UNIVERSIDAD POLITÉCNICA SALESIANA

SEDE QUITO

CARRERA:

INGENIERÍA DE SISTEMAS

Trabajo de titulación previo a la obtención del título de:

Ingenieros de Sistemas

TEMA:

ANÁLISIS Y EVALUACIÓN DE LA SEGURIDAD EN LA RED DE LA UNIDAD EDUCATIVA SALESIANA CARDENAL SPELLMAN, UTILIZANDO HERRAMIENTAS DE INGENIERÍA SOCIAL, Y RECOMENDAR MEDIDAS PREVENTIVAS.

AUTORES:

EDISON STALIN CAMINO RUIZ

EDWIN DAVID PUENTE PACHECO

TUTOR:

JOSÉ LUIS AGUAYO MORALES

Quito, agosto del 2020

CESIÓN DE DERECHOS DE AUTOR

Nosotros, Edison Stalin Camino Ruiz, con documento de identificación Nº 1719101154, y Edwin David Puente Pacheco con documento de identificación Nº 1722576590, manifestamos nuestra voluntad y cedemos a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que somos autores del trabajo de titulación con el tema: "ANÁLISIS Y EVALUACIÓN DE LA SEGURIDAD EN LA RED DE LA UNIDAD EDUCATIVA SALESIANA CARDENAL SPELLMAN, UTILIZANDO HERRAMIENTAS DE INGENIERÍA SOCIAL, Y RECOMENDAR MEDIDAS PREVENTIVAS.", mismo que ha sido desarrollado para optar por el título de INGENIEROS DE SISTEMAS en la Universidad Politécnica Salesiana, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En aplicación a lo determinado en la Ley de Propiedad Intelectual, en nuestra condición de autores nos reservamos los derechos morales de la obra antes citada. En concordancia, suscribimos este documento en el momento que hacemos la entrega del trabajo final en formato impreso y digital a la Biblioteca de la Universidad Politécnica Salesiana.

Edison Stalin Camino Ruiz

CI: 1719101154

Edwin David Puente Pacheco

CI: 1722576590

Quito, agosto del 2020

DECLARATORIA DE COAUTORÍA DEL TUTOR

Yo declaro que bajo mi dirección y asesoría fue desarrollado el proyecto técnico, con el tema: "ANÁLISIS Y EVALUACIÓN DE LA SEGURIDAD EN LA RED DE LA UNIDAD EDUCATIVA SALESIANA CARDENAL SPELLMAN, UTILIZANDO HERRAMIENTAS DE INGENIERÍA SOCIAL, Y RECOMENDAR MEDIDAS PREVENTIVAS.", realizado por Edison Stalin Camino Ruiz y Edwin David Puente Pacheco, obteniendo un producto que cumple con todos los requisitos estipulados por la Universidad Politécnica Salesiana, para ser considerado como trabajo final de titulación.

Quito, agosto del 2020

JOSÉ LUIS AGUAYO MORALES

CI: 1709562597

UNIDAD EDUCATIVA SALESIANA

Cardenal Spellman

Formando con el espíritu y estilo de Don Bosco

Quito, 23 de septiembre de 2019

Señores
DIRECCIÓN DE CARRERA DE INGENIERÍA DE SISTEMAS
UNIVERSIDAD POLITÉCNICA SALESIANA
Presente.

La Unidad Educativa Salesiana "Cardenal Spellman", presenta sus más atentos saludos a la Universidad Politécnica Salesiana y tiene el honor de comunicar lo detallado a continuación:

Mediante el presente deseamos manifestar nuestro apoyo al tema del Proyecto de titulación "Análisis y evaluación de la seguridad en la red de la Unidad Educativa Salesiana Cardenal Spellman, utilizando herramientas de Ingeniería Social, y recomendar medidas preventivas.", a desarrollarse por los señores Edison Stalin Camino Ruiz con C.I. 1719101154 y Edwin David Puente Pacheco con C.I. 1722576590 para que pueda ser realizado en nuestra institución, el mismo que ratificamos la facilidad de información necesaria por parte de la institución para la correcta ejecución del proyecto de titulación.

Atentamente,

UNIDAD EDUCATIVA SALESIANA CARDENAL SPELLMAN
RECTORADO

P. Naún Tapia,sdb.
DIRECTOR

DEDICATORIA

Este proyecto de titulación está dedicado, a mi héroe, mi padre Walter que siempre estuvo a mi lado, por su constante preocupación, consejos y enseñanzas tanto en mí vida académica, profesional y personal, por siempre escucharme y nunca dejarme caer.

