IMPLEMENTACION DE TECNICAS DE INGENIERIA SOCIAL EN LA INSTITUCION EDUCATIVA TECNICA DE PANQUEBA

WILLIAM JAVIER CORDERO SALCEDO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BASICAS TECNOLOGIA E INGENIERIA
ESPECIALIZACION EN SEGURIDAD INFORMATICA
MALAGA - SANTANDER
2018

MPLEMENTACION DE TECNICAS DE INGENIERIA SOCIAL EN LA INSTITUCION EDUCATIVA TECNICA DE PANQUEBA

WILLIAM JAVIER CORDERO SALCEDO

Proyecto de grado Aplicado para optar el título de
Especialista en Seguridad Informática

Directora de Proyecto
Ing. Yina Alexandra González Sanabria

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BASICAS TECNOLOGIA E INGENIERIA
ESPECIALIZACION EN SEGURIDAD INFORMATICA
MALAGA - SANTANDER
2018

Nota de aceptación:

_____

_____

_____

_____

Firma del presidente del jurado

_____

Firma del jurado

_____

Firma del jurado

Málaga, 4 de Diciembre de 2018

AGRADECIMIENTOS

Agradezco a Dios, quien es el todo poderoso que nos permite llevar a cabo cada objetivo que nos proponemos día a día iluminando nuestros pasos y guiándonos por el camino correcto.

También a mis familiares que han hecho parte con su apoyo y motivación en mi proceso de formación durante este año.

Y a la Universidad Abierta y a Distancia por permitirme formar y afianzar mis conocimientos con el diario vivir aplicando ética profesional por medio de su estrategia de investigación, también por las actividades basadas en problemas para resolver y así mejorar mi perfil profesional en busca de brindar apoyo a la sociedad en los temas de seguridad informática.

CONTENIDO

pág.

LISTA DE TABLAS

pág.

LISTA DE FIGURAS

pág.

LISTA DE GRAFICAS

pág.

LISTA DE ANEXOS

pág.

INTRODUCCIÓN

Este proyecto tiene como finalidad usar técnicas de Ingeniería Social para analizar el nivel de seguridad de la información que se maneja en el Colegio Técnico de Panqueba del Departamento de Boyacá en sus diferentes dependencias que tienen acceso a sistemas de información, con esta idea de diagnosticar lo que se busca es tomar la información recopilada sobre el estado actual, las falencias, amenazas, revisión de los activos como la parte física hardware y del software, analizar la infraestructura de la red y plantear estrategias de Ingeniería Social a los funcionarios que garanticen el respaldo y seguridad de la información.

La información actualmente es identificada hoy en día como el activo más valioso dentro cualquier entidad ya que dando buen uso de esta se puede garantizar la confiabilidad de los recursos y demás actividades que a diario se llevan a cabo en el interior buscando el bien común.

El avance tecnológico cuenta con beneficios, pero también trae sucesos negativos y más aún cuando se ve hoy en día que seres humanos han desarrollado una serie de técnicas o métodos encaminados a obtener beneficios ilegítimos en función de la ingenuidad, necesidad, avaricia o compasión de las personas en situaciones específicas sin medir las consecuencias que aplica la ley en estos casos.

Por esta razón es necesario que los usuarios de la Entidad Educativa de Panqueba que manejan información, identifiquen la importancia de darle el uso adecuado y por medio de esta investigación se detecten vulnerabilidades que permitan hacer caer cuenta de los errores y falencias que se tienen y así por medio de estrategias y buenas prácticas se reduzcan los riesgos y se garantice la total seguridad de los datos en pro del éxito de la entidad y del bien común.

1. DEFINICIÓN DEL PROBLEMA

1.1 DESCRIPCION DEL PROBLEMA

En la actualidad una buena parte de las Instituciones Educativas del departamento de Boyacá se apoyan en el uso de las TIC para realizar aquellas actividades que a diario se gestionan en su entorno laboral con el fin de cumplir a cabalidad todas sus funciones como ente educativo.

Las entidades educativas tienen como propósito implementar sistemas de seguridad para proteger recursos y activos informáticos por medio de mecanismos de seguridad en sus sistemas de información en la búsqueda de evitar errores y mal funcionamiento en los procesos, retraso de las actividades y pérdidas de dinero, credibilidad del buen nombre de la Institución Educativa y obtener mayor rendimiento en la ejecución de sus procesos.

La Institución Técnica de Panqueba en sus procesos informáticos se encuentra en vulnerabilidad de perder información ya que nunca se han tenido en cuenta procesos al momento de proteger la información; estas vulnerabilidades deben ser analizadas y revisadas por medio de un diagnostico como se plantea en uno de los objetivos para que por medio de las distintas metodologías de Ingeniería Social se defina qué medidas de control se debe tomar para minimizar los riesgos inminentes que representen estas fallas.

Con esto se establece dejar como evidencia final a los usuarios un manual de políticas de seguridad y recomendaciones implementando estrategias de prevención de delitos informáticos e Ingeniería social y así fomentar cultura social y educativa.

1.2 FORMULACIÓN DEL PROBLEMA

¿Con qué técnicas de Ingeniería Social se puede verificar el nivel de seguridad de la información en la Institución Educativa Técnica de Panqueba?

2. JUSTIFICACIÓN

Teniendo en cuenta que la Institución no cuenta con personal que dé solución a inconvenientes informáticos, o que genere estrategias de seguridad de la Información se define que la mejor solución es partir desde el análisis de riesgo de la información para detectar las amenazas o vulnerabilidades a las que está expuesta la entidad y así implementar estrategias de mejora y recomendaciones de seguridad que impacten en la disminución de los ataques a la información y así dar cumplimiento a las metas propuestas por la entidad para cumplir sus objetivos como ente educador.

Con este proyecto se busca determinar vulnerabilidades y falencias que afectan la seguridad y privacidad de la información con la que cuenta el Colegio en los diversos servicios que presta mediante el proceso de Ingeniería Social que permite el uso de técnicas que resultan la gran mayoría de veces inocentes aprovechando la ingenuidad o ganando la confianza de una persona para obtener la información sin que se den cuenta con qué fin se hace.

El resultado final tras aplicar técnicas de Ingeniería Social es dejar en los usuarios un manual de seguridad y recomendaciones implementando estrategias de prevención de delitos informáticos e Ingeniería Social y así dar solución a los riesgos encontrados en los procesos y recursos que cuentan con información sensible para el Colegio, permitiendo usar estrategias y así generar cultura en las personas por medio de capacitaciones que concienticen el personal en el uso adecuado de los recursos tecnológicos que garanticen la seguridad de la información.

3. OBJETIVOS DE PROYECTO

3.1 OBJETIVO GENERAL

Realizar una implementación en el área de Seguridad Informática aplicando metodologías de Ingeniería Social en la Institución Educativa Técnica de Panqueba (Boyacá).

3.2 OBJETIVOS ESPECÍFICOS

1. Levantar la información de las metodologías de Ingeniería Social que garanticen seguridad y privacidad de la información en la Institución.

2. Determinar las metodologías de Ingeniería social para aplicar al personal que usa equipos de cómputo en la Institución Educativa.

3. Aplicar técnicas y metodologías de Ingeniería Social a los servidores públicos de la Institución Educativa Técnica de Panqueba.

4. Generar un manual de seguridad con las recomendaciones para evitar ser víctima de Ingeniería Social implementando estrategias de prevención de delitos informáticos y así fomentar cultura social y educativa.

4. ALCANCE Y DELIMITACIÓN DEL PROYECTO

Como alcance se tiene establecer estrategias en el ámbito informático que busquen dar solución a la serie de falencias que se encuentran en el manejo de la información y así no estar expuestos a la pérdida o modificación de los datos por no conocer las vulnerabilidades y no dar buen manejo a la Ingeniería social que se encarga de aprovecharse de aquellos usuarios que de una forma tan simple y fácil dan datos ya sea por medio de alertas al teléfono móvil, mensajes curiosos al correo o sencillamente mediante el uso de Internet entre muchas que existen.

Se aclara que en el desarrollo del proyecto no se incurrirá en conductas delictivas que infrinjan la ley 1273 de 2009 sobre la protección de la información y los datos y la ley 842 de 2003 que es la ley de ética del ingeniero.

En el proceso del desarrollo de las pruebas técnicas se van a crear cuentas de correo electrónico de ensayo y en ningún caso se atacaran sitios diferentes a los permitidos, ni se causaran daños ni perjuicios en infraestructuras o bienes ajenos ya que esta pruebas se llevaran a cabo en ambientes controlados. El procedimiento va dirigido a todo el personal desde capacitaciones hasta la entrega final del manual de políticas de seguridad y recomendaciones implementando estrategias de prevención de delitos informáticos e Ingeniería social y así fomentar cultura social y educativa.

La Identidad Educativa cuenta con:

- Información almacenada en la nube.
- Base de datos en el área de trámites de secretaria.
- Aplicaciones web que llevan una información a diario de los estudiantes como:
- Notas de las materias.
- Registro de Inasistencias.
- Anotaciones en el observador de alumnos.
- Enlaces desde la página web institucional para acceder a lugares o fechas de actividades programadas tanto en la Institución como en la comunidad.

Como actividades iniciales que no están incluidas dentro de los objetivos se realizara la identificación de activos y análisis de riesgos que se localizan en el contexto de acceso y administración de la red, identificando activos para determinar sus vulnerabilidades y así al final poder realizar una serie de recomendaciones que permitan mitigar los riesgos hallados en el manejo de la Información del Colegio Técnico de Panqueba y así bloquear cualquier acceso que alguien desee hacer y que permita la confiabilidad y privacidad de la información dejando todo explicado en capacitaciones, practicas reales y manual de políticas de seguridad para los usuarios.

4.1 DATOS DE LA ENTIDAD

Figura 1. Fachada Colegio Técnico de Panqueba

Fuente: El Autor

Nombre:	Institución Educativa Técnica de Panqueba.
NIT:	826002642-4
Dirección:	Carrera 5 No. 4-79 Panqueba- Boyacá
Teléfono:	7881979
Email:	panqueb_coltecpanqueba@sedboyaca.gov.co

4.1 MISION

Somos un Colegio Oficial en búsqueda de satisfacer efectiva y competitivamente el deseo auténtico de la persona por el conocimiento, incentivar el afecto por el saber,

desarrollar la alta inteligencia y vivir los valores humano-cristianos, que le permitan transformarse y transformar su realidad. [1]

4.3 VISION

En el año 2018 el Colegio Técnico de Panqueba consolidará su proceso como Institución Educativa con reconocimiento nacional, que acoge la diversidad general, será líder en la formación integral de jóvenes que se caractericen por sus valores éticos que les permitan estar a la vanguardia en lo cultural, social, político y tecnológico para que sean agentes de cambio en un mundo globalizado. [2]

4.4 POLITICA DE CALIDAD

El Colegio Técnico de Panqueba tiene basada su política de calidad como parte de su filosofía en satisfacer efectiva y competitivamente el deseo auténtico de la persona por el conocimiento, el afecto por el saber, el desarrollo de la alta inteligencia y la vivencia de los valores cristianos, apoyados en un equipo humano competente y respaldado en nuevas tecnologías, que lo impulsan a mejorar continuamente y a ser líder en la prestación del servicio. [1]

4.5 ORGANIGRAMA DEL COLEGIO

Figura 2. Organigrama Institucional

Fuente: https://colpanqueba.jimdo.com/

[1] Tomado textualmente de: https://colpanqueba.jimdo.com/mision/

[2] Tomado textualmente de: https://colpanqueba.jimdo.com/vision/

5. MARCO REFERENCIAL

5.1 ANTECEDENTES

Este tema del proyecto es de mucha relevancia en la actualidad ya que toda entidad pequeña, mediana o grande acude a buscar este tipo de diagnóstico con el fin de solventar y evitar problemas con lo referente al entorno de la seguridad de la información.

En la búsqueda de investigaciones para el área de seguridad informática en cuanto a proyectos de grado que se relacionan con el tema en empresas específicas y también en entidades educativas, los ejemplos están en la Universidad Católica de Pereira que desarrollo su política de seguridad a partir de un trabajo de grado, también se encuentran la elaboración de políticas de seguridad para organizaciones como Apostar, de igual manera el CDA de Cartago y en general mucha documentación sobre el tema y sobre los diferentes métodos de detección y ataques a sistemas informáticos. [3]

La inconsistencia de este tipo de proyectos es que a su vez no se encuentra en el momento una persona encargada que sirva de guía para revisar lo relacionado con la seguridad y a partir de allí generar recomendaciones que sirvan para concientizar la importancia de implementar estrategias que generen un ambiente confiable en la manipulación de los sistemas informáticos.

5.2 MARCO TEÓRICO

El eje primordial de toda entidad es el ser humano, que es quien controla, sabe, maneja y procesa la información y en cierta parte de él depende de que se garantice tranquilidad en el acceso a los sistemas informáticos.

5.2.1 Pilares de la Información. Dentro del contexto de la seguridad informática actualmente abarca mecanismos tanto de prevención como de corrección que utilizan las personas y las empresas de hoy para proteger su mayor tesoro “la información”, para esto se debe tener en cuenta los 4 pilares elementales que conlleva a que la información sea proteja a un nivel adecuado.

[3] Tomado textualmente de: https://es.slideshare.net/evilbyteperu/tesis-ingenieria-social

La figura 3 muestra los 4 pilares que se explican a continuación con su respectiva recomendación que se debe tener:

Figura 3. Pilares de la información

Fuente:http://recursostic.educacion.es/observatorio/web/images/upload/elvira_mifsud/Introduccion_seguridad_html_6045ac9b.png

- 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.

- Integridad: Hace referencia a cuando la información no es borrada, copiada o modificada, es decir cuando se conserva tal como el propio actor la creo, para esto se usa uno de los mecanismos más utilizados para asegurar la integridad de la información que es a través de firmas digitales.

- Disponibilidad: Es cuando la información que se tenga en cualquier medio digital o software se encuentra disponible para compartirla, para este tipo de ataque los controles de seguridad es evitar los intrusos por medio del uso de firewall como barreras de seguridad lógicas y físicas, que eviten cualquier daño malintencionado que proviene de extraños.

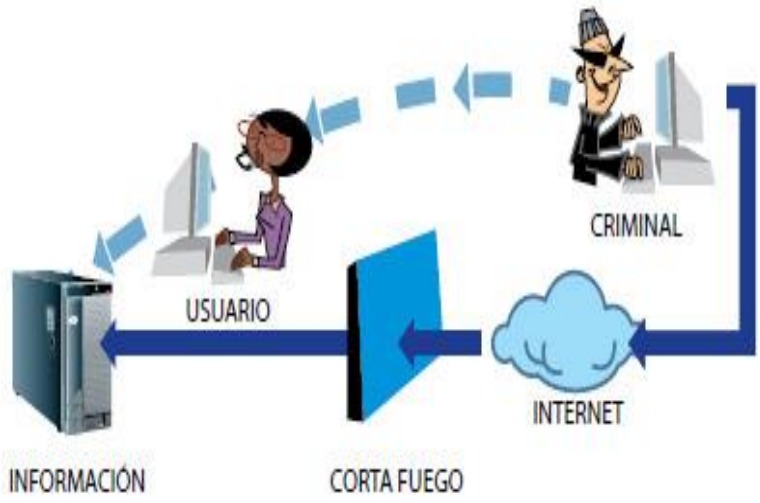
- Autenticidad: Es la forma como debe quedar la información ya que es única y no debe ser interceptada y copiada de forma que uno pierda los derechos de autor por parte del atacante.

5.2.2 Ingeniería Social. Ingeniería social es la técnica de hackeo que se usa para obtener información de otras personas teniendo como estrategia la interacción social, las personas víctimas de estos ataques no se dan cuenta de que forma entregan los datos necesarios para ser vulnerados y atacados en sus sistemas informáticos.

Una opción que se tiene en el mundo informático para evitar ser víctima de ataques es poner en práctica la Ingeniería Social por medio de capacitaciones a empleados para enseñarlos a usar o utilizar el sentido común y no caer en preguntas tontas o mensajes curiosos que lo único que buscan es filtrar información.

En la figura 4 se muestra como puede ser un método que usa un ciberdelincuente informático para obtener datos así este sistema cuente con un *firewall* de seguridad ya que el delincuente informático interactúa directamente con la víctima obteniendo información concreta.

Figura 4. Interacción de una técnica de Ingeniería Social



Fuente: The GBM Journal

Como estrategias iniciales que pueden usarse en toda entidad para ayudar a evitar ser una víctima más de este tipo de ataques se puede tener en cuenta:

- No decir o escribir por celular o correo datos personales y confidenciales como claves de acceso, cuentas bancarias, números de tarjetas de crédito, etc., debido a que ninguna entidad de estas hace ese tipo de solicitud.

- No ingresar o dar clic a los enlaces de una página web que lleguen por medio de correo electrónico en el que le soliciten datos personales.

- Desconfiar de cualquier tipo mensaje que ofrezca la oportunidad de ganar dinero de una forma rápida y fácil.

- Cuando arroje a la basura papelería de la entidad por favor revisar que no vayan registradas datos de la entidad como claves, usuarios, números telefónicos o cualquier otro tipo de pistas porque los expertos en ingeniería social se valen de este tipo de táctica para lograr a organizar ideas para captar información.

- Instalar un Antivirus complejo y recomendable que incluya una funcionalidad antispyware y antimalware para minimizar riesgos que generen daños y pérdida de información.

- Utilizar el sentido común, es decir cada vez que se reciba una llamada o mensaje sospechoso evitar entrar en detalle que comprometan la información.

5.2.3 Recomendaciones de Seguridad. Este ítem es muy fundamental que se aplique en toda organización o de forma personal ya que si se cuenta con estas podrá estar tranquilo de que la privacidad de su información está garantizada, a continuación se resume las buenas prácticas que se debe tener para fortalecer la seguridad informática desde diferentes frentes.

5.2.3.1 Seguridad con el equipo. El equipo de cómputo es de uso personal pero en algunas empresas se determinan varios cargos para el mismo equipo, cada persona debe cumplir con las políticas de seguridad que se establezcan que garantice la confiabilidad de la información, para esto se debe tener en cuenta las siguientes recomendaciones:

- Tener instalado un sistema operativo y sus aplicaciones con licencia mas no descargadas de internet.

- Instalar un Antivirus recomendablemente con licencia, kasperksy o Bit defender son según estadísticas los que cumplen con mayor nivel de seguridad.

- Instalar un Firewall que permita restringir accesos no autorizados de Internet.

- Instalar software anti-spyware, para evitar entrada de programas espías que buscan solo recopilar información confidencial.

- Generar contraseñas seguras es decir aquellas que tengan combinación de letras, números y símbolos y que estas las modifique con frecuencia.

- Desactivar la opción autocompletado en formularios de internet.

- Se recomienda bloquear el computador en el momento en que se retire del puesto de trabajo para no dejar la tentación a la mano.

5.2.3.2 Seguridad en internet. El acceso a Internet es el *hobbie* día a día, pero a la vez es una de la debilidad que se tiene y para la cual se recomienda aplicar lo siguiente:

- No descargar ni ejecutar ficheros desde sitios sospechosos.

- Configurar el nivel de seguridad del navegador.

- Descargar los programas desde sitios oficiales no en web como softonic o *uptodown* que ofrecen una gama variada de software gratis.

- Eliminar las ventanas emergentes (pop-up) o configurar el navegador para evitarlas.

- Borrar todo lo que tiene que ver con *cookies*, ficheros temporales e historial de internet frecuentemente.

- Entrar a internet a páginas web seguras y de confianza, se pueden diferenciar viendo las que inician por https:// en lugar de http.

- Estar pendiente que en la barra del navegador web se vea un icono que representa un candado cerrado, en donde este identifica que se puede acceder a un certificado digital lo que garantiza la autenticidad de la página que se ingresa.

- Cuando se coloque contraseñas en otros equipos recomendable no darle que indique recordar contraseña.

5.2.3.3 Seguridad en el correo electrónico. Se debe tener en cuenta lo siguiente:

- No dar la cuenta de correo electrónico a desconocidos.
- Limitarse a no detallar el *spam* o correo no deseado.
- No responder a mensajes falsos o de promociones que llegan al email.
- Nunca responder correos en los que entidades bancarias o cualquier otra compañía de subastas o sitios de venta online le piden información ya que esa es una estrategia muy usada para capturar información. [7]
- No compartir información ni hacer publicaciones de eventos de donde trabaja ya que esto facilita el modo de actuar del atacante.

Con estas recomendaciones y las que se dejan al final en el manual lo que se busca es cumplir con los 4 pilares de la información como lo es confidencialidad, integridad, autenticidad y disponibilidad para así no tener dolores de cabeza en cuanto a pérdida de datos.

5.3 MARCO CONCEPTUAL

Entre las variables de seguridad a tener en cuenta en el proyecto se tienen los siguientes conceptos:

• Activos: Hace referencia a todo el entorno con que cuenta las entidades como lo es los sistemas de información, las redes, el personal, la infraestructura, el software, los servicios que se presta, entre otros.

• Amenazas: Acciones que ocasionan consecuencias negativas en el interior de la entidad, son muy comunes destacar como amenazas a las fallas, a los virus, a los ingresos no autorizados y los desastres ocasionados por fenómenos físicos o ambientales.

- Confidencialidad: Pilar de la información al que sólo puede tener acceso aquel sujeto de la empresa que tiene la autorización de hacerlo, es decir esta información no se puede revelar a otros, ni mucho menos ser pública, por lo que se debe proteger y así cumplir con la función de este pilar.

- Delito informático: Conducta ilícita que debe ser sancionada por el derecho penal, consiste en aquella acción indebida que se hace en cualquier medio informático para llevar acabo delitos comunes, conductas inapropiadas, falta de éticas con el fin de causar daños en la información.

- Ingeniería Social: Es la ciencia que usan aquellos individuos por medio de técnicas o tácticas que no necesitan sino de la astucia y de la inocencia de la víctima para poder obtener información valiosa.

- *Pretexting:* Técnica de Ingeniería Social usada por medio de pretextos ya sea por medio del uso del teléfono en llamadas o por chat donde haciendo uso de charlas claves se puede obtener datos concretos de alguna entidad.

- Riesgo: Es toda eventualidad que impide que se cumpla un objetivo, para lo cual se deben poner en práctica una serie de recomendaciones con el fin de mitigarlos.

- *Spoofing:* Técnica empleada por los ingenieros sociales con el fin de captar información habiendo suplantado algún sitio web el cual da a entender a la víctima que es algo legal.

- *Spam:* Son aquellos correos no deseados que en ocasiones traen incorporado código malicioso para afectar la seguridad en las personas y entornos laborales.

