gov.co/senado/basedoc/ley_1266_2008.html

SALAZAR, Natalia. GONZÁLEZ, Marcela. “Phishing”: La Automatización de la Ingeniería Social [en línea], octubre de 2007. Disponible en Internet:

https://repository.eafit.edu.co/bitstream/handle/10784/2443/salazar_natalia_2007.pdf?sequence=1

OWASP, Education Project. Ingeniería social [en línea], 2007. Disponible en Internet: http://osl.ugr.es/descargas/OWAND11/OWAND11%20Granada%20-%20Ingenier%C3%ADa%20social.pdf

OWASP. Ingeniería Social: Hacking Psicológico [en línea], 2016. Disponible en Internet: https://www.owasp.org/images/2/27/02_INGENIER%C3%8DA_SOCIAL.pdf

MUSSETTA, Paula. Estado e ingeniería social. Particularidades y dimensiones morales de un programa para la resolución de conflictos [en línea], agosto de 2009. Disponible en Internet: http://148.202.18.157/sitios/publicacionesite/pperiod/espiral/espiralpdf/espiral45/estado2.pdf

MINTIC. Seguridad y privacidad de la información [en línea], 03 de mayo de 2017. Disponible en Internet: https://www.mintic.gov.co/gestionti/615/articles-5482_G3_Procedimiento_de_Seguridad.pdf

ARCOS, Sergio. Ingeniería social: Psicología aplicada a la seguridad informática [en línea], 01 de junio de 2011. Disponible en Internet: http://upcommons.upc.edu/bitstream/handle/2099.1/12289/73827.pdf?sequence=1