A mí ángel de la guarda, mi madre Graciela, por su apoyo incondicional, que nunca perdió la fe en mí, con su bendición y consejos me he levantado y salido adelante, he aquí mi promesa.

A mi querida hermana Mishel, quien me demostró que todo en esta vida es posible con esfuerzo y trabajo constante, siempre orgulloso de ser tu hermano.

A mi amiga, mi compañera, mi amorcito corazón, Valeria, llegaste en un momento importante de mi vida, nunca dejaste que me rinda, me ayudaste a llegar al final, no sé qué nos depare el futuro, pero a tu lado todo estará bien.

A mi abuelita Isabel, con sus enseñanzas y bendiciones supo guiarme, a mis tíos, tías, primos y primas que han estado en las buenas y sobre todo en las malas, para las futuras generaciones, nunca caminamos solos, en la familia está la fortaleza y sabiduría, que esto les sirva de inspiración.

Edison Stalin Camino Ruiz

El presente trabajo de titulación va dedicado, para mi papa en el cielo por enseñarme a ser una gran persona y sé que está muy contento por la meta cumplida.

A mi mami Lucí por ser, cálida, exigente y consentidora en todos estos años, a mis hermanas por apoyarme incondicionalmente, Michelle y María José, esto es con amor para ustedes.

Para mi amor eterno Karen, sin ti no lo hubiera hecho, es un esfuerzo de dos, sin tu fuerza y tu amor, el camino hubiese sido más difícil.

Y al amor de mi vida mi hija Julieta es para ti amor, tu eres mi motor y fuerza para conseguir mi título, y seguir luchando por ti.

Para toda mi familia y amigos que estuvieron conmigo de una u otra manera, cuando más lo necesitaba.

Y una mención especial para mi mami Carla, por ser mi pilar que, gracias a su esfuerzo de muchos años, logre mi objetivo, muy orgulloso de ser tu hijo no puedo decir más que “mami lo logramos esto es para ti “con todo mi amor.

Edwin David Puente Pacheco

AGRADECIMIENTO

Agradezco a mi tutor José Luis Aguayo Morales, por su guía, esfuerzo, dedicación, y sobre todo por el conocimiento depositado en mí para la culminación de este proyecto de titulación.

A la Universidad Politécnica Salesiana, a la cual considero mi segundo hogar, por abrirme las puertas y formarme como una persona de bien, capaz de afrontar cualquier reto profesional, por todo lo aprendido y vivido estaré eternamente agradecido

Del mismo modo a mi gran amigo y compañero de tesis, que con su ayuda y apoyo hemos podido realizar con gran satisfacción el presente proyecto, a la Vieja Guardia, que nunca me han dejado caminar solo.

Finalmente agradezco a la Unidad Educativa Salesiana Cardenal Spellman, por permitirnos realizar este proyecto de titulación, brindándonos toda facilidad y apoyo para culminarlo, siempre agradecido con toda la comunidad salesiana.

Edison Stalin Camino Ruiz

Agradezco a Dios por bendecirme y darme la sabiduría, y fortaleza en aquellos momentos difíciles, y poder finalizar la carrera.

Gracias a mi papa en el cielo, que también es parte de este sueño, sé que está orgulloso de mi.

Gracias a mis madres Lucía y Carla, por ser las principales promotoras de mis sueños, gracias por permitirme cumplir este sueño, por confiar en mí, por brindarme sus consejos y sabiduría.

A mi esposa Karen y a mi hija Julieta, gracias por estar conmigo, por apoyarme en este proyecto de estudio, sin ustedes esto no tendría sentido.

A mis hermanas, y a mi familia en general, que gracias a su apoyo y con sus palabras me hacían sentir orgulloso de lo que soy.

De igual manera agradezco a la Universidad Politécnica Salesiana, a la carrera de Sistemas a mis profesores durante mi periodo de estudios y a mi tutor José Luis Aguayo, quienes con la enseñanza de sus valiosos conocimientos hicieron que pueda crecer día a día como profesional, gracias a cada una de ustedes por su paciencia, dedicación, apoyo incondicional y amistad.

Edwin David Puente Pacheco

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE ANEXOS

RESUMEN

El objetivo de este proyecto es analizar la seguridad de la información de la red de la Unidad Educativa Salesiana Cardenal Spellman, utilizando técnicas y herramientas de Ingeniería Social, que permiten evadir la protección en hardware y software, ya que estos ataques van directamente al usuario.