- Seguridad informática: Área encargada de proteger o salvaguardar la información o datos de los usuarios almacenados en un sistema informático.

- Vulnerabilidad: Son aquellas debilidades por las que se expone la información ya sea en intereses personales o en un entorno laboral.

5.4 MARCO LEGAL

Dentro del entorno de las leyes y normas que existen en la legislación colombiana y que se relacionada con seguridad informática se tienen en cuenta:

- *LEY 1273 DE 2009*

Cuando entro en vigencia la ley 1273 de 2009, nuestro país blinda en materia de seguridad de la información los delitos informáticos cometidos en Colombia, ya que estaba expuesta la privacidad, confidencialidad e integridad de los datos de los colombianos, ya que antes no se había tipificado sobre esta clase de delitos. [4]

A su vez el país entra hacer parte de los países con los más altos estándares para contrarrestar el delito informático. Colombia es el primer país de la región en penalizar los delitos informáticos, esta ley fue sancionada por el expresidente.

Aquí la ley establece que aquella persona que con objeto ilícito y sin tener autorización trafique, venda, diseñe, programe, desarrolle, ejecute y envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en una pena de prisión de 48 a 96 meses, y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con alguna pena más grave.

- *LEY 599 DE 2000*

Se estipula que los delitos que están consagrados en el Código Penal Colombiano, tienen plena aplicación bajo el entendido en que se cumplan las condiciones establecidas para aquellos actos criminales sin importar si se comete en medios electrónicos o tradicionales. [5]

[4] Tomado textualmente de: http://www.mintic.gov.co/portal/604/w3-article-3705.html

[5] Copiado textualmente de : https://www.policia.gov.co/denuncia-virtual/normatividad-delitos-informaticos

- *LEY 1266 DE 2008*

En esta ley se regula el manejo de la información de las bases de datos creadas a modo personal, en especial la comercial, financiera y crediticia de servicios y la proveniente de terceros países y se dictan otras disposiciones.

6. DISEÑO METODOLÓGICO

6.1 TIPO DE INVESTIGACIÓN

El ámbito de este proyecto basado en una investigación aplicada que busca determinar vulnerabilidades y amenazas que pueden afectar la información que maneja el Colegio en los diferentes servicios que presta lo cual permitirá identificar las principales falencias, mediante el proceso de Ingeniería Social.

6.2 METODOLOGIA APLICADA

El proceso a seguir que se incluye en el proyecto aplicado de Ingeniería Social se refleja en el siguiente esquema:

Las fases de recopilación de información y establecimiento de relaciones se llevaron a cabo mediante la observación y ejecución de la encuesta al plantel educativo, la tabulación de las preguntas con las respuestas permitieron sacar conclusiones para decidir algunas técnicas a aplicar.

En cuanto a las fases de explotación y análisis, se ejecutaron las pruebas de explotación y por otro analizar los resultados obtenidos para complementar las pruebas cuyo resultado no fue rápido de obtener como fue el proceso de *Spoofing* y pretexting.

Finalmente los resultados quedan documentados de la siguiente forma:

- Respuestas de la encuesta ejecutada al plantel.
- Manual impreso sobre recomendaciones a seguir en cuanto a seguridad informática.
- Detalle fotográfico de las pruebas realizadas.
- Conclusiones.

6.3 HIPÓTESIS CONCEPTUAL

Tras la identificación de que en la actualidad una buena parte de las Instituciones Educativas del departamento de Boyacá se apoyan en el uso de las TIC para realizar actividades a diario que se gestionan en su entorno laboral con el fin de cumplir a cabalidad todas sus funciones como ente educativo, se tiene como propósito implementar sistemas de seguridad para proteger recursos y activos informáticos por medio de mecanismos de seguridad en sus sistemas de información en la búsqueda de evitar errores y mal funcionamiento en los procesos, retraso de las actividades, y pérdidas de dinero, credibilidad del buen nombre de la Institución Educativa y obtener mayor rendimiento en la ejecución de sus procesos.

La Institución Técnica de Panqueba en sus procesos informáticos se encuentra en vulnerabilidad de perder información ya que nunca se han tenido en cuenta procesos al momento de proteger la información; estas vulnerabilidades deben ser analizadas y revisadas por medio de un diagnostico como se plantea en uno de los objetivos para que por medio de las distintas metodologías de Ingeniería Social se defina qué medidas de control se debe tomar para minimizar los riesgos inminentes que representen estas fallas.

6.3.1 Variable, medida y dimensiones.

Dentro de las variables del proyecto tiene en cuenta la siguiente con su respectiva medida y sus dimensiones:

*Variable: Nivel de seguridad de la información en el Colegio.

*Medida: Correcta, alta, media, baja.

*Dimensiones:

1. Protección de los activos
2. Capacitación sobre seguridad informática
3. Ejecución de test prácticos sin infringir la ley
4. Recomendaciones sobre técnicas de Ingeniería Social

6.3.2 Hipótesis de la investigación (Hi). Existen técnicas de Ingeniería Social para poner en práctica en el Colegio y así determinar el nivel de seguridad de la información.

6.3.3 Hipótesis Nula (Ho). No existen técnicas de Ingeniería Social para poner en práctica en el Colegio y así determinar el nivel de seguridad de la información.

6.4 POBLACIÓN Y MUESTRA

- Población:

Rector, docentes encargado del área de Sistemas, Secretaria, Bibliotecaria y demás administrativos, docentes y estudiantes de la Institución Técnica de Panqueba.

- Muestra:

Se realizó una encuesta al personal tanto docente como administrativo y a estudiantes de grado Once que diseñaron algunas bases de datos con el fin de identificar falencias y conocimientos en cuanto a la seguridad informática.

6.5 TÉCNICAS DE RECOLECCIÓN DE DATOS

De acuerdo a la metodología de investigación, en este proyecto se empleó lo siguiente:

- En cuanto a infraestructura

Listado de activos del Colegio

Identificar el tipo de vulnerabilidades, riesgos y amenazas

- Directas al personal:

Encuesta

Entrevistas donde usando técnicas de Ingeniería Social de modo pasivo “observando” y presenciales “por medio de llamadas y uso de chat”, además usando Ingeniería Social Inversa” se va a medir el nivel de confiabilidad que se tiene en el Colegio.

- Directas en el hardware disponible de la Institución.

Pruebas leves en equipos de cómputo sin infringir la ley con el permiso del encargado del área de sistemas del Colegio.

6.6 TÉCNICAS DE ANÁLISIS DE DATOS

El análisis de datos se realizó tabulando los resultados obtenidos según las técnicas de recolección a aplicar como la encuesta aplicada a todo aquella persona que tiene acceso a los equipos, base de datos, páginas web y enlaces de la institución.

También se hizo un análisis tras las pruebas que se hacen en equipos de la Institución.

7. ESQUEMA TEMATICO

Como parte inicial del proyecto y teniendo en cuenta que es lo primordial para saber con qué cuenta la entidad y que riesgos pueden haber se realizó dos tareas como lo fueron:

- Identificación de Activos y amenazas en el Colegio.

Este ítem ya recolectado se describe más adelante en el campo de productos esperados y resultados a entregar.

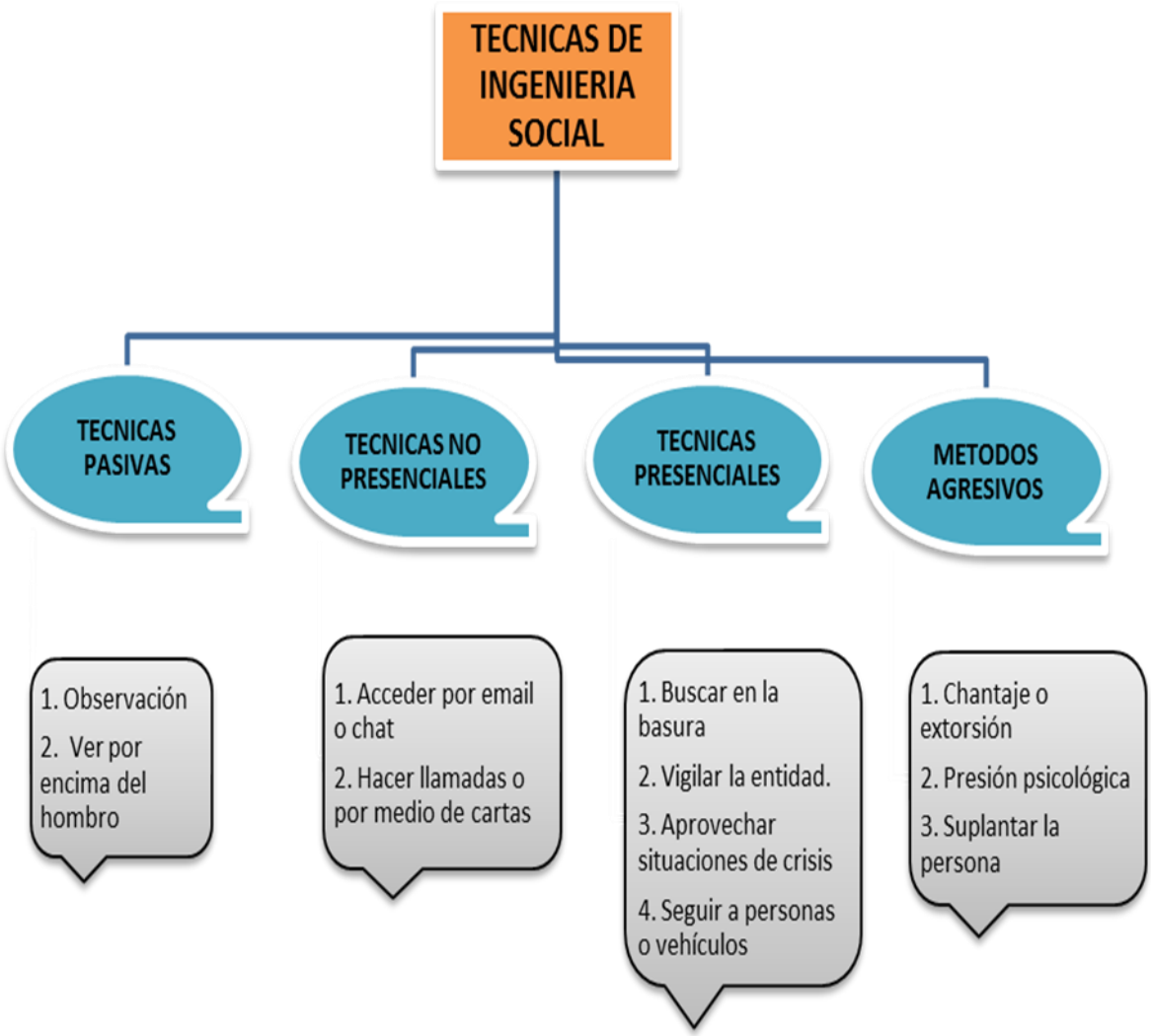
- Según el primer objetivo que es levantar la información de las metodologías de Ingeniería Social para aplicar en la Institución se realiza una investigación de las distintas estrategias y como se pueden aplicar en el proyecto para lograr identificar hasta donde es vulnerable la entidad.

7.1 INFORMACIÓN SOBRE METODOLOGÍAS DE INGENIERÍA SOCIAL

La Ingeniería Social es un término tecnológico actual muy usado ya que es el pan de cada día porque más seres humanos usan están técnicas con la finalidad de explotar las debilidades del otro y así tener acceso a una entidad o sistema de información para cumplir propósitos personales.

Algunas de estas técnicas que abundan en el ámbito informático se evidencian en la figura 5 que se muestra a continuación.

Figura 5. Técnicas de Ingeniería Social



Fuente: El Autor

7.1.1 Tips de ingeniería social. Según la experiencia de los más expertos en estos temas el ingeniero social utiliza una amplia variedad de tips para dar inicio a obtener acceso a la información confidencial desde familiarizarse con la victima hasta inventar situaciones en donde se ofrece a ayudar o solventar casos, esto aumenta ya que cada día más surgen nuevos métodos para romper la seguridad de la información.

A continuación se enumeran los 7 métodos más usados por los ingenieros sociales y los cuales se emplean en el desarrollo del Proyecto en la Institución Educativa de Panqueba.

1. Captura de información: Se utilizan varios métodos de confianza que animan a la gente a que comparta información en redes sociales para que el Ingeniero vaya sabiendo datos como donde vive, a que destinos se desplaza o incluso que tipo de actividades hace.

Acá se crean pretextos para inventar escenarios como que se tienen problemas informáticos que incitan a la víctima a permitir voluntariamente al ingeniero a tener acceso al computador y así romper la seguridad.

2. Ir familiarizando con la gente: Este método es el inicial que aplica un ingeniero social donde logra establecer confianza con la víctima, demostrando capacidades y habilidades que hacen llamar la atención y del cual ofrecen sus servicios para que la persona acuda a ellos en momentos que se deba solucionar alguna situación. También se utilizarán redes sociales para reforzar su familiaridad, su interés y así hacer amistades.

3. Ganar confianza con lenguaje corporal: El Ingeniero social resulta ser muy experto en este campo ya que demuestra mucha educación en la forma de expresarse usando un lenguaje que lo diferencia de los demás en lo forma de tratar a un empleado para traspasar la seguridad lógica y perimetral.

4. Aprovechar las entrevistas: Durante una entrevista se intercambia una cantidad de información sensible y confidencial, acá el ingeniero social es experto en hacer preguntas concretas sobre temas de tecnología y su buen funcionamiento para así detallar procesos de negocio. En este caso el Ingeniero Social puede tener éxito en la infiltración de la empresa y la obtención de las credenciales de ingreso.

5. Ganar la confianza con el sexo: Es muy curioso mencionar este ítem, pero según revistas y publicaciones el término de “sexo” cabe como método de ingeniería social, ya que puede ganar la confianza al mostrarse atractivo (a) para un individuo en la sociedad y con el pasar del tiempo el objetivo de obtener la información se obtendrá sin problemas.

6. Hablar de la charla: Una de las tácticas de gran alcance a disposición de los Ingenieros sociales es el conocimiento, debido a que puede usar esas habilidades para conseguir una entrevista o incluso un puesto de trabajo; pero él o ella puede crear confianza simplemente por estar bien informado y tener un parlamento convencedor.

Las personas de pocos conocimientos técnicos pueden ser superadas por las personas que tienen derecho a las palabras de moda en tecnología.

7. Ingeniería Social Inversa: Acá el Ingeniero social crea un problema y en seguida interviene para resolverlo. Esta táctica se basa en el sabotaje inicial para buscar asistencia y de este modo poder hacer la infiltración.

Un ejemplo común es que se utiliza una jugada para alertar departamento de sistemas que están bajo ataque, el cual es una falsa alarma como ver un aviso de ataque de denegación de servicio en la página web que lo único que busca es hacer ver que la información está comprometida.

Algunos de estos tips nombrados anteriormente se ponen en práctica en el Colegio con el fin de ver por cual lado es más fácil acceder a los sistemas de información del plantel educativo

- Para el segundo objetivo: Determinar las metodologías de Ingeniería social para aplicarlas al personal que usa equipos de cómputo en la Institución Educativa, se definió que las pruebas de Ingeniería Social son necesarias para ver en qué punto crítico está fallando los usuarios de la Institución.

7.2 METODOLOGÍAS DE INGENIERÍA SOCIAL

En la actualidad destacan 4 técnicas de Ingeniería Social que el individuo puede usar para atacar y probar la seguridad de cualquier entidad: *Spoofing, Pretexting, Media Dropping y Tailgating.*

7.2.1 Pruebas de seguridad mediante *Spoofing.* Esta técnica consiste en enviar un correo a un usuario donde lo que busca es convencer de que dé respuesta haciendo algo. La intención de este ataque de prueba es que el usuario en el correo de clic en un enlace, o se asigne una IP para suplantar y después de registrar esa actividad, se obtenga el dato de la clave de correo y así tomar el control de la información que se desee.

La solución para no caer en esta técnica es la personalización del correo dirigido al usuario, tener en cuenta en abrir solo correos conocidos ya que el atacante se

disfraza y puede redactar excelentemente y con buena ortografía y gramática pero esa tentación la debemos dejar a un lado.

La herramienta que se va emplear en este proyecto es el paquete Social *Engineering Toolkit* (SET) de código abierto que viene entre las aplicaciones que dispone *Kali Linux.*

7.2.2 Pruebas de seguridad usando *Pretexting.* El *Pretexting* es la técnica más conocida como "pretextos" en donde el actor básico es el teléfono en donde por medio de una llamada o chat se busca pedir información generalmente simulando ser alguien que solicita ayuda muy importante.

Esta puede resultar exitosa si aplica en usuarios recién ingresados a la entidad y que tengan acceso a información sensible, en esa conversación el Ingeniero Social simula necesitar ayuda de la víctima dando datos exactos de los integrantes de la entidad y explicando casos que suelen pasar en dicha empresa para dar más credibilidad a la llamada e iniciar a entrar en confianza y así recopilar datos valiosos.

La solución en este caso es usar herramientas como Maltego la cual puede impedir o detectar de donde proviene el ataque, además existen otro tipo de aplicaciones en el mercado que pueden llegar a mostrar el número de teléfono de la persona que solicita información haciéndose pasar por alguien de la entidad.

7.2.3 Pruebas de seguridad con Media *Dropping.* La acción de realizar descargas es normal en toda entidad acá el Ingeniero social busca el interés de la persona que por necesidad utiliza algún dispositivo para guardar algún tipo de información, acá el mago informático instala un pequeño programa dentro de la red y después lo ejecuta en modo de acceso remoto contra el equipo donde se conecta el medio extraíble con la intención de capturar la información.

Una aplicación del paquete de Kali que se usa para crear estos archivos es *Metasploit* que genera automáticamente este tipo de cargas maliciosas. Una solución para este caso es mediante el paquete Social *Engineering Toolkit* (SET) en donde se crea un ejecutable que automáticamente se activa en el computador señalado.

7.2.4 Pruebas de seguridad por medio de la técnica *Tailgating.* Esta técnica de *Tailgating* consiste en acceder a una instalación física mediante engaños al personal

o intentar manipular a una persona con el fin de poder ingresar a las instalaciones al atacante, el objetivo del test es demostrar que el atacante puede sobrepasar las barreras de la seguridad física. La persona que usa esta técnica debe instalar el dispositivo cuanto antes y que no deje sospechas para así lograr el éxito de su labor y lograr la información sensible.

Como conclusión se puede describir que por medio de estas 4 técnicas de ingeniería social se pueden determinar las falencias y así recomendar que acciones se deban corregir para reducir el riesgo de sufrir ataques mal intencionado.

A continuación se relaciona lo desarrollado en el objetivo 3 y 4 del proyecto:

- Para el tercer objetivo sobre Aplicar técnicas y metodologías de Ingeniería Social a los servidores públicos de la Institución Educativa Técnica de Panqueba.

Se define que tras utilizar un instrumento de recolección de datos como lo es la encuesta y por medio de entrevistas, también por una serie de preguntas al aire y por simple observación dentro de las instalaciones se pueden ver puntos claves para obtener datos que determinan las falencias encontradas por medio de técnicas de Ingeniería Social de la siguiente forma:

1. Técnica Pasiva: “Observación”

2. Técnica No Presencial: Por medio de llamadas y por chat se medirá la inocencia de las personas y así medir el nivel de confiabilidad que se tiene en el Colegio.

3. En este objetivo también se plantea aplicar una prueba en ambientes controlados sin infringir la ley para demostrar que el atacante en este caso quien desarrolla el proyecto puede superar a la seguridad física y acceder a la información.

*Se usó *Spoofing* para engañar por medio de correos electrónico ficticio.

En esta parte que es práctica se usó la herramienta *Kali Linux* que cuenta con el paquete Social *Engineering Toolkit* (SET), con este software se pueden ejecutar automáticamente una serie de ataques que comprometen el recurso humano de cualquier entidad partiendo desde el envío de mensajes de texto con números falsos, la implementación de servidores *“phishing”* y suplantación de sitios web entre otros.

*Se aplicó la técnica de *pretexting* por medio de una conversación por chat donde se evidencia la forma como la secretaria por medio de un dato del SIMAT de matrículas accedió a que ingresaran a su oficina y se obtuvo datos valiosos.

7.3 PLANTEAMIENTO DE LA ENCUESTA

Para tener más claridad de los conocimientos informáticos del plantel educativo se planteó una encuesta basada en una serie de 12 preguntas cerradas de una o varias opciones de respuesta.

Esta se ejecutó a mediados del mes de Octubre de 2017 en donde participaron 38 integrantes que hacen parte del plantel educativo, entre quienes dieron su opinión se encuentran por cargos distribuidos así:

- Rector
- Coordinador
- Tesorera
- Bibliotecaria
- 2 Secretarias Administrativas
- 20 Docentes
- Pagador
- Técnico en Soporte de Red
- Enfermero
- Personero Estudiantil
- 2 Celadores
- Encargado de Mesa de Ayuda Enlace SENA

- 5 Estudiantes grado 11 (encargados de diseñar página web de la especialidad de Sistemas y también los que diseñan las bases de datos que el Colegio requiere para cumplir con algunos servicios)

Esta actividad concluyo satisfactoriamente con la opinión de cada uno de los encuestados, en donde los resultados se muestran a continuación por medio del uso de tablas y graficas con su respectivo análisis y conclusión de los datos encontrados.

7.4 RESULTADOS DE LA ENCUESTA

1. Considera que la información que maneja en su equipo es segura para cumplir con las actividades de la Institución.

Tabla 1. Opinión a Pregunta 1

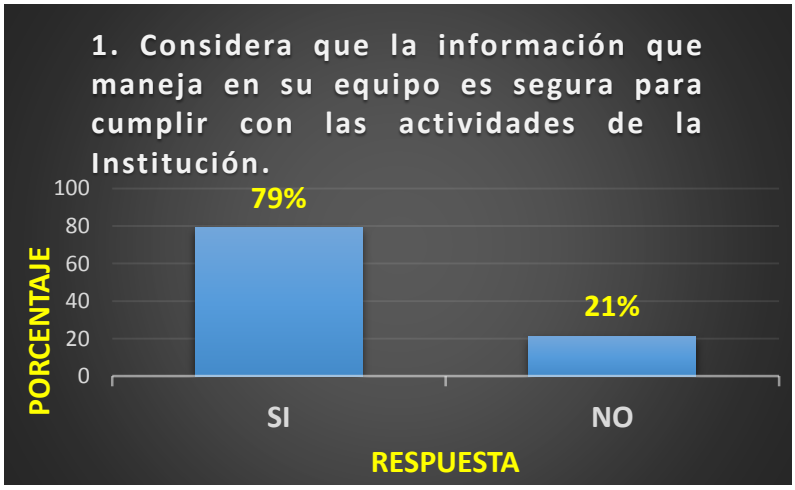
OPCION	CANTIDAD	%
SI	30	79
NO	8	21
TOTAL	**38**	**100**

Fuente: El Autor

Como conclusión 30 personas de las encuestadas que representa el 79% de la población dijeron que si tienen confianza en cuanto a la seguridad de los datos que administran en el equipo para dar cumplimiento a las actividades que plantea el Colegio.