Se diseñaron dos escenarios de prueba implementados en diferentes áreas de la institución. Se utilizaron dos metodologías Proyecto Piloto y Cadena de Ataques Informáticos.

En el primer escenario, el personal administrativo fue atacado con Social-Engineer Toolkit (SET) que se utilizó para clonar la página de acceso a las cuentas de Google y el sistema académico Esemtia, en el cual se obtuvo un 40% de éxito, como resultado de esto, las credenciales capturadas se utilizaron en un ataque de robo de identidad.

En el segundo escenario, las técnicas de Phishing y Pretexting se utilizaron para enviar un mensaje falso, ofreciendo capacitación gratuita a los maestros, por correo electrónico se obtuvo un 29.6% de éxito, un 8% de éxito a través de WhatsApp, se obtuvo información personal y laboral, luego se encontraron datos familiares, residenciales con la ayuda de redes sociales y servicios de Google.

Como resultado final se proporcionarán recomendaciones para prevenir ataques de ingeniería social y resolver las vulnerabilidades encontradas, para crear conciencia en la comunidad educativa sobre los riesgos que implica no tener el conocimiento correcto de la gestión de la información y no tener una política de seguridad propia en la UESCS.

ABSTRACT

The goal of this project is to analyze the information security of the network of the Unidad Educativa Salesiana Cardenal Spellman, using techniques and tools of Social Engineering, which allow evading protection in hardware and software, since these attacks go straight to the user.

Two test scenarios implemented in different areas of the institution were designed. Two methodologies were used Pilot Project and Cyber Kill Chain.

In the first scenario, the administrative personnel were attacked with Social-Engineer Toolkit (SET) that it was used to clone the access page to Google accounts and the Esemtia academic system, in which a 40% success rate was obtained, as result of this, the credentials captured was used in a theft identity attack.

In the second scenario, the Phishing and Pretexting techniques were used to send a fake message, offering free training to teachers, 29.6% success was obtained by email and 8% through WhatsApp, personal and work information was obtained, then family and residential data was found with the help of Social Networks and Google's services.

As final results provide recommendations to prevent social engineering attacks and resolve the vulnerabilities found, to raise awareness in the educational community of the risks involved in not having the right knowledge of information management and don't have an own security policy's in the UESCS.

INTRODUCCIÓN

Antecedentes

A través de los años, la información se ha convertido en un activo valioso para las empresas tanto públicas como privadas, esta al ser procesada genera el conocimiento para realizar las acciones cotidianas, así que, si se necesita resolver un problema o tomar una decisión, se emplea esta información para crear una fuente de conocimiento para resolver un problema o tomar una decisión.

Según la norma ISO 27001, la información debe ser recopilada, manejada, almacenada y transmitida, garantizando la confidencialidad, integridad y disponibilidad de la misma, independientemente de su formato (audio, video, texto, etc.). (ISO, 2005)

Mitnick describe que la seguridad en muchos de los casos es nada más que una utopía, y mucho peor cuando la ingenuidad, inocencia y la incredulidad forman parte del juego. (Mitnick, 2001)

Problema de estudio

En palabras de Mitnick, quien reconoce que el usuario es el eslabón más débil respecto a la seguridad de la red, la Unidad Educativa Salesiana Cardenal Spellman (UESCS) que trabaja con información importante y sensible para toda la comunidad educativa, ha tomado las medidas necesarias, para asegurar la información de daños, pérdida, alteración, sustracción, y demás amenazas. (Mitnick, 2001)

Las amenazas hacia las redes informáticas han evolucionado de tal manera que, para hacerles contra, se han llegado a crear sistemas, programas, antivirus, antimalware, etc., que ayuden a mantener la seguridad.

Pablo Huerta, señala que, no importa que se implemente todo tipo de seguridad en la red, si no se capacita a los usuarios en las diferentes amenazas que existen en la actualidad, sobre todo cuando se habla acerca de la ingeniería social. (Huerta, 2010)

Según David Harley, la ingeniería social se ha mantenido igual a través de los años, lo que ha cambiado son los vectores de contagio, de manera que, si antes se realizaba una llamada telefónica para conseguir información, en la actualidad basta con enviar un correo electrónico con un enlace a una página web maliciosa. (Harley, 2015)

Justificación

Las diferentes prácticas de ingeniería social, se han transformado a la par del crecimiento y evolución de la tecnología, esto ha hecho que la seguridad en las redes informáticas se vuelva vulnerable ante este tipo de ataques. La ingeniería social es un método no necesariamente técnico, utilizado para realizar engaños obtener información, fraudes, o garantizar acceso ilegal a las computadoras de los usuarios de la red.