En la gráfica 1 se reflejan los resultados.

Gráfica 1. Respuesta pregunta 1



Fuente: El Autor

2. ¿Sabe en qué consiste las Técnicas de Ingeniería Social?

Tabla 2. Opinión a Pregunta 2

OPCION	CANTIDAD	%
SI	12	32
NO	26	68
TOTAL	**38**	**100**

Fuente: El Autor

Como conclusión 26 personas de las encuestadas que representa el 68% de la población dieron la opinión de que desconocer este término informático, y es un alto porcentaje de usuarios que pueden ser víctimas de ataques informáticos, en donde solo el 32% de la población conoce las técnicas de Ingeniería Social.

El tema de Ingeniería Social es conocido solo por los docentes del área de Sistemas y por los estudiantes debido a que este tipo de charlas se dio a inicio de año por parte del SENA pero solo en las salas de informáticas e hizo falta integrar a los demás integrantes del plantel.

En la gráfica 2 se reflejan los resultados del desconocimiento del tema de Ingeniería Social.

Gráfica 2. Respuesta pregunta 2

3. Ha recibido llamadas, correos electrónicos o por chat solicitudes donde le piden datos personales o de su Institución.

Tabla 3. Opinión a Pregunta 3

OPCION	CANTIDAD	%
SI	18	47
NO	20	53
TOTAL	**38**	**100**

Fuente: El Autor

En esta pregunta que en el mundo laboral es algo muy común y que a diario ocurre, acá resulta muy pareja en cuanto a la opinión recibida debido a que 18 personas que representa el 47% de la población manifiestan haber recibido este tipo de estrategias donde le solicitan datos tanto personales como laborales.

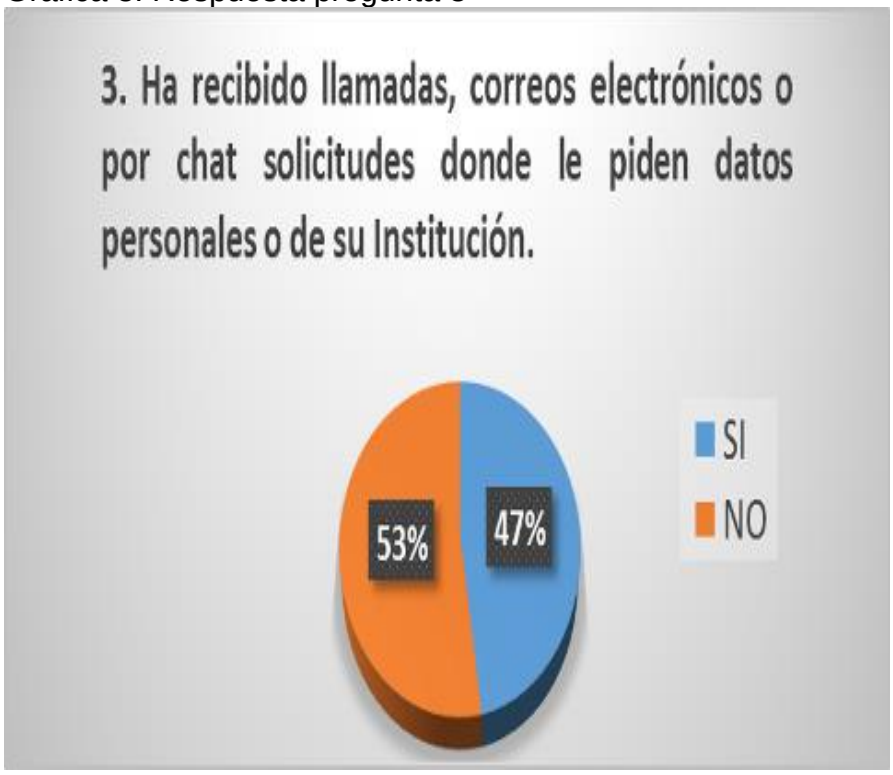
Y queda reflejado que el 53% de la población no ha recibido este tipo de técnicas que lo único que buscan es empezar a saber datos para luego usar estrategias que

permitan capturar más información valiosa que puede ser usada para fines comunes.

En esta instancia del proyecto se puede evidenciar que las capacitaciones que orientare a fin de mes deben mejorar esos tips en el plantel educativo mejorando esos puntos débiles que se tienen en cuanto a seguridad informática.

En la gráfica 3 se muestran los resultados.

Gráfica 3. Respuesta pregunta 3



Fuente: El Autor

4. ¿Se siente seguro con el antivirus de su equipo?

Tabla 4. Opinión a Pregunta 4

OPCION	CANTIDAD	%
SI	18	47
NO	18	47
NO USA ANTIVIRUS	2	5
TOTAL	**38**	**100**

Fuente: El Autor

Esta pregunta rueda a diario en el ámbito informático, y la encuesta refleja un empate en opinión del 47% que manifiesta que confía en el antivirus y la otra mitad desconfía.

Es preocupante la opinión de 2 personas que dicen que no usan antivirus y esa es una de las falencias esenciales para que el usuario tenga problemas y pérdidas en su información, aconsejable usar el Kaspersky en versión que cuenta con licencia de pago ya que cumple todos los ítems de seguridad y se garantiza la seguridad de la información.

En la gráfica 4 se refleja los resultados.

Gráfica 4. Representación pregunta 4

Fuente: El Autor

5. ¿Qué causas han afectado la seguridad de su información?

Tabla 5. Opinión a Pregunta 5

OPCION	CANTIDAD	%
VIRUS	28	35
FALLAS DE PROGRAMAS	14	18
SPAM	9	11
DAÑO DEL HARDWARE	7	9
MAL USO DE REDES SOCIALES	7	9
PERDIDA DE CLAVES	13	16
NINGUNA	2	3
TOTAL	**80**	**100**

Fuente: El Autor

La seguridad de la información incluye los 4 pilares que son factor determinante en el mundo informático, y el plantel educativo según la encuesta determina que los virus en primera instancia, enseguida de las fallas que presentan algunos programas y la perdida de claves son los factores que más han afectado la seguridad de su información.

Se puede dar conclusión que la gran mayoría de los integrantes del Colegio pueden ser vulnerables a perder su información muy fácil con el hecho de que no cuentan con las condiciones mínimas para dar buen uso de la información según lo manifestado en la encuesta y que se refleja en la gráfica 5.

Gráfica 5. Representación pregunta 5

Fuente: El Autor

6. ¿Cambia frecuentemente sus contraseñas?

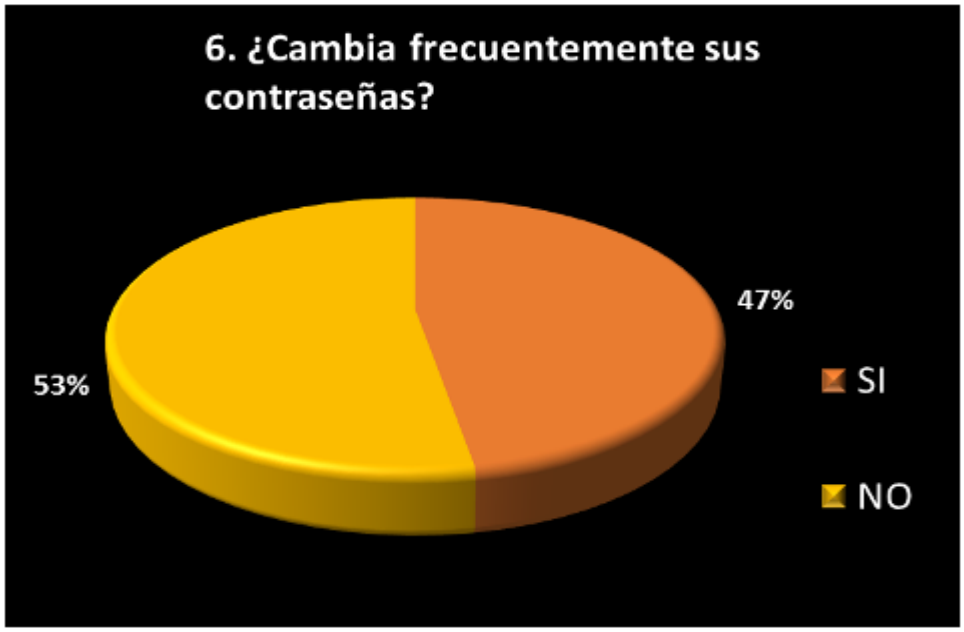
Tabla 6. Opinión a Pregunta 6

OPCION	CANTIDAD	%
SI	18	47
NO	20	53
TOTAL	**38**	**100**

Fuente: El Autor

Como conclusión 20 personas de las encuestadas que representa el 53% de la población dicen que no le ven la necesidad de cambiar las claves de su equipo, cuentas de usuario y herramientas que usan en línea, pero el 47% de la población si pone en práctica esta táctica que a muchos no les suele gustar pero que en ocasiones periódicamente se puede implementar. A continuación en la gráfica 6 se reflejan los resultados.

Gráfica 6. Representación pregunta 6



Fuente: El Autor

7. Alguien más sabe las contraseñas que usted usa en su ámbito de Sistemas.

Tabla 7. Opinión a Pregunta 7

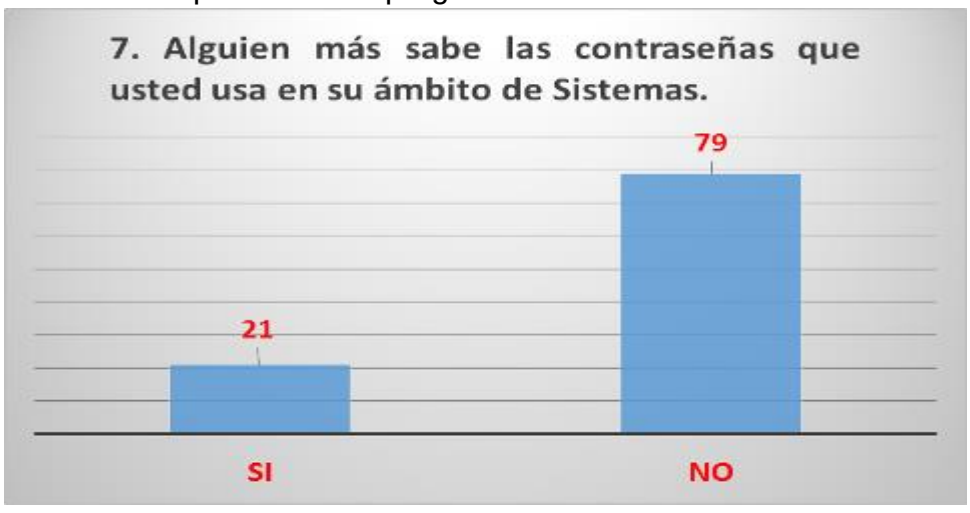
OPCION	CANTIDAD	%
SI	8	21
NO	30	79
TOTAL	**38**	**100**

Fuente: El Autor

Como conclusión 30 personas de las encuestadas que representa el 79% de la población y es un porcentaje alto de usuarios que aplican la regla informática de que una clave es personal y privada y nadie más tiene derecho a saberla.

Pero si el 21% de la población deja preocupación ya que se puede decir que es el ítem más llamativo para caer en técnicas de ingeniería social proporcionando perdidas en datos y baja productividad en entornos laborales.
En la gráfica 7 se pueden observar los resultados.

Gráfica 7. Representación pregunta 7



Fuente: El Autor

8. ¿Cuándo crea una contraseña la establece teniendo en cuenta que parámetros?

Tabla 8. Opinión a Pregunta 8

OPCION	CANTIDAD	%
COMBINA NUMEROS, MAYUSCULAS Y MINUSCULAS	27	41
LONGITUD MENOR A 8 CARACTERES	7	11
USA SOLO LETRAS	6	9
USA SOLO NUMEROS	8	12
COLOCA PALABRAS COMUNES	5	8
USA CARACTERES #$%&/( )?	13	20
TOTAL	**66**	**100**

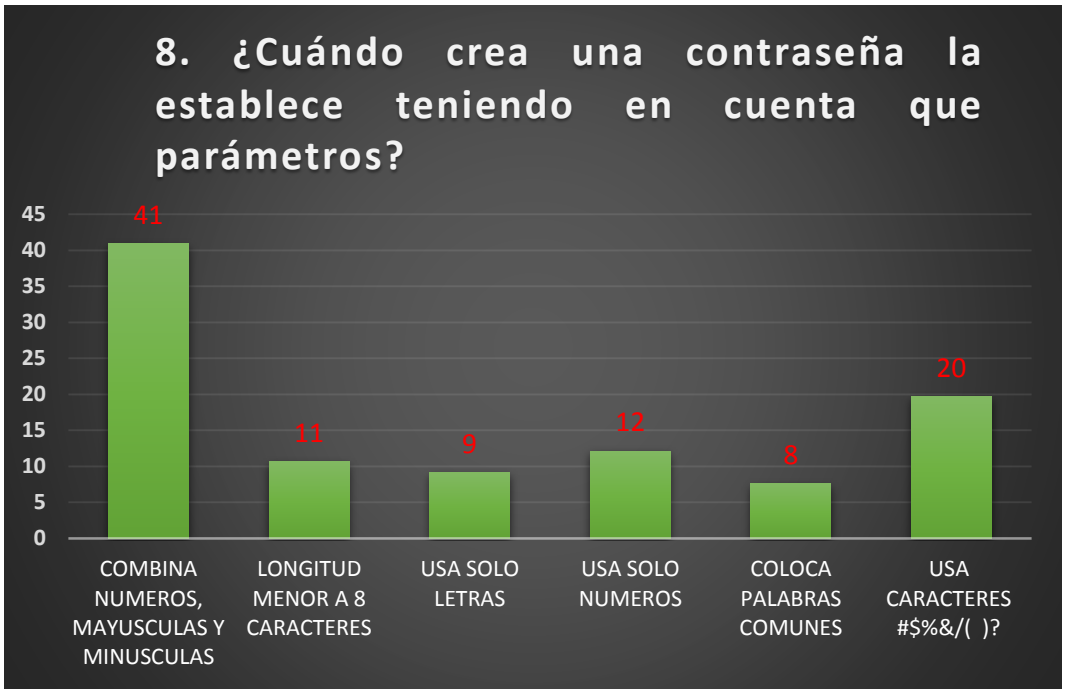
Fuente: El Autor

Otro tema importante alrededor de las contraseñas es el de las técnicas que se pueden usar para su elaboración.

Se preguntó a los encuestados sobre cuáles parámetros usa para crear contraseñas seguras, y el resultado encontrado fue que 27 usuarios usan la técnica de combinar números, mayúsculas y minúsculas y 13 empleados del plantel usa distintos símbolos o caracteres, lo cual es buena estrategia y se puede deber a las políticas de seguridad establecidas por algunas plataformas o sistemas de información propios o ajenos a la universidad que exigen esa estructura como requisito para crear usuarios.

Se pudo deducir a la vez, como lo demuestra la gráfica 8 a continuación, que quizás las técnicas menos usadas es la de poner nombres o palabras comunes y este tip es de vital importancia ya que es un punto positivo que se tiene para no ser víctima de que alguien le averigüe la clave

Gráfica 8. Representación pregunta 8



Fuente: El Autor

9. De los siguientes medios de comunicación cuál cree que puede afectar su información.

Tabla 9. Opinión a Pregunta 9

OPCION	CANTIDAD	%
CORREO	15	22
CHAT	8	12
DESCARGAS	18	26
REDES SOCIALES	16	23
USAR SOFTWARE EN LINEA	12	17
TOTAL	**69**	**100**

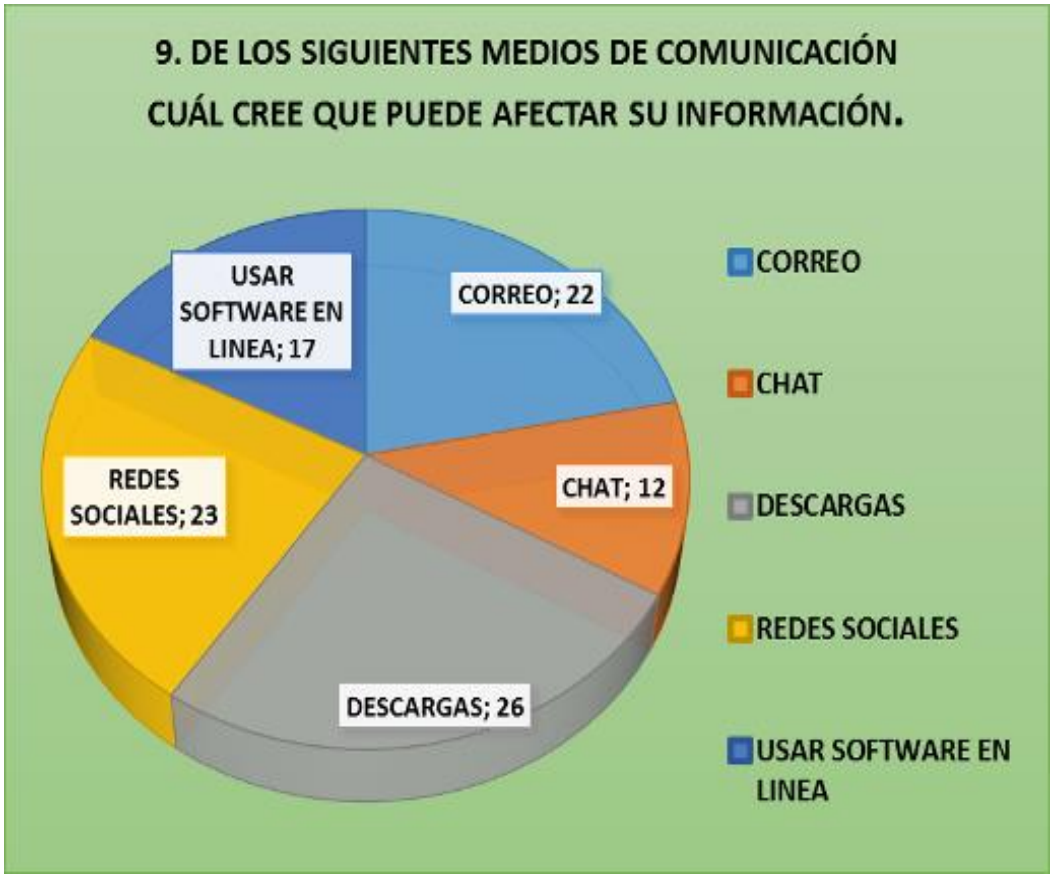
Fuente: El Autor

En esta pregunta se refleja que no se tienen claro cuáles pueden ser las paginas para hacer descargas apropiadas desde internet y están usando páginas web de autores y compañías desconocidas lo cual puede incurrir en un factor clave para caer en manos de los ingenieros sociales.

Otro factor clave que se puede ver es que la Institución no cuenta con controles de acceso a páginas de redes sociales en donde según la encuesta se refleja que el 23% del plantel se ha visto afectado para altera su información.

En la gráfica 9 se refleja los resultados.

Gráfica 9. Representación pregunta 9



Fuente: El Autor

10. ¿Ha recibido capacitación sobre temas de seguridad informática?

Tabla 10. Opinión a Pregunta 10

OPCION	CANTIDAD	%
SI	17	45
NO	21	55
TOTAL	**38**	**100**

Fuente: El Autor

Durante el desarrollo de este proyecto se irá dando solución a este desconocimiento del tema que se refleja en el 55% de los integrantes del Colegio por medio de las distintas charlas de seguridad informática, y en el final del proyecto con el manual de políticas de seguridad que se deja en la Institución para dar buen uso de la información en todo el ámbito informático tanto personal como laboral.

En la gráfica 10 se refleja los resultados.

Gráfica 10. Representación pregunta 10

Fuente: El Autor

11. En su experiencia de manejo de computador, celular y redes sociales que mensajes curiosos ha encontrado en sus dispositivos

Tabla 11. Opinión a Pregunta 11

OPCION	CANTIDAD	%
GANASTE UN PREMIO	24	34
ACTUALICE SU CUENTA	7	10
DIGITE CLAVE DE SU EQUIPO	5	7
CLICK Y PARTICIPE SORTEO	23	33
OTRAS	11	16
TOTAL	**70**	**100**

Fuente: El Autor

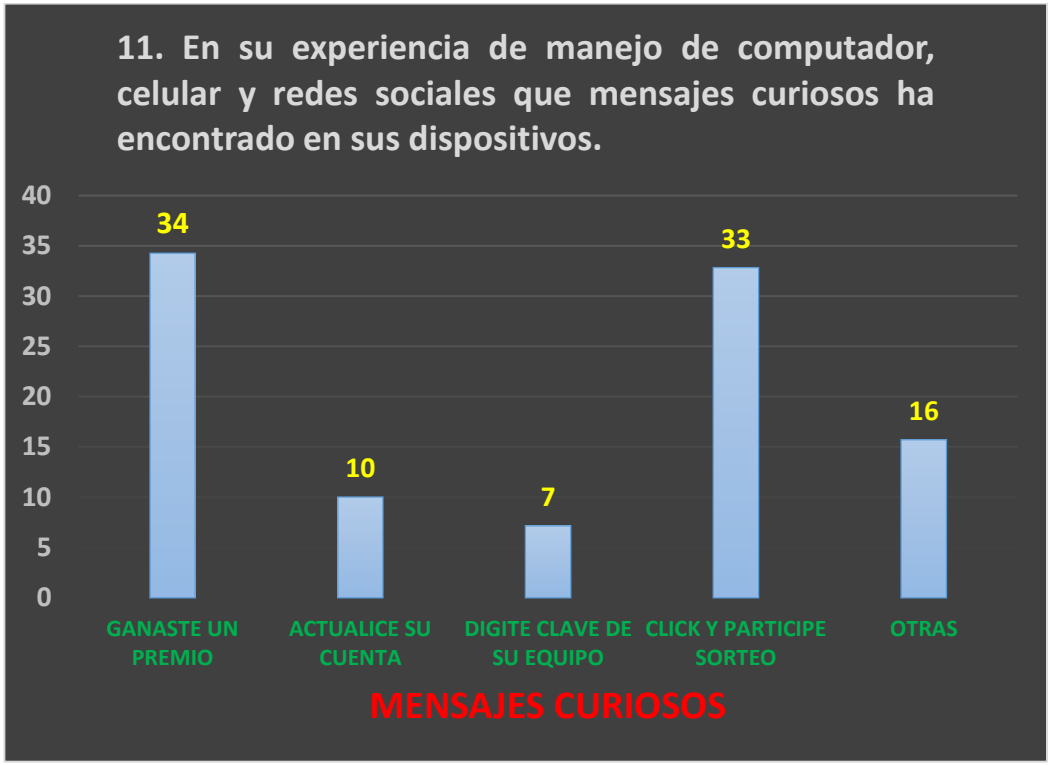
Este tipo de estrategias se determinan como las técnicas de ingeniería social pasiva y no presencial, en donde por medio de estos aspectos de ingeniería social inversa se busca tratar de ganar confianza para día a día convencer a la víctima para que entregue cualquier tipo de información.

En el plantel es muy común que a sus empleados les ha llegado mensajes de que han ganado premio con un 34% de la población, seguido del 23% que les llega invitaciones para dar clic a enlaces que no se sabe cuál sea la finalidad del atacante.

Es por eso que todos estos aspectos se tendrán en cuenta en el manual que se deja al final del proyecto con una serie de recomendaciones y consejos para uso adecuado de correo, redes sociales, chat, acceso a servicios de internet, claves de usuario, privacidad de la información, técnicas de ingeniería social.

En la gráfica 11 se refleja los resultados.

Gráfica 11. Resultado de la pregunta 11



Fuente: El Autor

12. Considera que el ingreso a las instalaciones de su Institución son aptas y confiables.

Tabla 12. Opinión a Pregunta 12

OPCION	CANTIDAD	%
SI	30	79
NO	8	21
TOTAL	**38**	**100**

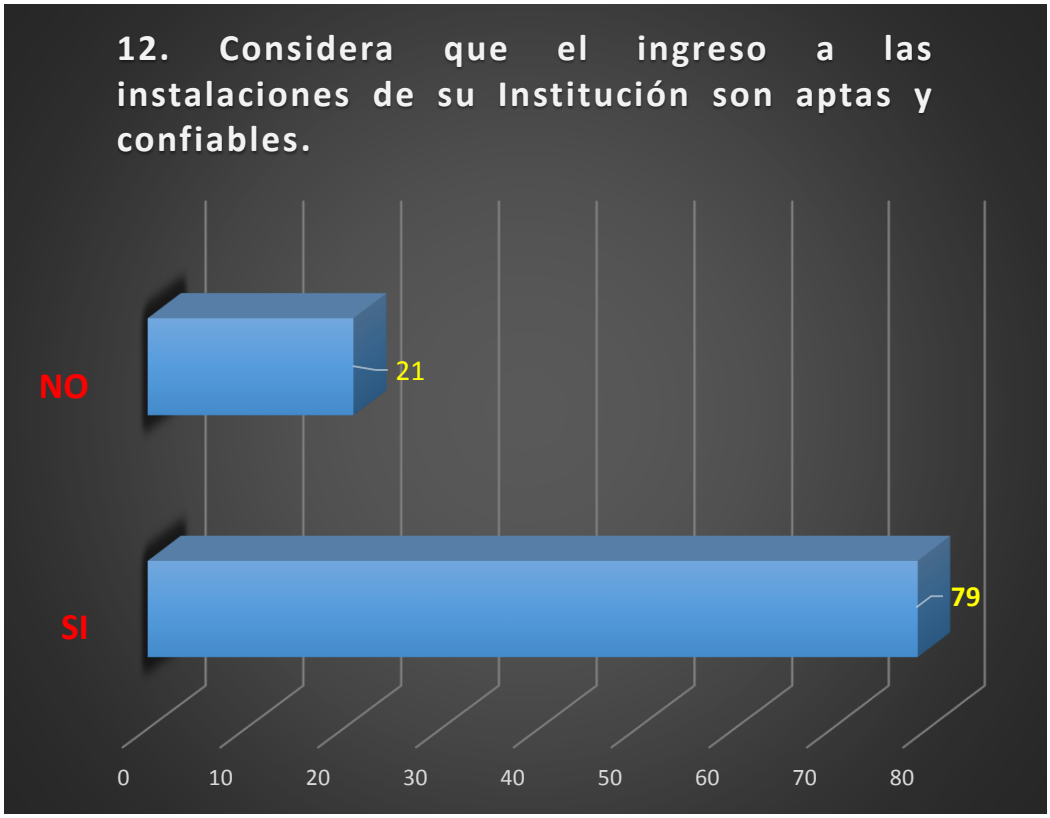
Fuente: El Autor

En esta pregunta se enfoca a saber si los activos del Colegio no tienen forma de perderse o extraviarse en cuanto a si se tiene un control en la entrada de las instalaciones.

Como conclusión se dice que el Colegio es seguro demostrado por la opinión de 30 personas de las encuestadas que representa el 79% de la población, aunque el 21% de la población ve en ciertos detalles inseguridad y es porque en horas de la tarde se presta servicio a la comunidad del Municipio de Biblioteca donde entra cualquier tipo de persona a realizar diversas actividades informáticas.

Con la gráfica 12 se da por terminado el análisis de la encuesta.

Gráfica 12. Resultado de la pregunta 12



Fuente: El Autor

7.5 PRACTICA CON TECNICA DE SPOOFING

La intención no es aprovechar las vulnerabilidades a nivel tecnológico sino ver respuesta al recurso del ser humano. Es por eso que se aplicó con una de las distribuciones que trae *Kali Linux* la siguiente técnica de *Spoofing:*

Email Spoofing: Creando un correo ficticio parecido al institucional con el fin de ver cómo actúan determinados integrantes del Colegio al revisar un mensaje en el correo donde se anuncia que no abra acceso normal a unos servidores de correo.

SOLUCION CASO PRÁCTICO

Este caso que se muestra a continuación se utilizó una técnica de Ingeniería Social y demuestra como un delincuente informático con tan solo conocer un par de direcciones de correo electrónico y usar un párrafo como parlamento puede capturar datos sensibles para poder acceder a cualquier información sin que la víctima se dé cuenta.

El objetivo es demostrar que en las instalaciones del Colegio Técnico de Panqueba sus usuarios caen de una forma muy fácil aprovechando las vulnerabilidades existentes, no solo a nivel tecnológico sino también en el recurso humano.

La herramienta viene incorporada en Kali Linux y se llama SET “Social *Engineer Toolkit”.* Con este software se pueden ejecutar automáticamente una serie de ataques que comprometen el recurso humano de cualquier entidad desde el envío de mensajes de texto con números falsos, la implementación de *phishing*, servidores y la suplantación de sitios web el cual este es el caso a ejecutar.

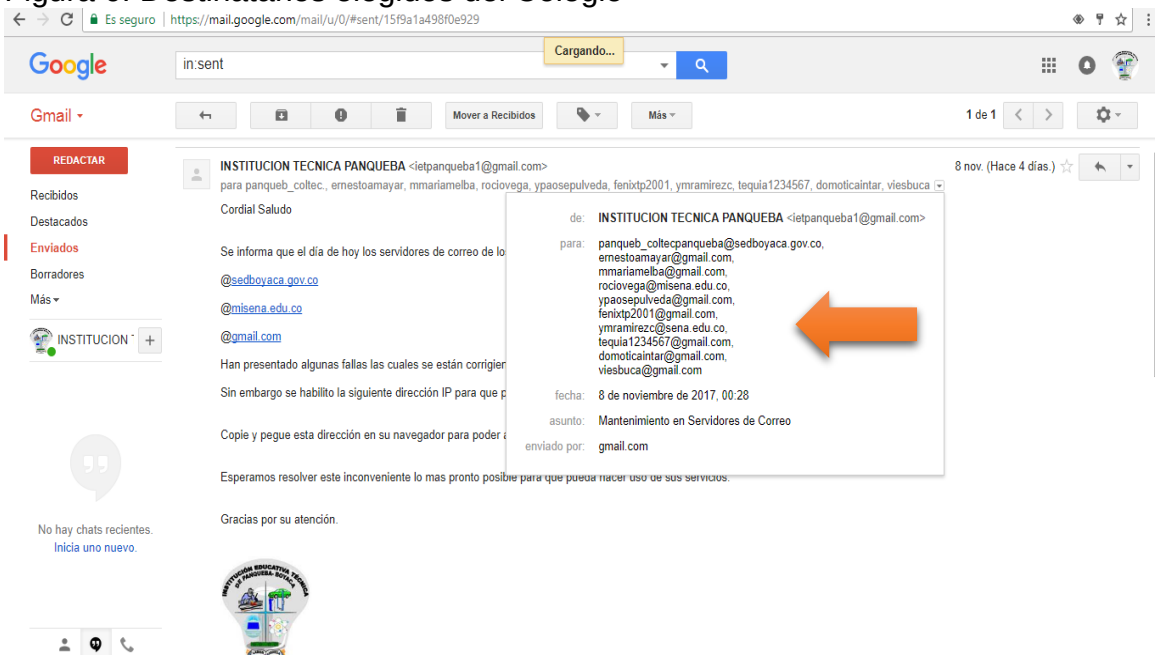
Esta técnica va emplear 4 pasos enumerados y explicados a continuación:

1. Identificación de las víctimas
2. Crear el escenario.
3. Realizar el ataque
4. Captura de información

PASO 1: Identificación de las víctimas

Para este tipo de técnica de Ingeniería Social se aplicó en 10 funcionarios del Colegio Técnico de Panqueba como se ve en la figura 6.

Figura 6. Destinatarios elegidos del Colegio



Fuente: El Autor

PASO 2: Crear el escenario

Se decide suplantar la página del logueo del correo institucional con el objetivo de ver como la ingenuidad y el desconocimiento de aspectos informáticos pueden ser elementales al momento de acceder a la información confidencial manejada por los usuarios del Colegio según la estrategia planteada.

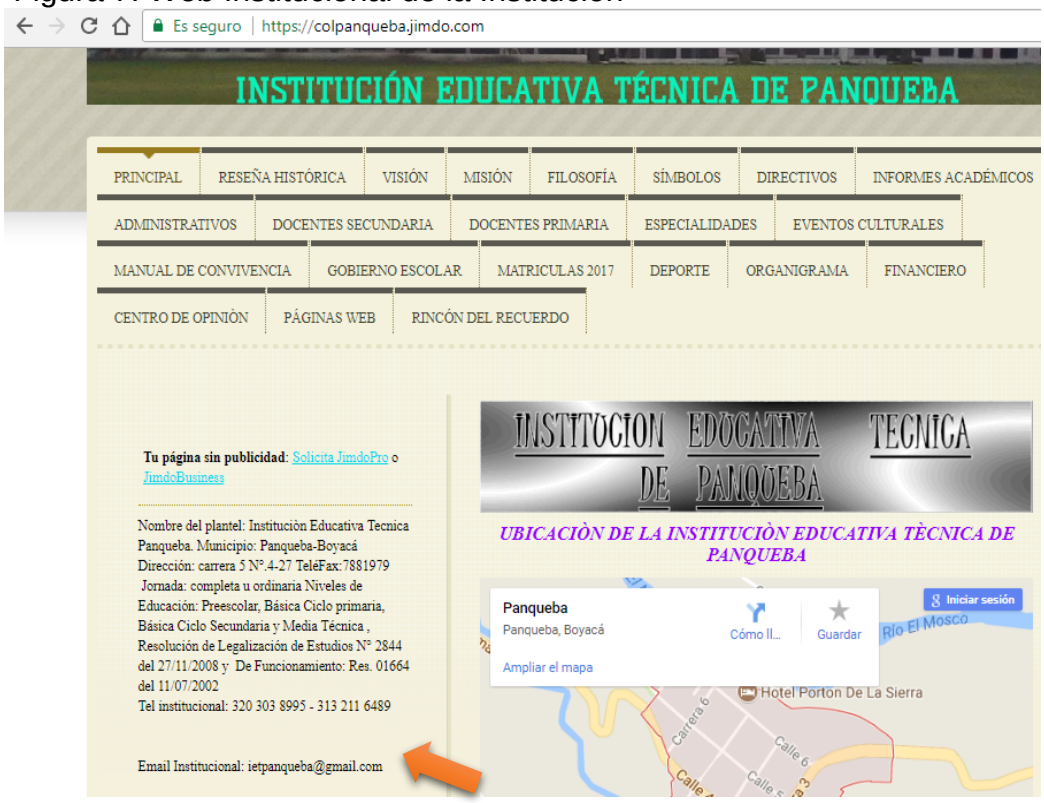
El Ingeniero Social en este caso quien está desarrollando el Proyecto como meta propuso conseguir el correo institucional de algunos usuarios lo cual no resulto complicado, basto con preguntar y fingir que era para poblar una base de datos y así dar a conocer novedades de cursos ofertados que llegan al despacho de la Alcaldía.

PASO 3: Realizar el ataque

Para la ejecución de la técnica de Ingeniería Social el procedimiento fue el siguiente:

Primero se creó una cuenta de correo ficticia con usuario ietpanqueba1@gmail.com Este correo es muy similar al que maneja la secretaria principal ietpanqueba@gmail.com y se encuentra en la web institucional como se ve en la figura 7.

Figura 7. Web Institucional de la Institución



Fuente: https://colpanqueba.jimdo.com/

Como segunda medida antes de enviar el mensaje a los usuarios seleccionados, se inicia la configuración del SET “Social *Engineer Toolkit”* en el computador del atacante.

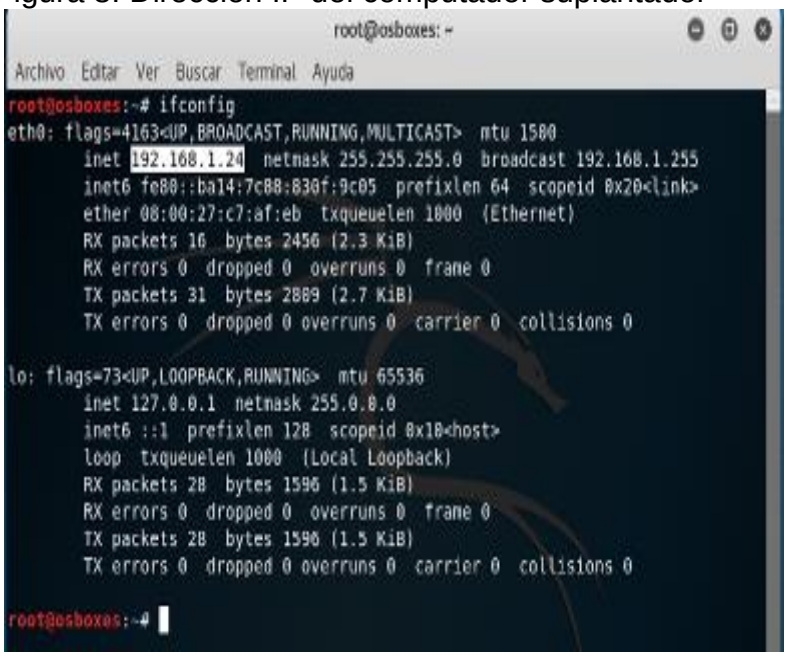
Es importante resaltar que esta herramienta solo funciona dentro de una red local y que antes de usarla de sebe actualizar mediante los comandos propios de Linux, ya sea; apt-get update o. /set-update.

El SET Social *Engineer Toolkit* está incluido las distribuciones dentro Linux de *Kali y Backtrack* y su objetivo principal es la de servir como medio para hacer pruebas de penetración en las redes de cualquier entidad.

Las imágenes a continuación describen paso a paso ese proceso.

En este punto, se verifica la dirección IP asignada al computador que suplantará la página web seleccionada desde la que se hará el ataque **192.168.1.24**

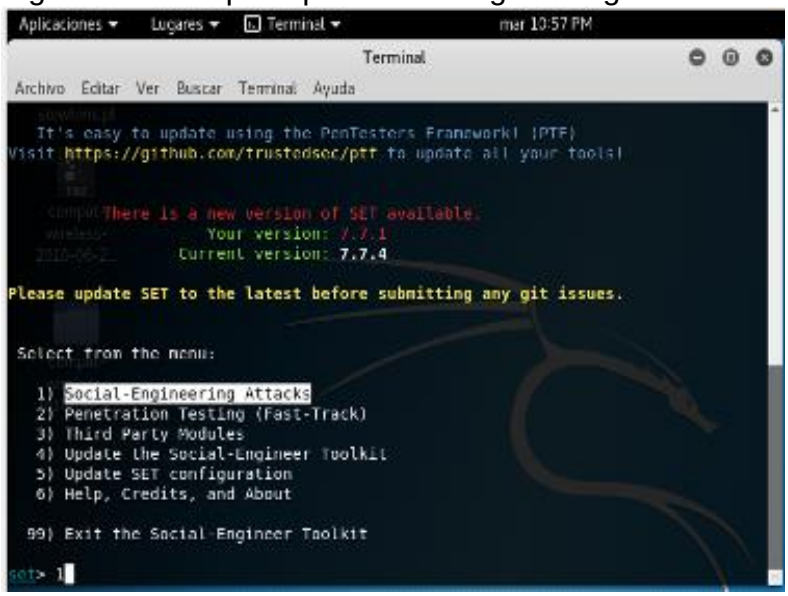
Figura 8. Dirección IP del computador suplantador



Fuente: El Autor

Después del primer pantallazo que es aceptar los términos se despliega un menú principal en el que se debe seleccionar la opción 1, en este caso.

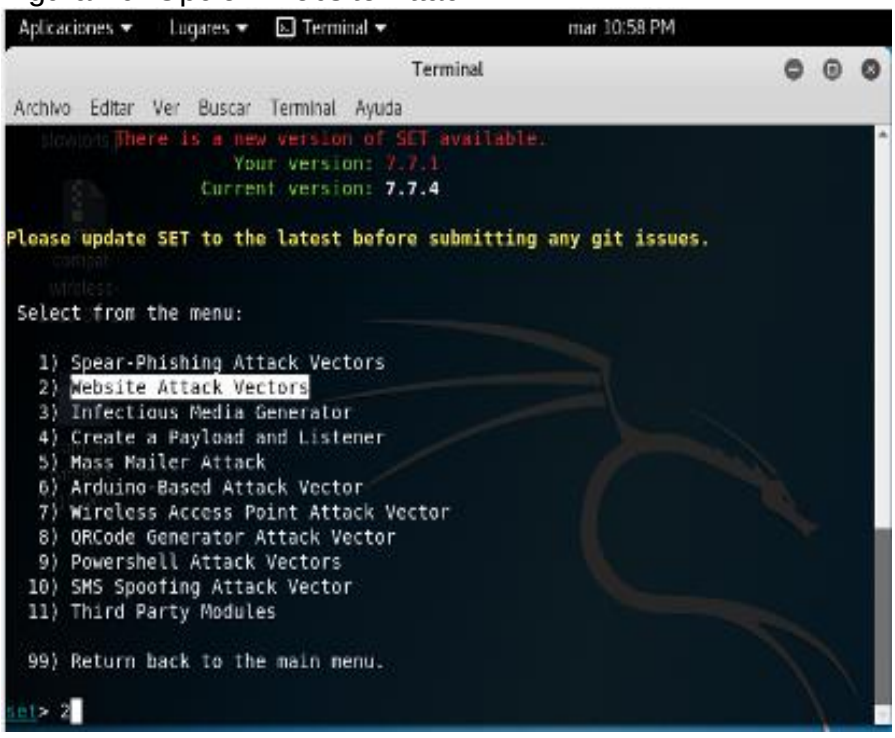
Figura 9. Menú principal Social Engineering Toolkit



Fuente: El Autor

En la figura 10 se debe seleccionar la opción "*Website Attack Vectors*".

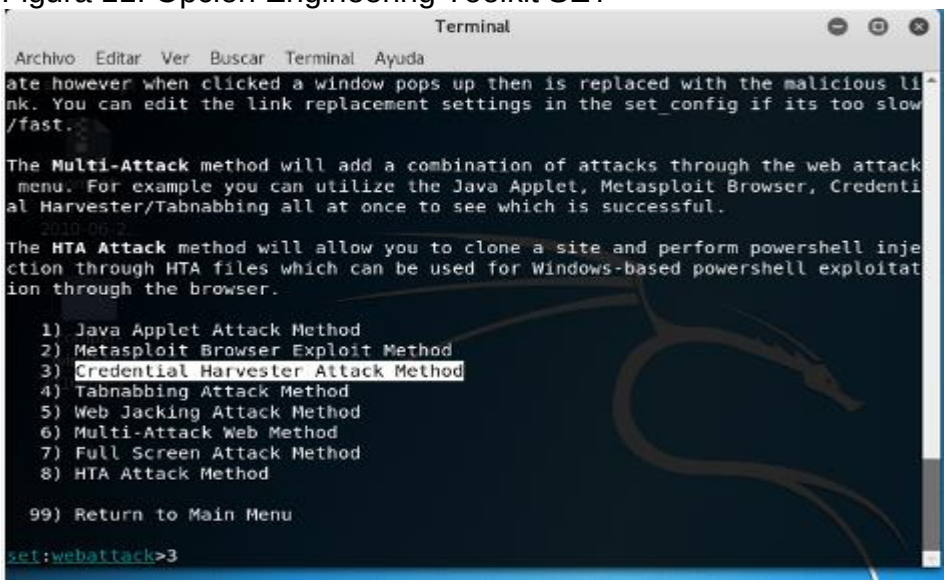
Figura 10. Opción Website Attack



Fuente: El Autor

Luego seleccionamos la tercera opción (3)

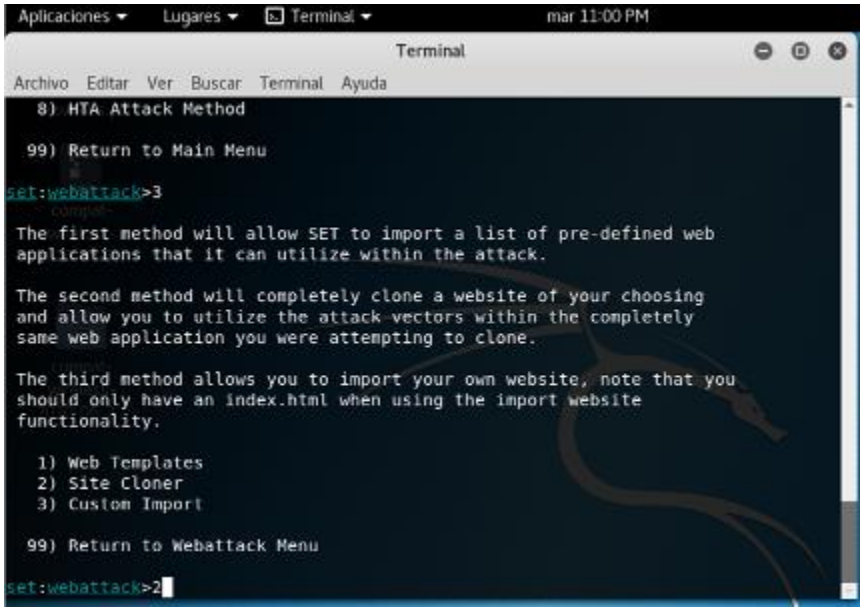
Figura 11. Opción Engineering Toolkit SET



Fuente: El Autor

Luego seleccionamos la segunda opción (2) “Site cloner”.

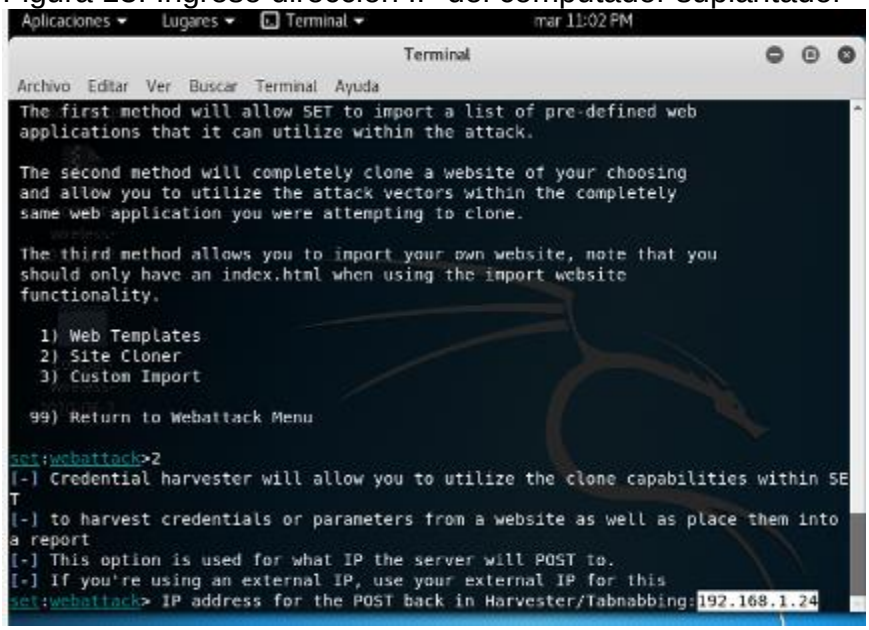
Figura 12. Opción de sitio a clonar



Fuente: El Autor

Aquí se escribe la IP del computador o maquina suplantador.

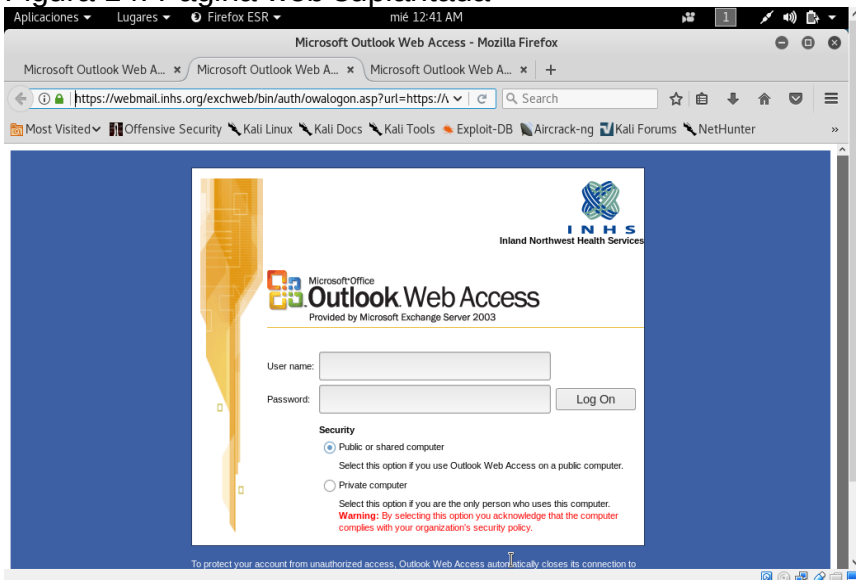
Figura 13. Ingreso dirección IP del computador suplantador



Fuente: El Autor

Luego se ingresa la página web que se suplantara.

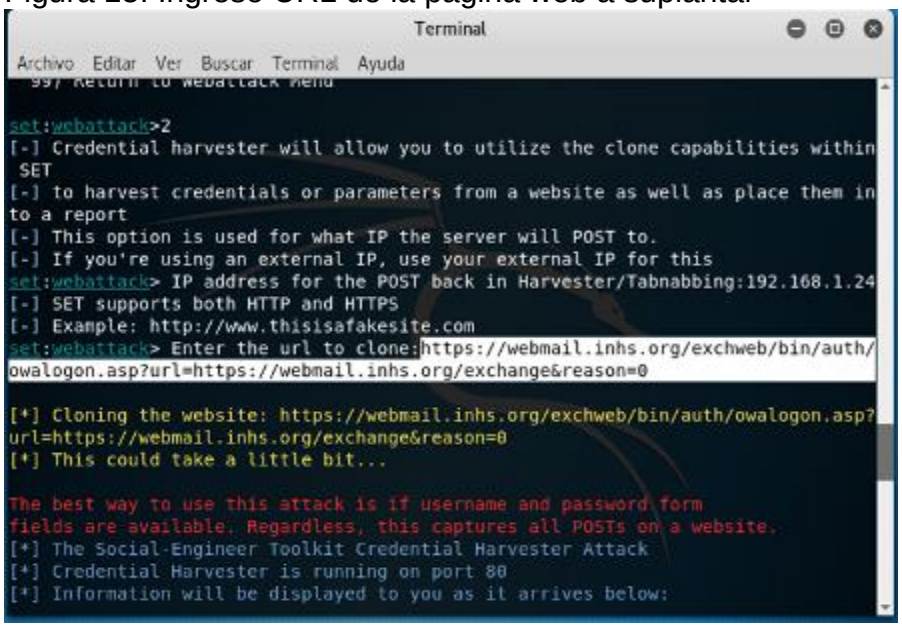
Figura 14. Página web suplantada



Fuente: El Autor

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

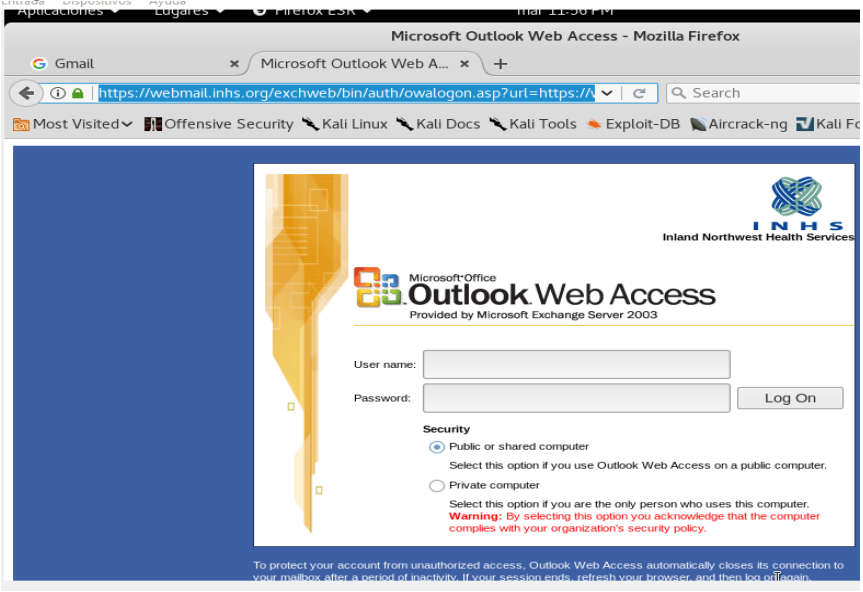
Figura 15. Ingreso URL de la página web a suplantar



Fuente: El Autor

Acá en la figura 16 se muestra la Página web ya suplantada en *kali Linux.*

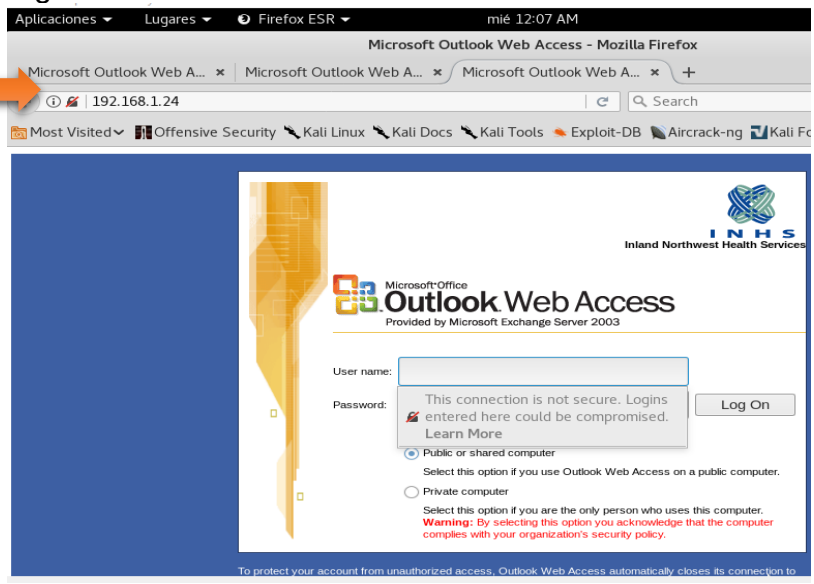
Figura 16. Sitio web oficial



Fuente: El Autor

Y en la figura 17 se ve el sitio web falso que recibirá los datos de aquel usuario que haga el debido proceso.

Figura 17. Sitio web falso



Fuente: El Autor

- El tercer paso es redactar el siguiente mensaje dirigido a los elegidos del plantel educativo.

Lo que se tuvo en cuenta fue que los correos a donde se envió el falso mensaje fueran de personas de fácil acceso por parte del personal según las visitas hechas al colegio.

Figura 18. Mensaje enviado

Fuente: El Autor

Después de ingresar la dirección web de la página a suplantar, el servidor queda listo y a la espera de que se envíen datos por parte de los usuarios.

Paso 4: Captura de información.

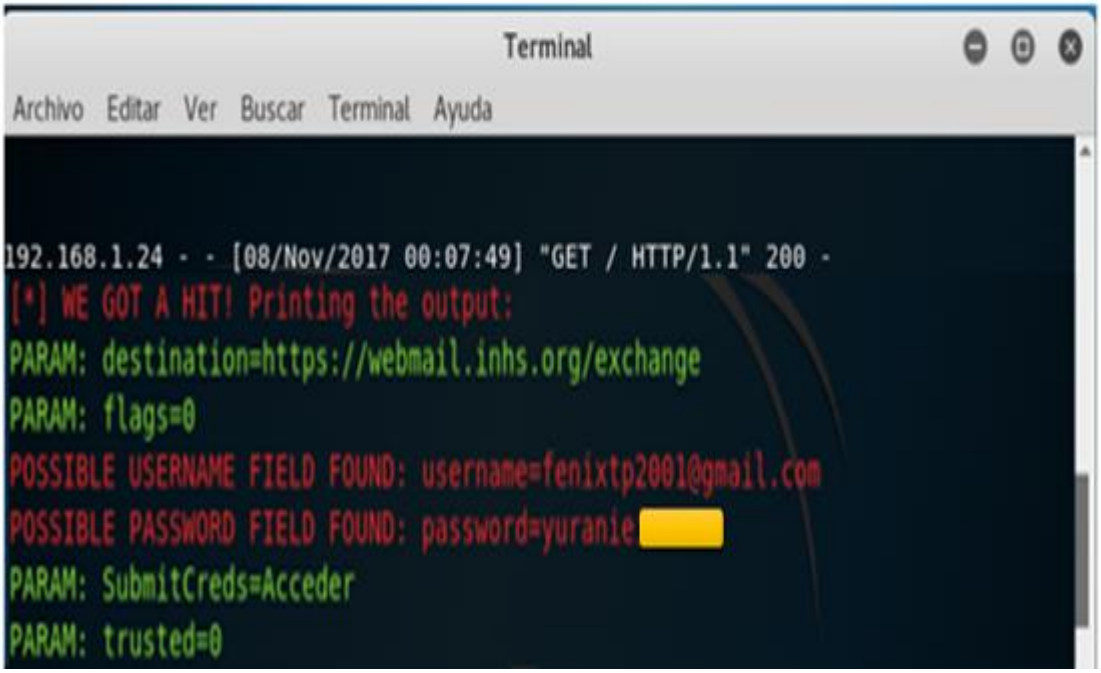
Para esta acción se dejó activa la maquina determinadas horas mientras que alguno de los usuarios a los que se les envió el falso mensaje siguiera sus instrucciones:

A continuación se muestran los pantallazos desde Kali de 3 víctimas que accedieron a esta IP, donde se puede observar el nombre de usuario y la contraseña de cada uno de los integrantes que por inocencia intentaron ingresar al correo institucional desde la página web falsa. Con los datos recolectados el atacante puede acceder a los correos de los usuarios y apoderarse de información confidencial para afines personales.

Nota: "La clave le tape unos caracteres con una barra amarilla para evitar no divulgar esos datos privados"

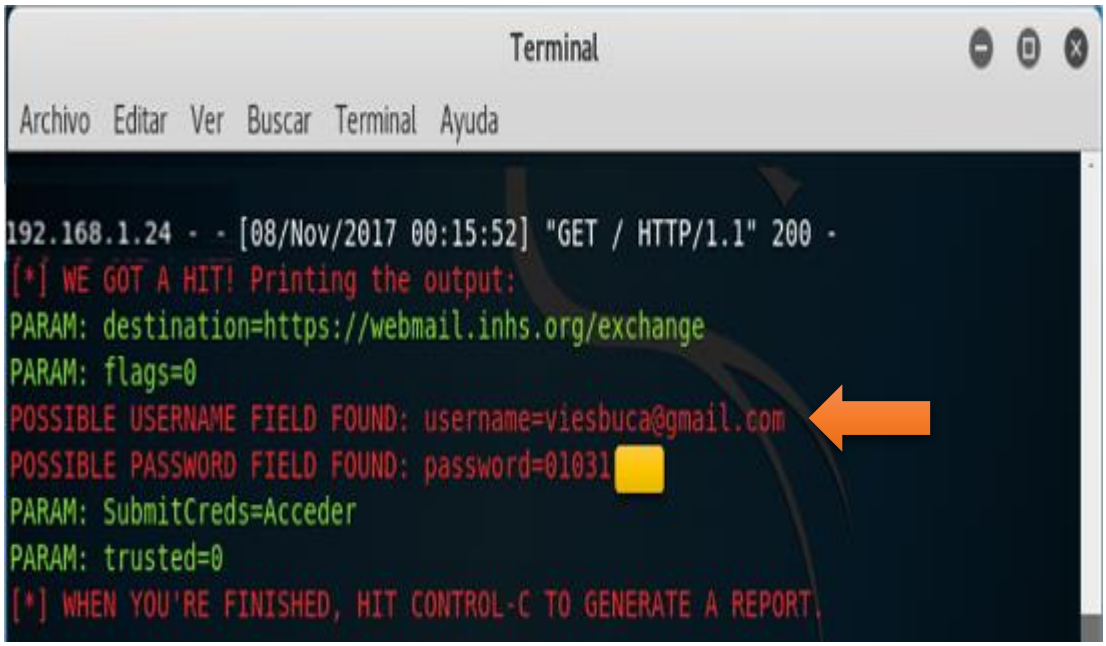
Las figuras 19, 20 y 21 muestran los datos obtenidos de las 3 víctimas.

Figura 19. Datos registrados victima 1



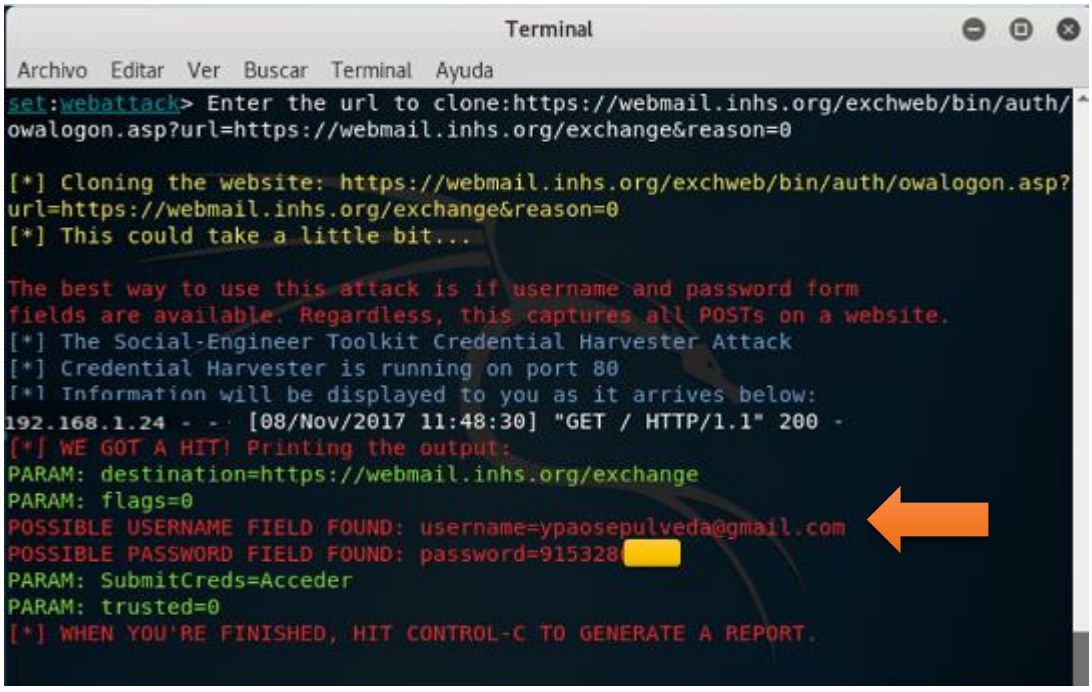
Fuente: El Autor

Figura 20. Datos registrados victima 2



Fuente: El Autor

Figura 21. Datos registrados victima 3



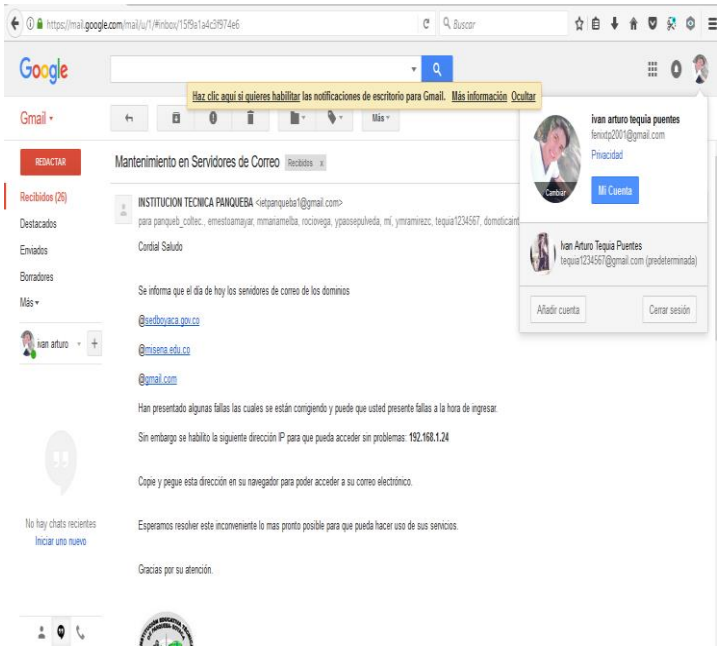
Fuente: El Autor

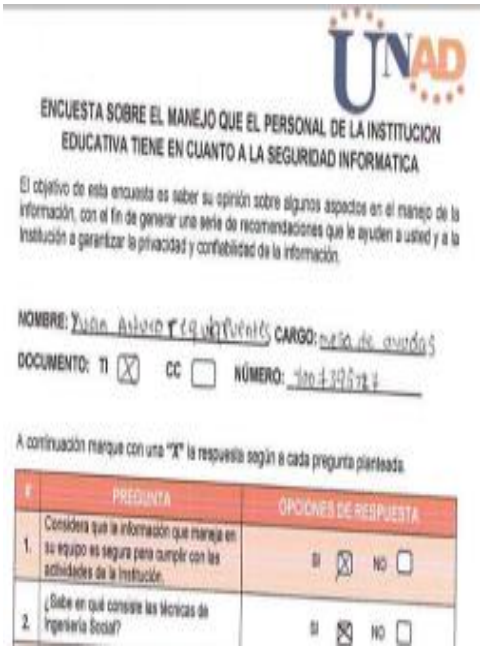
Luego de haber visto el proceso que mostro que 3 integrantes del plantel educativo hicieron caso al correo enviado se muestran las imágenes a continuación del acceso al correo de esos 3 usuarios engañados, se puede dar un vistazo al buzón de entrada para verificar que el correo es real por varios mensajes que tiene por leer.

Además en 2 de las víctimas junto al pantallazo del correo se anexa el encabezado de la encuesta contestada en este proyecto.

En este caso de la primera víctima es el encargado de mesa de ayuda que tiene asignado el Colegio.

Figura 22. Ingreso al correo victima 1 y evidencia de encuesta

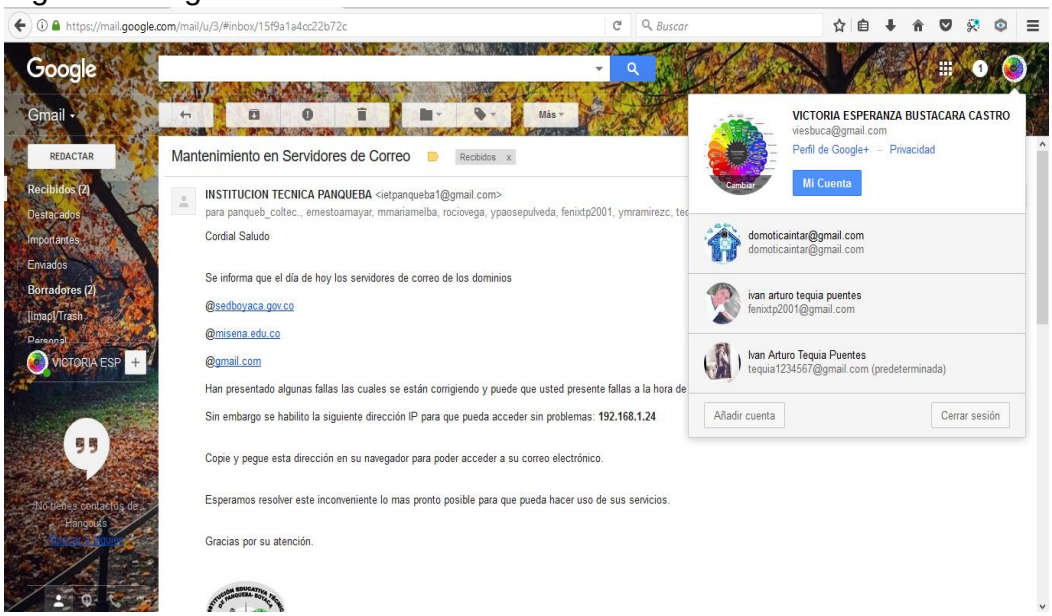




Fuente: El Autor

Esta segunda víctima es la docente del área de Biología, a quien no se le pudo indagar la encuesta por motivos de incapacidad los días que se aplicó.

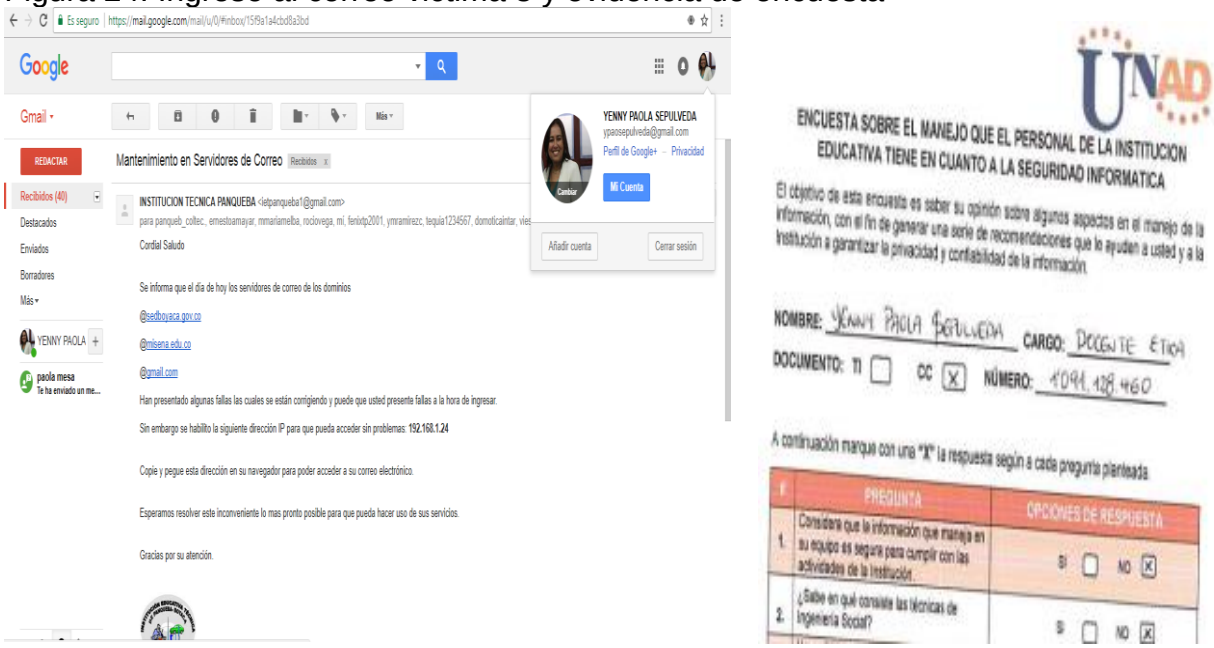
Figura 23. Ingreso en el correo de la víctima 2



Fuente: El Autor

Para el último caso evidenciado se muestra a continuación la figura 24 que muestra que se pudo acceder al email de la docente del área de ética del plantel Educativo.

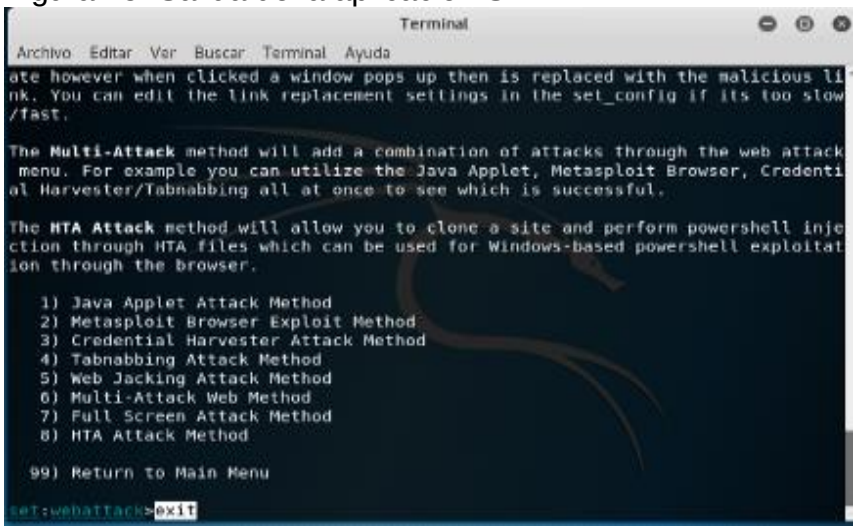
Figura 24. Ingreso al correo victima 3 y evidencia de encuesta



Fuente: El Autor

Después de este proceso que resulta exitoso lo único que queda es dar salida deteniendo el servidor instaurado sin despertar ninguna sospecha.

Figura 25. Salida de la aplicación SET



Fuente: El Autor

7.6 PRACTICA CON TECNICA PRETEXTING

El *Pretexting* es la técnica más conocida como “pretextos” en donde el elemento que usa el actor es el teléfono en donde por medio de una llamada o chat se busca pedir información generalmente simulando ser alguien que solicita ayuda muy importante a partir de tener datos claves para que la otra persona caiga en su enredo.

Este análisis se ha venido llevando a cabo durante el último mes buscando la forma ideal de encaminar una conversación con la víctima teniendo datos básicos que ayudo a detectar ciertos aspectos por medio de una conversación vía Whatsapp claves como lo fue:

- Acceso a la oficina sin la presencia de la secretaria
- Ingreso al correo Institucional
- Descubrimiento de la clave para el ingreso al SIMAT de matrículas.

Los pasos de este proceso fueron los siguientes:

1. Se realizó una llamada a la secretaria del Colegio.

El Ingeniero Social en este caso el autor de este proyecto se enteró por la queja de algunos padres de familia que el proceso de matrícula para el 2018 estaba demorado por inconvenientes que tenía la plataforma del SIMAT y se dio cuenta que días anteriores algunos integrantes del personal de la secretaria de Boyacá estaban en la Institución y en esa ocasión se tuvo la oportunidad de registrar el nombre de uno de ellos en el Carné que portaba.

El paso final fue que se aprovechó que la Secretaria y el Rector el pasado 17 de Noviembre viajaron a Tunja a dar solución a dicho inconveniente y se realizó una llamada a la secretaria mencionando que los integrantes del SIMAT estaban en la Institución, y por chat se evidencia el proceso que facilito el acceso a la oficina de Secretaria del Colegio por medio de la colaboración del Celador y se ve en la figura

26 la conversación en donde el numero celular 3202038995 es el mismo que se evidencia en la web de la institución https://colpanqueba.jimdo.com/

Y la imagen que se muestra en la última opción de la conversación es la misma que se encuentra en el Anexo D de este archivo.

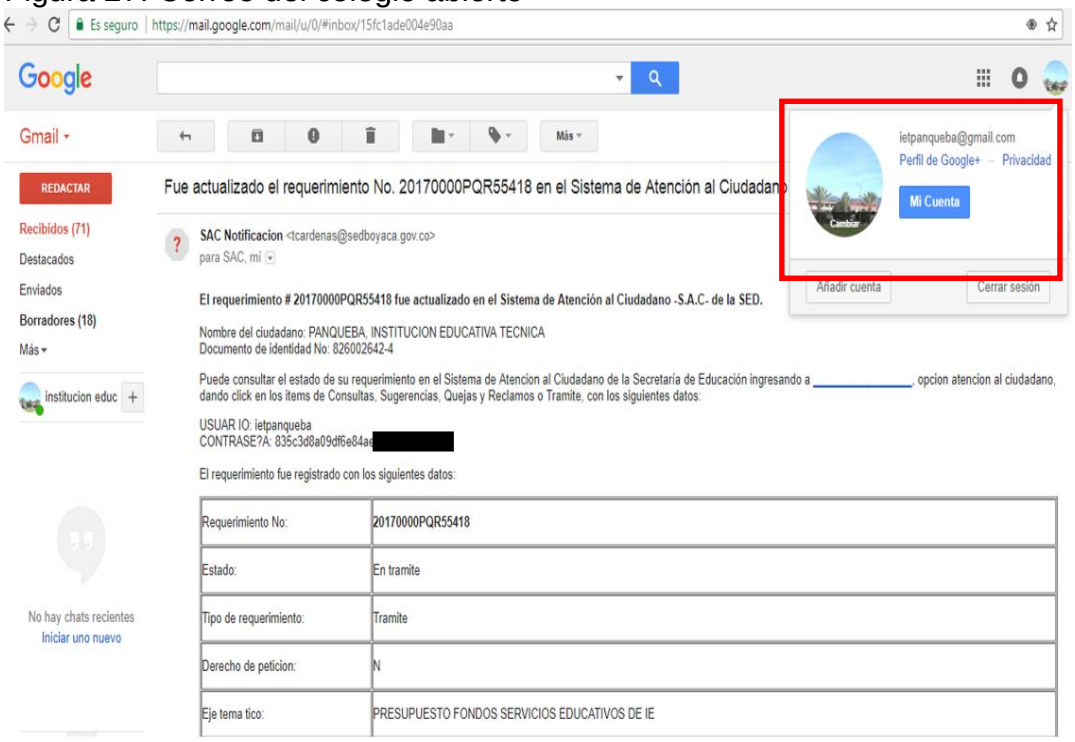
Figura 26. Chat aplicando Pretexting

Fuente: El Autor

1. Acceso al correo institucional

Durante el ingreso a la oficina el computador que usa la secretaria se prendio y al registrar el correo este automáticamente abrió debido a que tenía contraseña guardada automáticamente, el dato del correo se ve en la web institucional https://colpanqueba.jimdo.com/, y se evidencia en la figura 27 el ingreso a la cuenta, aclarando que en el cuerpo del mensaje tape una parte de la clave.

Figura 27. Correo del colegio abierto

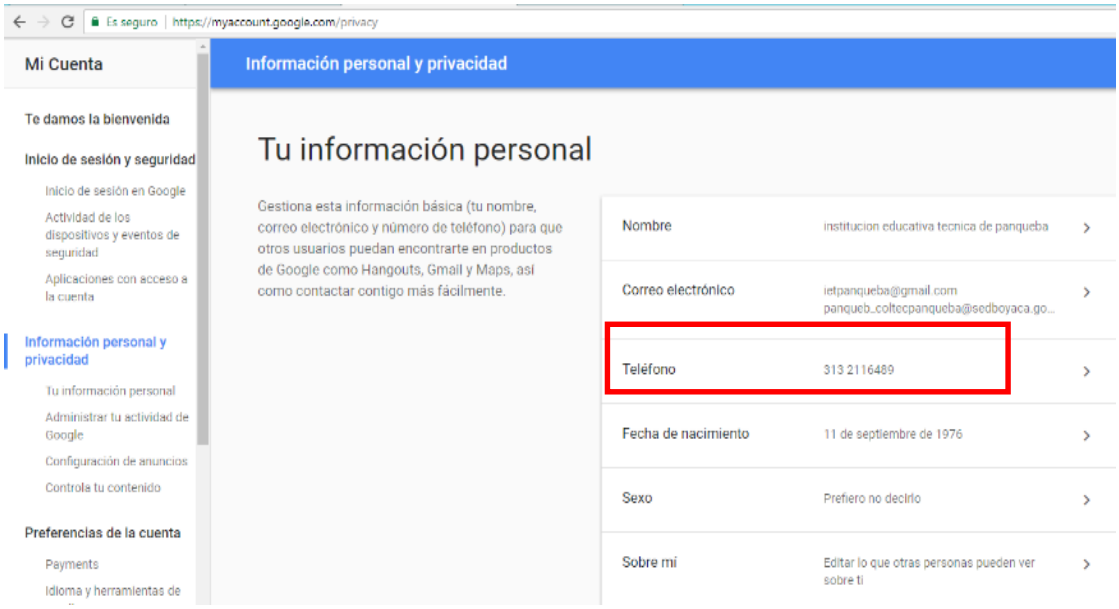


Fuente: El Autor

2. Privacidad del correo

Ya estando en el correo y como el autor del proyecto fue quien ingreso lo único que hice para tomar evidencia y dar más credibilidad a que accedí con esta técnica de *pretexting* es que se va mostrar la opción que registra el número celular que se añadió cuando se creó el usuario de este correo.

Figura 28. Información personal y privacidad



Fuente: El Autor

Este número telefónico que corresponde al rector del plantel Educativo se evidencia en la figura 29 de la página web institucional.

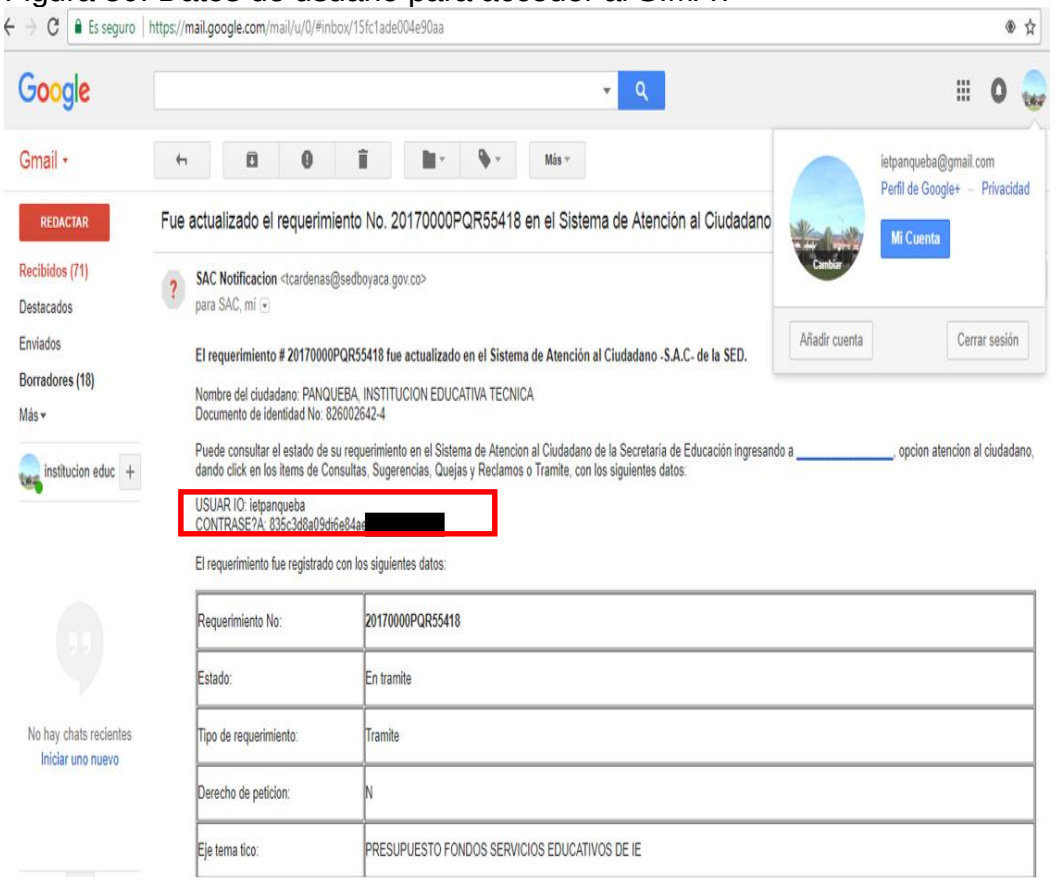
Figura 29. Evidencia de número Rector

Fuente: https://colpanqueba.jimdo.com/directivos/rector/

3. Ingreso a la plataforma de matrícula del SIMAT.

Para seguir proporcionando más evidencias claras en este proyecto se procede a acceder a la plataforma del SIMAT en donde por medio de la ayuda de un correo proveniente de la secretaria de Boyacá con el registro de usuario del Rector se realizó la acción.

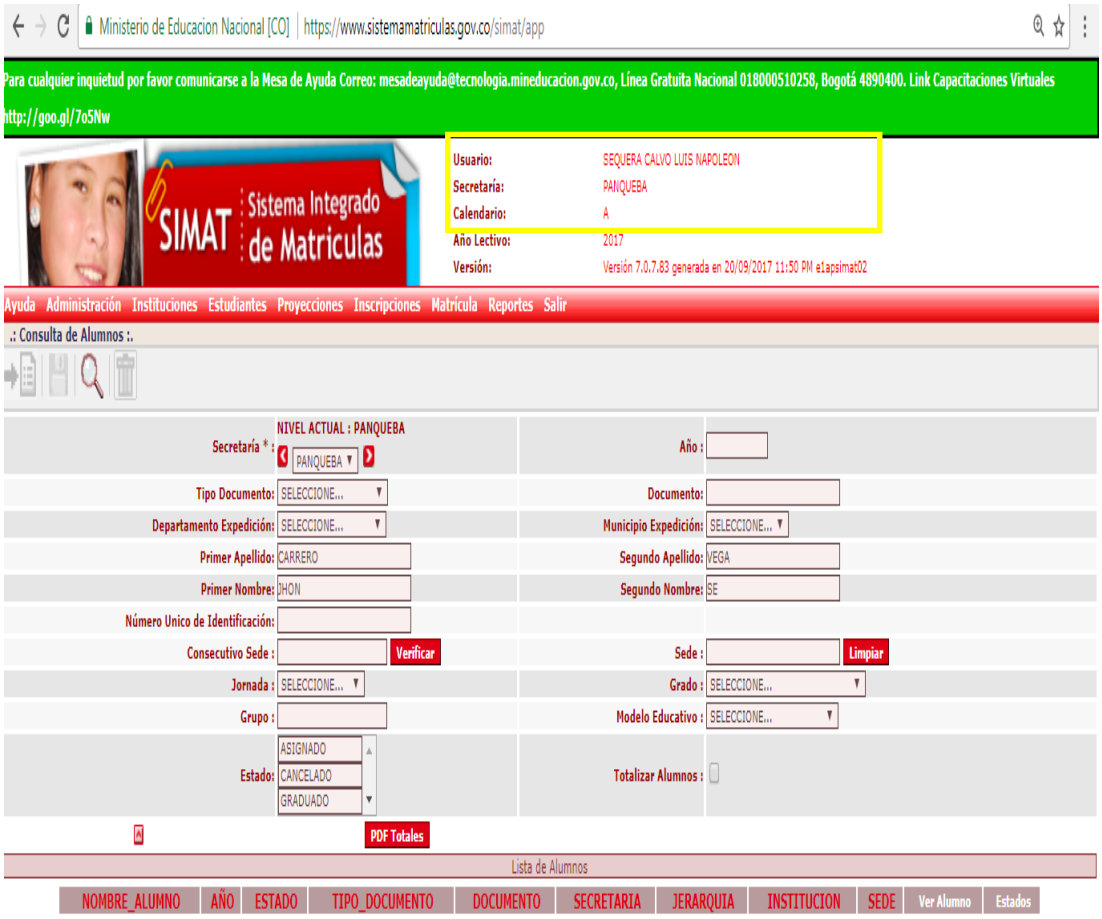
Figura 30. Datos de usuario para acceder al SIMAT



Fuente: El Autor

Ya con estos a la mano se logró acceder a la plataforma de matrículas del colegio donde se revela el nombre del Rector en el recuadro amarillo de la figura 31.

Figura 31. Acceso al SIMAT con login del Rector



Fuente: https://www.sistemamatriculas.gov.co/simat/app

- Con el último objetivo se deja de forma física ya que es Generar un manual de seguridad con las recomendaciones para evitar ser víctima de Ingeniería Social implementando estrategias de prevención de delitos informáticos y así fomentar cultura social y educativa.

Este objetivo se entrega impreso en la Institución, al igual queda plasmado en la página web institucional, también como estrategia de apoyo se tienen en cuenta las capacitaciones que se vienen haciendo el último jueves de cada mes para que todo el personal sea consiente de cómo debe actuar ante las diversas estrategias que pueden poner en riesgo la confiabilidad de la información y así lograr prevenir que alguien sea víctima de la Ingeniería Social.

8. RECURSOS DISPONIBLES

Este Proyecto está liderado por el Ingeniero de Sistemas WILLIAM JAVIER CORDERO SALCEDO, quien se ha desempeñado como Instructor SENA en el área de Sistemas en este colegio dando cumplimiento a las 3 competencias del Programa de Formación que orienta como lo son:

- Aplicar herramientas ofimáticas y herramientas TIC en diferentes contextos.
- Ejecutar el Mantenimiento Predictivo y correctivo de equipos de cómputo
- Implementar la estructura de redes cableadas o inalámbricas.

8.1 RECURSOS MATERIALES E INSTITUCIONALES

Para poder llevar a cabo el proceso del desarrollo del diagnóstico y documentación del proyecto se utilizará un portátil de propiedad del autor del proyecto y algunos elementos físicos de la institución, los elementos usados fueron:

Tabla 13. Recursos Materiales e Institucionales

ELEMENTO	CARACTERISTICAS - CANTIDAD
1 Portátil	ASUS de 12”
Disco Duro	1 Terabyte
Procesador	Intel Core 5 4,60 GHz
Memoria RAM	4 Gigabyes
Sistema Operativo	Windows 10 y Kali Linux
Versión de Office	Office 2016
Antivirus	McAfee
Equipos de escritorio de la Institución	25
Portátiles de la Biblioteca	15
Fotocopiadora	2
Impresora	2
Escáner	1

Fuente: El Autor

8.2 RECURSOS FINANCIEROS

En el desarrollo del proyecto es necesario de unos aportes económicos que fueron fundamentales para llevar a cabo la ejecución del proyecto.

Haciendo una recopilación de los requisitos y costos que se necesitaron y se implementaron en la elaboración del proyecto se determinó los siguientes valores en donde el encargado del Proyecto y la Institución hacen acuerdo de la distribución de lo que se necesitó:

Tabla 14. Presupuesto

ELEMENTO	CANTIDAD	VALOR UNITARIO	VALOR TOTAL
Persona Encargada del Proyecto: Ingeniero William Javier Cordero	80 horas	Valor Hora $30.000	2´400.000
Conexión banda ancha Mensual	1 plan	50.000	50.000
Resma de Papel	1	10.000	10.000
Tintas impresora	2	90.000	180.000
Varios (transporte, servicio de fotocopiadora)		260.000	260.000
TOTAL			**2´900.000**

Fuente: El Autor

9. RESULTADOS ESPERADOS

9.1 RESULTADOS DEL PROYECTO

A continuación se menciona lo que se espera dentro del proyecto:

- Listado con los activos con que cuenta la Institución. (Tabla)

- Información relativa sobre metodologías de Ingeniería Social.

- Resultados de la encuesta aplicada al personal del Colegio. (Graficas Tabuladas y conclusión sobre cada pregunta)

- Resultados de los test y pruebas en ambientes controlados sin infringir la ley. (Pantallazos de la Practica de *Spoofing y Pretexting*).

- Manual de buenas prácticas y recomendaciones para prevenir la Ingeniería social.

9.1.1 Identificación de Activos. La Institución cuenta con una serie de activos los cuales tienen un valor correspondiente, como se ve en la tabla 1.

• M: Medio • A: Alto • MA: Muy alto

Tabla 15. Identificación de Activos

TIPO ACTIVO	DESCRIPCIÓN	VALORACIÓN DE ACTIVOS
HARDWARE	[pc] 60 computadores distribuidos en 2 salas de sistemas [pc] 20 portátiles en área de la biblioteca [pc] 5 equipos en el área de secretaria, rectoría y área administrativa [print] 4 impresoras [scan] 4 escáner [Switch] 3 switches de red.	Alto (A)

Fuente: El Autor

Tabla 15. (Continuación)

TIPO ACTIVO	DESCRIPCIÓN	VALORACIÓN DE ACTIVOS
ACTIVO DE INFORMACIÓN	*Bases de datos *Sistema Notas de los alumnos *Página web de la Institución *Contratos *Normativas *Copias de respaldo *Datos de configuración *Contraseñas *Registro de actividad	Muy Alto (MA)
RED	Redes de comunicación e Internet [wi-fi] 2 zonas de acceso inalámbrico [LAN] red local en Biblioteca	Muy Alto (MA)
SOFTWARE O APLICACIÓN	[Browser] Navegador web: Google Chrome y Safari [office] ofimática: Office 2013 y 2016 [av] Antivirus: Avast y McCaffe [os] Sistema Operativo: Windows 10, Windows 8 *Servidor de aplicaciones *Servidor de correo electrónico *Sistema de gestión para bases de datos	Muy Alto (MA)
EQUIPAMIENTO AUXILIAR	[disk] discos duro Hitachi [usb] memorias USB [dvd] DVD [power] fuentes de alimentación [ups] sistemas de alimentación [cabling] cableado [wire] cable eléctrico	Medio (M)

Fuente: El Autor

Tabla 15. (Continuación)

TIPO ACTIVO	DESCRIPCIÓN	VALORACIÓN DE ACTIVOS
INSTALACIÓN	[building] edificio 3 pisos [local] cuarto [channel] canalización [backup] instalaciones de respaldo	Medio (M)
SERVICIOS	Redes internas y externas de las diferentes oficinas que cuenta el colegio [PSTN] red telefónica [wifi] Red inalámbrica. [mobile] telefonía móvil [LAN] red local	Medio (M)
PERSONAL	[ue] usuarios externos [ui] usuarios internos [dba] administradores de BBDD Junta Directiva Coordinación Académica	Alto (A)

Fuente: El Autor

9.1.2 Identificación de amenazas. En cuanto a la identificación de las amenazas con sus respectivas valoraciones de impacto y riesgos, se toma como base la metodología MAGERIT.

A continuación se definen los pasos que se deben seguir:

1. Elegir los activos relevantes para la Organización.
2. Identificar las posibles amenazas en cada activo.
3. Determinación de qué tipo de protección existe para estos activos y que tan fuertes y efectivas son para estos riesgos.
4. Valorar el impacto en caso de que se ejecuten las posibles amenazas.
5. Valorar el riesgo con base en el impacto de la tasa de ocurrencia de las amenazas.

En este análisis se determina que el Colegio tiene 14 tipos de amenazas que involucran riesgo en los activos que se tienen y se muestran en la tabla 16.

Tabla 16. Identificación de Amenazas

AMENAZAS	
1	Daños por Fuego
2	Daños por agua
3	Corte del suministro eléctrico
4	Condiciones inadecuadas de temperatura o humedad
5	Fuga de información
6	Corrupción de la información
7	Destrucción de información
8	Difusión de software dañino
9	Errores en actualización de aplicaciones
10	Errores de mantenimiento de equipos hardware
11	Pérdida de equipos
12	Abuso de privilegios
13	Acceso no autorizado
14	Robo

Fuente: El Autor

10. DIVULGACIÓN

La divulgación de este proyecto se ejecutó en la Institución Educativa Técnica de Panqueba municipio de la Provincia de Norte y Gutiérrez del departamento de Boyacá.

Allí por medio de esta propuesta se llevó a cabo actividades como capacitaciones, conversatorios, puesta en marcha de técnicas de Ingeniera social y de forma física se dejó un manual con recomendaciones para no ser víctima de los curiosos informáticos y así concientizar al plantel educativo que la información es el activo más importante y el cual se debe proteger siguiendo una serie de pasos que garantice los cuatro pilares de la información.

De igual manera se espera compartir este proyecto en el repositorio o espacio que tenga asignado la UNAD en la nube para que se dé a conocer la propuesta ejecutada en la Institución que generó cambios en el personal en cuanto al ámbito informático.

11. CONCLUSIONES

1. Aplicando el primer objetivo por medio de la investigación sobre estrategias de Ingeniería Social se logró identificar el nivel de vulnerabilidad en donde se concluye que cualquier integrante del plantel educativo es muy fácil capturar la información que desempeña en su rol debido a que son muy escasos los conocimientos de la mayoría en el manejo del ámbito informático y queda evidenciado en la observación, el desarrollo de la encuesta y la práctica que se llevó a cabo.

2. Resulto muy positivo según el segundo objetivo en donde se aplicó metodologías de Ingeniería social para aplicar al personal que usa equipos de cómputo en la Institución Educativa ya que se vio cuáles son las mayores falencias que se deben corregir.

3. Por medio de la encuesta, entrevistas y una serie de preguntas se obtuvo información clave para obtener datos y así por medio de la implementación de técnicas de Ingeniería Social se logró cumplir con el tercer objetivo.

4. Se hizo el compromiso con los docentes de que a medida que lleguen alumnos nuevos reunirlos de forma periódica y darles a conocer el manual que se dejó para la Institución sobre Recomendaciones de Seguridad Informática.

5. Se plantea junto a los dos docentes del área de Informática dar continuidad a las capacitaciones que se llevaron a cabo en la parte de actualizaciones tecnológicas y manejo de seguridad informática con el fin de consolidar algunos aspectos de sistemas en el plantel educativo.

6. Se determinó más control en la entrada de la Institución puesto que el día que se ejecutó la prueba de *pretexting* no hubo ninguna sospecha de la persona que acompaño a la oficina de la secretaria, y además se observa la facilidad de ingresar cualquier elemento informático para cambiarlo por otro.

7. Se manifestó a los administrativos de la Institución Educativa que se debe validar la información que se solicita vía telefónica o por chat ya que estas personas usan estos indicios con la intención de ir consiguiendo detalles para acceder a la información.

8. El personal de la Institución se compromete a destruir los documentos con información sensible antes de desecharlos, esto con el fin de no dejar ni el más mínimo detalle que sirva de evidencia para los curiosos.

9. Por parte del Rector se dio la orden de que las claves de WI-FI queden protegidas en los equipos para así no facilitarla a cualquier persona que accede a servicios como biblioteca y ludoteca.

10. Se estableció la instalación del programa *Deep Freeze* en las salas de sistemas para que las dos particiones queden congeladas y así evitar problemas de seguridad muy comunes cuando estos equipos se dejan libres.

11. Se aconsejó reubicar tres cámaras de seguridad hacia las entradas de las salas de sistemas debido a que en el transcurso del año se han perdido ciertos dispositivos sin encontrar el responsable del hecho.

12. RECOMENDACIONES

- La Institución Educativa para el 2018 debe dar continuidad a las capacitaciones que se llevaron a cabo el segundo semestre del presente año y así establecer un cronograma de capacitación de forma periódica para todo el plantel basado en las últimas novedades de la seguridad informática con el objetivo principal de consolidar una cultura de protección de la información dentro la institución.

- Se aconsejó al Rector del Colegio en la ampliación del número de cámaras de seguridad con los que cuenta, esto debido a que la institución últimamente está siendo dotada por parte de computadores para educar y Vive digital de activos de gran valor que se deben cuidar en las áreas asignadas.

- Se debe generar un control que evite que los estudiantes puedan compartir recursos en la red, la forma aconsejable es negando los privilegios a las cuentas de usuario en cada equipo o desde el controlador de dominio.

- Una idea que se propuso al docente del área de Sistemas y a los aprendices SENA que terminan el año entrante la Formación es que apliquen como proyecto de grado la implementación de la identificación biométrica o electrónica a través de los códigos de barras de los carnet institucionales.

- Se debe concientizar que la papelería que se arroja a la basura y que pueden contener datos valiosos se debe destruir por completo.

- En el entorno de infraestructura la Institución debe reubicar en algunas oficinas los puestos de trabajo y demás dispositivos ya que es una falencia que cualquier persona que visita la Institución lo va notar en algunos sitios.

- Se recomienda periódicamente cambiar la contraseña de acceso a las redes inalámbricas que dispone la Institución con el fin de evitar que se saturen y se vuelvan lentas lo cual ha sido la constante en los meses que se desarrolló el proyecto.

- En cuanto a los puntos de red del cableado estructurado con que cuenta el plantel educativo y que se encuentran al alcance de cualquier persona se aconseja mantenerlos desconectados y así evitar daños en la estructura del cableado UTP.

- Se acordó con las directivas del Colegio bloquear o restringir el acceso a algunas páginas de internet, ya que esta idea genera beneficios en el desempeño educativo de los estudiantes e incentiva el uso de páginas de investigación acordes a la planeación de la formación de cada área.

- Las directivas de la Institución se comprometieron a tramitar software original en algunos equipos que no cuentan con este aspecto para así evitar cometer delito en cuanto a promover el uso de software pirata.

- Se estableció que la Secretaria de la Institución va cumplir la directriz de realizar copias de seguridad de forma periódica sobre las bases de datos y plataformas institucionales que maneja el Colegio.

BIBLIOGRAFÍA

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

ARCOS, Sergio. 2011. Tesís Ingeniería social: Psicología aplicada a la seguridad informática. Madrid. s.n., 2011.

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

Hernández Flores Geovanna Belén. 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.

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

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

TIC CONSULTING, Claves de Ingenieria Social, [En línea] 31 Enero 2011. [Revisado 5 septiembre 2017]. disponible en: http://www.ticsconsulting.es/blog/generar-claves-seguras-3

Cisco. (2017). Seguridad para redes empresariales. [En línea] [Revisado 5 Octubre 2017]. Disponible en: http://www.cisco.com/c/es_mx/solutions/enterprise-networks/enterprise-network-security/index.html

Datos instucionales de la Institucion Tecnica Panqueba, [En línea] Enero 2012. [Revisado 2 Septiembre 2017]. Disponible en: https://colpanqueba.jimdo.com

ENTER. 2016. Ingenieria social: El hackeo silencioso. [En línea] 25 de Julio de 2016. [Revisado 20 Septiembre 2017]. Disponible en: http://www.enter.co/guias/tecnoguias-para-empresas/ingenieria-social-el-hackeo-silencioso

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

Ley 1273 de 2009. Mayo 03 de 2017. [En línea] [Revisado 1 Septiembre 2017]. Disponible en: http://www.mintic.gov.co/portal/604/w3-article-3705.html

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

Métodos de Ingeniería Social, [En línea] [Revisado 25 Septiembre 2017]. Disponible en: https://deepwebiupsm.wordpress.com/category/ingenieria-social/

OPENBSDCOLOMBIA. 2010. Ingenieria social. [En línea] Diciembre de 2010. [Revisado 15 Octubre 2017]. Disponible en: http://www.openbsdcolombia.org/documentos/others/IngenieriaSocial_CasodeEstudio.pdf

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

PENAGOS BERMUDEZ, Edilberto. 2015. INGENIERÍA SOCIAL, UN FACTOR DE RIESGO INFORMÁTICO INMINENTE EN. Neiva: Tesis de grado Especializacion, 2015.

Seguridad y privacidad de la información. [En línea] Mayo 03 de 2017. [Revisado 1 Septiembre 2017]. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G3_Procedimiento_de_Seguridad.pdf

Técnicas de ingeniería Social, [En línea] [Revisado 5 Octubre 2017]. Disponible en:https://www.welivesecurity.com/la-es/2014/05/21/tecnicas-ingenieria-social-evolucionaron-presta-atencion/

WEBSECURITY. 2017. La Ingeniería social [En línea] abril de 2017. [Revisado 17 Septiembre 2017]. Disponible en http://www.websecurity.es/ingenier-social-introduccion

ANEXO A. Carta de aceptación del Colegio

SECRETARIA DE EDUCACION DE BOYACA
Institución Educativa Técnica de Panqueba
Aprobado por Res. De las S.E. No. 000047 del 16 de enero de 2009.
NIT. 826002642-4 DANE: 115522000126
Carácter Oficial. Jornada Ordinaria

Panqueba, Octubre 20 de 2016

Señor:
WILLIAM JAVIER CORDERO SALCEDO
INGENIERO DE SISTEMAS
Málaga – Santander

Respetado Ingeniero

Por medio de la presente en mi condición de Rector de la Institución Educativa Técnica de Panqueba, me permito notificarle que de acuerdo a su solicitud para desarrollar su trabajo de grado: "**IMPLEMENTACION DE TECNICAS DE INGENIERIA SOCIAL EN LA INSTITUCION EDUCATIVA TECNICA DE PANQUEBA**", para optar el título de Especialista en Seguridad Informática ha sido **APROBADA** por esta entidad para que a partir de la fecha inicie el desarrollo del proyecto.

Cordialmente,

LUIS NAPOLEON SEQUERA
Rector
C.C 4´113.510 de El Cocuy

ANEXO B. Encuesta

ENCUESTA SOBRE EL MANEJO QUE EL PERSONAL DE LA INSTITUCION EDUCATIVA TIENE EN CUANTO A LA SEGURIDAD INFORMATICA

El objetivo de esta encuesta es saber su opinión sobre algunos aspectos en el manejo de la información, con el fin de generar una serie de recomendaciones que le ayuden a usted y a la Institución a garantizar la privacidad y confiabilidad de la información

NOMBRE: _____ **CARGO:** _____

DOCUMENTO: TI ☐ CC ☐ **NÚMERO:** _____

A continuación marque con una **"X"** la respuesta según a cada pregunta planteada.

#	PREGUNTA	OPCIONES DE RESPUESTA
1.	Considera que la información que maneja en su equipo es segura para cumplir con las actividades de la Institución	SI ☐ NO ☐
2.	¿Sabe en qué consiste las técnicas de Ingeniería Social?	SI ☐ NO ☐
3.	Ha recibido llamadas, correos electrónicos o por chat solicitudes donde le piden datos personales o de su Institución.	SI ☐ NO ☐
4.	¿Se siente seguro con el antivirus de su equipo?	SI ☐ NO ☐ NO USA ANTIVIRUS ☐
5.	¿Qué causas han afectado la seguridad de su información? "Puede marcar más de una"	☐ Virus. ☐ Fallas de Programas. ☐ Spam o correo no deseado ☐ Daño en el hardware. ☐ Perdida de claves. ☐ Mal uso de redes sociales. ☐ Ninguna.
6.	¿Cambia frecuentemente sus contraseñas?	SI ☐ NO ☐
7.	Alguien más sabe las contraseñas que usted usa en su ámbito de Sistemas.	SI ☐ NO ☐
8.	¿Cuándo crea una contraseña la establece teniendo en cuenta que parámetros? "Puede marcar más de una"	☐ Combina números, mayúsculas y minúsculas. ☐ Longitud menor a 8 caracteres. ☐ Usa solo letras. ☐ Usa solo números. ☐ Coloca palabras comunes. ☐ Usa caracteres como #$%&/()=?
9.	De los siguientes medios de comunicación cuál cree que puede afectar su información "Puede marcar más de una"	☐ Correo. ☐ Chat. ☐ Descargas. ☐ Redes sociales. ☐ Usar software en línea.
10.	¿Ha recibido capacitación sobre temas de seguridad informática?	SI ☐ NO ☐
11.	En su experiencia de manejo de computador, celular y redes sociales que mensajes curiosos ha encontrado en sus dispositivos. "Puede marcar más de una"	☐ Ganaste un premio. ☐ Actualice aquí su cuenta bancaria. ☐ Digite la clave de su equipo sino perderá la información del disco. ☐ Clic acá y participa del sorteo. ☐ Otras que generan caos.
12.	Considera que el ingreso a las instalaciones de su Institución son aptas y confiables.	SI ☐ NO ☐

4 – OCTUBRE - 2017

ANEXO C. Evidencia fotográfica diligenciamiento encuesta

ANEXO D. Solicitud para técnica de Pretexting

SIMAT Sistema Integrado de Matriculas

Panqueba, 17 de Noviembre 2017

Notificación:

Dando respuesta a su solicitud de requerimiento queremos informar que su Institución Educativa fue actualizada en el sistema de atención al ciudadano S.A.C de Boyacá.

Los datos registrados en el sistema y que se enviaron vía correo electrónico hace unas semanas fueron validados en el servidor de base de datos y ya está a disposición ingresando a https://www.sistemamatriculas.gov.co/simat/app, con el mismo usuario y contraseña que tenía asignado.

Usuario: ietpanqueba
Contraseña: 835c3d8a09df6e84ae

WILLIAM FERNEY SALCEDO
Administrador Ejecutivo S.A.C de Boyacá.
CC 4´583.510 de Tunja

ANEXO E. Manual de Seguridad

RECOMENDACIONES EN SEGURIDAD:

A continuación se da a conocer un manual de seguridad que enfoca 10 ítems generales del ámbito informático que por medio de acciones se debe tener una serie de precauciones para así darle el uso adecuado a la información y cumplir con mantener los 4 pilares de dicha información.

CONTENIDO

SEGURIDAD EQUIPO DE TRABAJO

RECOMENDACIONES

1. Estar actualizado de las novedades tecnológicas y visitar páginas web confiables sobre alertas de seguridad.
2. Mantener actualizado el Sistema Operativo y su paquete de aplicaciones.
3. Hacer periódicamente copias de seguridad en unidades extraíbles y evitar pérdida de datos.
4. Instalar software con licencia y garantía y no de páginas web desconocidas que ofrecen en el mercado.
5. Utilizar contraseñas con combinación de números, letras, caracteres.
6. Utilizar herramientas de seguridad (antivirus, antispyware, firewall) que ayuden a proteger de amenazas en la Red.

7. Crear diferentes usuarios y asignar algunos permisos para realizar determinadas acciones según los roles.
8. Dejar el equipo bloqueado cuando se levante del puesto de trabajo

CORREO ELECTRONICO

RECOMENDACIONES

1. Utilizar un filtro con función anti-spam para evitar llegada de correo no deseado.
2. No abrir ficheros adjuntos sospechosos que llegan de correos desconocidos.
3. Analizar con antivirus los archivos del buzón de entrada así sean correos conocidos antes de ejecutarlos en el computador.
4. No dar la opción de guardar contraseña en los navegadores que piden esa confirmación de usuario
5. No facilitar la dirección de correo a desconocidos ni publicarla en cadenas o en sitios que todo mundo pueda ver.
6. Desactivar la vista previa del cliente de correo para que en el cuerpo de los mensajes no se incluya código malicioso.

ACCESO A INTERNET

RECOMENDACIONES

1. Personalizar el nivel de seguridad del navegador en modo alto.
2. Descargar programas desde sitios oficiales para evitar entrada de código malicioso o inconvenientes en el hardware.
3. Eliminar el historial del navegador constantemente.
4. Analizar con un antivirus todas las descargas antes de ejecutar en el equipo.
5. Nunca diligencie formularios donde le pidan cualquier tipo de dato personal o laboral.

6. Configurar algún usuario sin permisos de acceso de Administrador para entrar a Internet con la intención de impedir modificaciones en el sistema o instalación de programas.
7. Actualizado el navegador para que esté protegido contra vulnerabilidades que traen algunos parches.
8. Instalar un cortafuego que impida accesos no deseados desde Internet.
9. Utilizar anti-dialers con la intención de evitar conectarse a Internet a través de ciertos números que generan tarificación adicional que se suman en la factura.
10. Activar la opción de borrar archivos temporales, cookies y el historial cuando este en otros ambientes del medio para no dejar evidencias de las actividades que realizo.

DISPOSITIVOS TECNOLOGICOS

RECOMENDACIONES

1. Instalar antivirus y realizar análisis constantes para proteger de cualquier código malicioso.

2. No hacer caso a los mensajes de texto de desconocidos que lo inducen a descargar o enviar códigos o pines.
3. No aceptar conexiones de dispositivos desconocidos para evitar transferencia de contenido no deseado.
4. Configurar el móvil en modo oculto para evitar ser descubierto por atacantes.
5. Hacer caso omiso a mensajes de cadenas donde pidan datos personales.
6. Bloquear la SIM Card para evitar que otros usen su identidad para actividades ilícitas.
7. No descargar software de tiendas online poco fiables y así evitar la entrada potencial de código malicioso.

COMERCIO ELECTRÓNICO

RECOMENDACIONES

1. Verificar que el “inicio de la dirección web” tiene el httpS que revela que es una conexión segura.
2. Observar que aparezca un “candado” al lado de la página web lo que indica que la conexión es segura.
3. Corroborar la validez que tienen los certificados dando clic en el candado donde debe coincidir con la entidad solicitada garantizando vigencia y validez.

4. Nunca envié datos personales ya que ninguna entidad los pedirá de esta forma ni por teléfono.
5. Haga transacciones comerciales desde su equipo personal y evite el uso de equipos públicos para estas actividades.
6. Desactivar la opción “autocompletar” para no dejar indicios de usuario.
7. Siempre cierre sesión de sus cuentas, en casos que la energía se vaya se recomienda acudir a otro sitio y realizar cambios de clave ya que en varias ocasiones cuando llega la luz las cuentas quedan abiertas.

8. Configurar una herramienta antifraude para restringir el acceso a páginas fraudulentas o suplantadas por ingenieros sociales.

MENSAJERIA INSTANTANEA

RECOMENDACIONES

1. No facilitar datos confidenciales (contraseñas, nombres de usuario, números de cuenta, etc.).
2. No dar clic en link de desconocidos que lo lleven a enlaces sospechosos.
3. No divulgue información más de lo normal en redes sociales ya que con esto se da inicio a los seguimientos de sus actividades.
4. Rechace invitaciones donde la imagen sea alguien llamativo que despierta curiosidad pues acá estas técnicas son de Ingeniería Social para empezar a capturar datos.
5. Vaciar el historial del chat.

ZONAS WI-FI

RECOMENDACIONES

1. Activar el filtrado de la dirección MAC con la intención de que solo ciertos dispositivos autorizados accedan a la red.
2. Cambiar contraseñas periódicamente para evitar bajo rendimiento en la señal de transmisión.
3. Tratar de no divulgar la clave para que no se disocie ese dato.
4. Desactivar la opción de SSID es decir el nombre de su red para que nadie la identifique automáticamente.
5. Elegir un límite bajo de computadores que se puedan conectar al Access Point y cuando a este no se le vaya a dar uso apagarlo.
6. Utilizar el tipo de encriptación WPA para así impedir que el tráfico de la red sea fácilmente legible.

RESTRICCIÓN EN MENORES DE EDAD

RECOMENDACIONES

1. Concientice al menor de edad dando a entender los posibles peligros que puede encontrar con el uso de internet.
2. Este al tanto y vigile lo que ellos realizan cuando navega en la web o hace uso de redes sociales.
3. Explique las consecuencias que puede generar si facilitar información personal a desconocidos.
4. Oriente por medio de ejemplos los casos comunes y que por medio de la astucia usan los ingenieros sociales para averiguar información.
5. Restrinja horarios de uso de los medios informáticos.
6. Generar ambiente de confianza con el fin de que sea informado de alguna mala conducta o situaciones que pueden afectar la integridad del ser humano.
7. Utilizar herramientas de control parental para filtrar cierto uso de contenido para menores de edad.
8. Administre las cuentas en línea que ellos tienen para llevar un control de sus actividades.
9. Aconsejar que si recibe cualquier tipo de mensaje, llamada u otro servicio donde le soliciten información de los padres de familia no la den.

JUEGOS EN LINEA

RECOMENDACIONES

1. No adquirir créditos en aquellas páginas de subastas en línea sin que estén certificados por el diseñador del juego.

2. No descargue este tipo de juegos en plataformas poco conocidas.

3. Restrinja la opción de compartir algún usuario y contraseña dentro y fuera de la plataforma online del juego.

4. Si recarga o paga mensualidades con tarjeta bancaria que se asocia al juego hágalo desde su equipo personal y no guarde datos de la cuenta de usuario y así se evitan cualquier movimiento ilícitos.

5. Distribuir el tiempo para este hobbie ya que puede ser muy adictivo.

REDES P2P

RECOMENDACIONES

1. Analizar todos los archivos que se descargan a través de las redes.

2. No compartir en línea software ilegal porque acarrea cometer delitos.

3. Ejecutar el cliente P2P en algún usuario que tenga ciertos permisos limitados.

4. Verificar la extensión de los ficheros que se descarga ya que hay puede haber software malicioso, en especial con archivos de extensión (.exe).

ANEXO F. Resumen Analitico

Título de Documento.	IMPLEMENTACION DE TECNICAS DE INGENIERIA SOCIAL EN LA INSTITUCION EDUCATIVA TECNICA DE PANQUEBA
Autor	WILLIAM JAVIER CORDERO SALCEDO
Palabras Claves	Seguridad, integridad, disponibilidad, confidencialidad, autenticidad, Ingeniería Social, activos, hardware, software, redes.

Descripción

En la actualidad una buena parte de las Instituciones Educativas del departamento de Boyacá se apoyan en el uso de las TIC para realizar aquellas actividades que a diario se gestionan en su entorno laboral con el fin de cumplir a cabalidad todas sus funciones como ente educativo.

Las entidades educativas tienen como propósito implementar sistemas de seguridad para proteger recursos y activos informáticos por medio de mecanismos de seguridad en sus sistemas de información en la búsqueda de evitar errores y mal funcionamiento en los procesos, retraso de las actividades, y pérdidas de dinero, credibilidad del buen nombre de la Institución Educativa y obtener mayor rendimiento en la ejecución de sus procesos.

La Institución Técnica de Panqueba en sus procesos informáticos se encuentra en vulnerabilidad de perder información ya que nunca se han tenido en cuenta procesos al momento de proteger la información; estas vulnerabilidades deben ser analizadas y revisadas por medio de un diagnostico como se plantea en uno de los objetivos para que por medio de las distintas metodologías de Ingeniería Social se defina qué medidas de control se debe tomar para minimizar los riesgos inminentes que representen estas fallas.

Con esto se establece dejar como evidencia final a los usuarios un manual de políticas de seguridad y recomendaciones implementando estrategias de prevención de delitos informáticos e Ingeniería social y así fomentar cultura social y educativa.

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

Fuentes Bibliográficas	ARCOS, Sergio. 2011. Tesís Ingeniería social: Psicología aplicada a la seguridad informática. Madrid. s.n., 2011. CONHEADY, Sharon. Social Engineering in IT Security: Tools, Tactics, and Techniques: Testing Tools, Tactics & Techniques. McGraw Hill Professional, 2014. Hernández Flores Geovanna Belén. 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. HINOJOSA JARAMILLO, Lucia Gabriela. Estudio del grado de incidencia de la ingeniería social en la primera fase de los ataques informáticos que se realizan actualmente en las empresas privadas del ecuador. Trabajo de grado Ingeniero de Sistemas. Quito: Universidad Internacional SEK. Facultad de Ciencias y Telecomunicaciones, 2010. 186 p. MANN, Lan. Hacking the Human: Social Engineering Techniques and Security Countermeasures. Ed. Gower Publishing, Ltd., 2012. Pg. 266. ISBN 1409458288. TIC CONSULTING, Claves de Ingenieria Social, [En línea] 31 Enero 2011. [Revisado 5 septiembre 2017]. disponible en: http://www.ticsconsulting.es/blog/generar-claves-seguras-3 Cisco. (2017). Seguridad para redes empresariales. [En línea] [Revisado 5 Octubre 2017]. Disponible en: http://www.cisco.com/c/es_mx/solutions/enterprise-networks/enterprise-network-security/index.html

Datos instucionales de la Institucion Tecnica Panqueba, [En línea] Enero 2012. [Revisado 2 Septiembre 2017]. Disponible en: https://colpanqueba.jimdo.com

ENTER. 2016. Ingenieria social: El hackeo silencioso. [En línea] 25 de Julio de 2016. [Revisado 20 Septiembre 2017]. Disponible en: http://www.enter.co/guias/tecnoguias-para-empresas/ingenieria-social-el-hackeo-silencioso

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

Ley 1273 de 2009. Mayo 03 de 2017. [En línea] [Revisado 1 Septiembre 2017]. Disponible en: http://www.mintic.gov.co/portal/604/w3-article-3705.html

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

Métodos de Ingeniería Social, [En línea] [Revisado 25 Septiembre 2017]. Disponible en: https://deepwebiupsm.wordpress.com/category/ingenieria-social/

OPENBSDCOLOMBIA. 2010. Ingenieria social. [En línea] Diciembre de 2010. [Revisado 15 Octubre 2017]. Disponible en: http://www.openbsdcolombia.org/documentos/others/IngenieriaSocial_CasodeEstudio.pdf

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

PENAGOS BERMUDEZ, Edilberto. 2015. INGENIERÍA SOCIAL, UN FACTOR DE RIESGO INFORMÁTICO INMINENTE EN. Neiva: Tesis de grado Especializacion, 2015.

Seguridad y privacidad de la información. [En línea] Mayo 03 de 2017. [Revisado 1 Septiembre 2017]. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G3_Procedimiento_de_Seguridad.pdf

Técnicas de ingeniería Social, [En línea] [Revisado 5 Octubre 2017]. Disponible en:https://www.welivesecurity.com/la-es/2014/05/21/tecnicas-ingenieria-social-evolucionaron-presta-atencion/

WEBSECURITY. 2017. La Ingeniería social [En línea] abril de 2017. [Revisado 17 Septiembre 2017]. Disponible en http://www.websecurity.es/ingenier-social-introduccion

CONTENIDO:

IMPLEMENTACION DE TECNICAS DE INGENIERIA SOCIAL EN LA INSTITUCION EDUCATIVA TECNICA DE PANQUEBA

- **DESCRIPCIÓN DEL PROBLEMA:**

En la actualidad una buena parte de las Instituciones Educativas del departamento de Boyacá se apoyan en el uso de las TIC para realizar aquellas actividades que a diario se gestionan en su entorno laboral con el fin de cumplir a cabalidad todas sus funciones como ente educativo.

Las entidades educativas tienen como propósito implementar sistemas de seguridad para proteger recursos y activos informáticos por medio de mecanismos de seguridad en sus sistemas de información en la búsqueda de evitar errores y mal funcionamiento en los procesos, retraso de las actividades, y pérdidas de dinero, credibilidad del buen nombre de la Institución Educativa y obtener mayor rendimiento en la ejecución de sus procesos.

La Institución Técnica de Panqueba en sus procesos informáticos se encuentra en vulnerabilidad de perder información ya que nunca se han tenido en cuenta procesos al momento de proteger la información; estas vulnerabilidades deben ser analizadas y revisadas por medio de un diagnostico como se plantea en uno de los objetivos para que por medio de las distintas metodologías de Ingeniería Social se defina qué medidas de control se debe tomar para minimizar los riesgos inminentes que representen estas fallas.

Con esto se establece dejar como evidencia final a los usuarios un manual de políticas de seguridad y recomendaciones implementando estrategias de prevención de delitos informáticos e Ingeniería social y así fomentar cultura social y educativa.

- **FORMULACIÓN DEL PROBLEMA**

¿Con qué técnicas de Ingeniería Social se puede verificar el nivel de seguridad de la información en la Institución Educativa Técnica de Panqueba?

OBJETIVO GENERAL.

Realizar una implementación en el área de Seguridad Informática aplicando metodologías de Ingeniería Social en la Institución Educativa Técnica de Panqueba (Boyacá).

OBJETIVOS ESPECÍFICOS.

1. Levantar la información de las metodologías de Ingeniería Social que garanticen seguridad y privacidad de la información en la Institución.

2. Determinar las metodologías de Ingeniería social para aplicarlas al personal que usa equipos de cómputo en la Institución Educativa.

3. Aplicar técnicas y metodologías de Ingeniería Social a los servidores públicos de la Institución Educativa Técnica de Panqueba.

4. Generar un manual de seguridad con las recomendaciones para evitar ser víctima de Ingeniería Social implementando estrategias de prevención de delitos informáticos y así fomentar cultura social y educativa.

RESUMEN DE LO DESARROLLADO EN EL PROYECTO.

- **Identificación de Activos del Colegio.**

Con autorización de la Institución se procedió a elaborar un inventario de los activos de con que cuenta el plantel educativo y así identificar el tipo de amenazas a lo que están expuestos.

- **Vulnerabilidades y amenazas.**

Una vez determinados los activos de información con los que cuenta la entidad se procede a identificar las amenazas a las cuales se exponen utilizando la metodología MAGERIT

- **Recopilar información de las metodologías de Ingeniería Social**

Para aplicar en la Institución se realiza una investigación de las distintas estrategias y como se pueden aplicar en el proyecto para lograr identificar hasta donde es vulnerable la entidad.

- **Determinar metodologías de Ingeniería social**

Acá se procede a aplicarlas al personal que usa equipos de cómputo en la Institución Educativa, se definió que las pruebas de Ingeniería Social son necesarias para ver en qué punto crítico está fallando los usuarios de la Institución.

- **Aplicar técnicas y metodologías de Ingeniería Social**

Se define que tras utilizar un instrumento de recolección de datos como lo es la encuesta y por medio de entrevistas, también por una serie de preguntas al aire y por simple observación dentro de las instalaciones se pueden ver puntos claves para obtener datos que determinan las falencias encontradas por medio de técnicas de Ingeniería Social de la siguiente forma:

4. Técnica Pasiva: “Observación”

5. Técnica No Presencial: Por medio de llamadas y por chat se medirá la inocencia de las personas y así medir el nivel de confiabilidad que se tiene en el Colegio.

6. En este objetivo también se plantea aplicar una prueba en ambientes controlados sin infringir la ley para demostrar que el atacante en este caso quien desarrolla el proyecto puede superar a la seguridad física y acceder a la información.

*Se usó Spoofing para engañar por medio de correos electrónico ficticio.

En esta parte que es práctica se va usar la herramienta Kali Linux que cuenta con el paquete Social Engineering Toolkit (SET), con este software se pueden ejecutar automáticamente una serie de ataques que comprometen el recurso humano de cualquier entidad partiendo desde el envío de mensajes de texto con números falsos, la implementación de servidores “phishing” y suplantación de sitios web entre otros.

*Se aplicó la técnica de pretexting por medio de una conversación por chat donde se evidencia la forma como la secretaria por medio de un dato del SIMAT de matrículas accedió a que ingresaran a su oficina y se obtuvo datos valiosos.

- **Generar un manual de seguridad**

Se diseñó con el fin de dar recomendaciones para evitar ser víctima de Ingeniería Social implementando estrategias de prevención de delitos informáticos y así fomentar cultura social y educativa, este manual se entregó impreso en la Institución, al igual quedo plasmado en la página web institucional

- **Capacitaciones al personal**

También como estrategia de apoyo se tuvo en cuenta las capacitaciones que se hicieron el último jueves de cada mes para que todo el personal sea consiente de cómo debe actuar ante las diversas estrategias que pueden poner en riesgo la confiabilidad de la información y así lograr prevenir que alguien sea víctima de la Ingeniería Social.

METODOLOGÍA DE DESARROLLO

Como parte inicial del proyecto y teniendo en cuenta que es lo primordial para saber con qué cuenta la entidad y que riesgos pueden haber ya se realizó dos tareas como lo es:

- Identificación de Activos y amenazas en el Colegio.

Luego de tener esta información recopilada se procede a cumplir con los objetivos específicos que se plantearon:

- Según el primer objetivo que es levantar la información de las metodologías de Ingeniería Social para aplicar en la Institución se realiza una investigación de las distintas estrategias y como se pueden aplicar en el proyecto para lograr identificar hasta donde es vulnerable la entidad.

- Para el segundo objetivo Determinar las metodologías de Ingeniería social para aplicarlas al personal que usa equipos de cómputo en la Institución Educativa, se definió que las pruebas de Ingeniería Social son necesarias para ver en qué punto crítico está fallando los usuarios de la Institución.

- Para el tercer objetivo sobre Aplicar técnicas y metodologías de Ingeniería Social a los servidores públicos de la Institución Educativa Técnica de Panqueba.

Se define que tras utilizar un instrumento de recolección de datos como lo es la encuesta y por medio de entrevistas, también por una serie de preguntas al aire y por simple observación dentro de las instalaciones se pueden ver puntos claves

para obtener datos que determinan las falencias encontradas por medio de técnicas de Ingeniería Social de la siguiente forma:

7. Técnica Pasiva: “Observación”

8. Técnica No Presencial: Por medio de llamadas y por chat se medirá la inocencia de las personas y así medir el nivel de confiabilidad que se tiene en el Colegio.

9. En este objetivo también se plantea aplicar una prueba en ambientes controlados sin infringir la ley para demostrar que el atacante en este caso quien desarrolla el proyecto puede superar a la seguridad física y acceder a la información.

*Se usó Spoofing para engañar por medio de correos electrónico ficticio.

En esta parte que es práctica se va usar la herramienta Kali Linux que cuenta con el paquete Social Engineering Toolkit (SET), con este software se pueden ejecutar automáticamente una serie de ataques que comprometen el recurso humano de cualquier entidad partiendo desde el envío de mensajes de texto con números falsos, la implementación de servidores “phishing” y suplantación de sitios web entre otros.

*Se aplicó la técnica de pretexting por medio de una conversación por chat donde se evidencia la forma como la secretaria por medio de un dato del SIMAT de matrículas accedió a que ingresaran a su oficina y se obtuvo datos valiosos.

- Con el último objetivo se dejó de forma física ya que es Generar un manual de seguridad con las recomendaciones para evitar ser víctima de Ingeniería Social implementando estrategias de prevención de delitos informáticos y así fomentar cultura social y educativa.

Este objetivo se entregó impreso en la Institución, al igual queda plasmado en la página web institucional, también como estrategia de apoyo se tienen en cuenta las capacitaciones que se hicieron el último jueves de cada mes para que todo el personal sea consiente de cómo debe actuar ante las diversas estrategias que pueden poner en riesgo la confiabilidad de la información y así lograr prevenir que alguien sea víctima de la Ingeniería Social.

Conclusiones

1. Aplicando el primer objetivo por medio de la investigación sobre estrategias de ingeniería social se logró identificar el nivel de vulnerabilidad en donde se concluye que cualquier integrante del plantel educativo es muy fácil capturar la información que desempeña en su rol debido a que son muy escasos los conocimientos de la mayoría en el manejo del ámbito informático y queda evidenciado en la observación, el desarrollo de la encuesta y la práctica que se llevó a cabo.

2. Resulto muy positivo según el segundo objetivo en donde se aplicó metodologías de Ingeniería social para aplicar al personal que usa equipos de cómputo en la Institución Educativa ya que se vio cuáles son las mayores falencias que se deben corregir.

3. Por medio de la encuesta, entrevistas y una serie de preguntas se obtuvo información clave para obtener datos y así por medio de la implementación de técnicas de Ingeniería Social se logró cumplir con el tercer objetivo.

4. Se hizo el compromiso con los docentes de que a medida que lleguen alumnos nuevos reunirlos de forma periódica y darles a conocer el manual que se dejó para la Institución sobre Recomendaciones de Seguridad Informática.

5. Se plantea junto a los dos docentes del área de Informática dar continuidad a las capacitaciones que se llevaron a cabo en la parte de actualizaciones tecnológicas y manejo de seguridad informática con el fin de consolidar algunos aspectos de sistemas en el plantel educativo.

6. Se determinó más control en la entrada de la Institución puesto que el día que se ejecutó la prueba de *pretexting* no hubo ninguna sospecha de la persona que acompaño a la oficina de la secretaria, y además se observa la facilidad de ingresar cualquier elemento informático para cambiarlo por otro.

7. Se manifestó a los administrativos de la Institución Educativa que se debe validar la información que se solicita vía telefónica o por chat ya que estas personas usan estos indicios con la intención de ir consiguiendo detalles para acceder a la información.

8. El personal de la Institución se compromete a destruir los documentos con información sensible antes de desecharlos, esto con el fin de no dejar ni el más mínimo detalle que sirva de evidencia para los curiosos.

9. Por parte del Rector se dio la orden de que las claves de WI-FI queden protegidas en los equipos para así no facilitarla a cualquier persona que accede a servicios como biblioteca y ludoteca.

10. Se estableció la instalación del programa *Deep Freeze* en las salas de sistemas para que las dos particiones queden congeladas y así evitar problemas de seguridad muy comunes cuando estos equipos se dejan libres.

11. Se aconsejó reubicar tres cámaras de seguridad hacia las entradas de las salas de sistemas debido a que en el transcurso del año se han perdido ciertos dispositivos sin encontrar el responsable del hecho.

Recomendaciones.

Las principales recomendaciones realizadas son:

- ✓ La Institución Educativa para el 2018 debe dar continuidad a las capacitaciones que se llevaron a cabo el segundo semestre del presente año y así establecer un cronograma de capacitación de forma periódica para todo el plantel basado en las últimas novedades de la seguridad informática con el objetivo principal de consolidar una cultura de protección de la información dentro la institución.

- ✓ Se aconsejó al Rector del Colegio en la ampliación del número de cámaras de seguridad con los que cuenta, esto debido a que la institución últimamente está siendo dotada por parte de computadores para educar y Vive digital de activos de gran valor que se deben cuidar en las áreas asignadas.

- ✓ Se debe generar un control que evite que los estudiantes puedan compartir recursos en la red, la forma aconsejable es negando los privilegios a las cuentas de usuario en cada equipo o desde el controlador de dominio.

- ✓ Una idea que se propuso al docente del área de Sistemas y a los aprendices SENA que terminan el año entrante la Formación es que apliquen como proyecto de grado la implementación de la identificación biométrica o electrónica a través de los códigos de barras de los carnet institucionales.

- ✓ Se debe concientizar que la papelería que se arroja a la basura y que pueden contener datos valiosos se debe destruir por completo.

- ✓ En el entorno de infraestructura la Institución debe reubicar en algunas oficinas los puestos de trabajo y demás dispositivos ya que es una falencia que cualquier persona que visita la Institución lo va notar en algunos sitios.

- ✓ Se recomienda periódicamente cambiar la contraseña de acceso a las redes inalámbricas que dispone la Institución con el fin de evitar que se saturen y se vuelvan lentas lo cual ha sido la constante en los meses que se desarrolló el proyecto.

- ✓ En cuanto a los puntos de red del cableado estructurado con que cuenta el plantel educativo y que se encuentran al alcance de cualquier persona se aconseja mantenerlos desconectados y así evitar daños en la estructura del cableado UTP.

- ✓ Se acordó con las directivas del Colegio bloquear o restringir el acceso a algunas páginas de internet, ya que esta idea genera beneficios en el desempeño educativo de los estudiantes e incentiva el uso de páginas de investigación acordes a la planeación de la formación de cada área.

- ✓ Las directivas de la Institución se comprometieron a tramitar software original en algunos equipos que no cuentan con este aspecto para así evitar cometer delito en cuanto a promover el uso de software pirata.

- ✓ Se estableció que la Secretaria de la Institución va cumplir la directriz de realizar copias de seguridad de forma periódica sobre las bases de datos y plataformas institucionales que maneja el Colegio.