Por lo que se propone la utilización de esta práctica dentro la UESCS, con el fin de conocer y detectar posibles brechas de seguridad que faciliten el robo de información sensible.

Los beneficios de realizar este tipo de procedimientos, además de conocer las vulnerabilidades de la red, en la parte técnica y humana, permite después de analizar los datos, recomendar planes de contingencia, planes de tratamiento de riesgos, planes de continuidad de negocio y demás, pero sobre todo la de concientizar a la comunidad educativa de los riesgos que conlleva el no tener el conocimiento del correcto manejo de la información en la internet, redes sociales y demás.

Objetivos

Objetivo general

Analizar y evaluar la seguridad en la red de la Unidad Educativa Salesiana Cardenal Spellman, utilizando herramientas de Ingeniería Social, y recomendar medidas preventivas.

Objetivos específicos

Conocer el estado actual de la seguridad de la red de la Unidad Educativa Salesiana Cardenal Spellman.

Investigar las herramientas de Ingeniería social para el desarrollo de los escenarios de investigación.

Diseñar escenarios de investigación utilizando herramientas de Ingeniería Social, para atacar a la red y sus usuarios.

Evaluar los resultados de los ataques de Ingeniería Social y analizar las vulnerabilidades encontradas en la red de la Unidad Educativa Cardenal Spellman.

Recomendar medidas preventivas, técnicas, económicas o legales, para concientizar a la comunidad educativa sobre el correcto manejo de la información en la red.

Metodología

En primera instancia se utilizará la metodología de Proyecto Piloto, que se caracteriza por ser un esfuerzo temporal para comprobar la factibilidad de un resultado exclusivo del trabajo propuesto.

Además, para el diseño de los escenarios de prueba se pondrá en práctica la Cadena de ataques informáticos, que es un modelo de defensa y seguridad que se basa

en investigación, recopilación de información e inteligencia para la identificación y prevención de ataques informáticos, además establece los pasos que deben seguir los atacantes, con el fin de lograr su meta

Alcance

Para el desarrollo del trabajo y la recopilación de información, se propone un ataque de ingeniería social, el cual será realizado a partir de la creación de escenarios de investigación utilizando software dedicado, varios medios de transmisión (correo electrónico, mensajería instantánea, páginas web, etc.), y la utilización de técnicas de ataques de ingeniería social.

Después de desarrollar los escenarios de investigación, se procederá a realizar los ataques a un grupo designado en la comunidad educativa de la UESCS, para evaluar los datos recolectados y analizar las vulnerabilidades encontradas en la red, para recomendar medidas preventivas, el proyecto no implementará ningún hardware ni software a la red de la UESCS.

Estructura capitular del documento

El presente documento se estructura de la siguiente manera:

- Capítulo 1, se analiza el estado inicial de la seguridad de la red de la UESCS.
- Capítulo 2, se presenta la teoría que sustenta el trabajo de titulación.
- Capítulo 3, presenta los escenarios diseñados para los ataques y los resultados de los mismos.
- Capítulo 4, presenta las medidas preventivas recomendadas.
- Finalmente se exponen las conclusiones y recomendaciones.

CAPÍTULO 1

1.1. Estado actual de la seguridad de la red de la UESCS

Según la metodología de proyecto piloto, se describe a continuación el levantamiento de información de la red interna de la UESCS.

1.1.1. Ubicación

La Unidad Educativa Salesiana Cardenal Spellman (UESCS), está ubicada en la ciudad de Quito, en la parroquia Cumbayá, Vía a Lumbisí km 3, sector San Patricio.

Ubicación.

Figura 1. Ubicación de la Unidad Educativa Salesiana Cardenal Spellman.
Fuente: *(Spellman, Contactos, 2016)*, obtenido de https://www.spellman.edu.ec/index.php/contact-sidebar

1.1.2 Misión

La figura 2, muestra la misión de la UESCS.

Misión.

Figura 2. Misión de la Unidad Educativa Salesiana Cardenal Spellman.
Fuente: *(Spellman, Misión y Visión, 2016)*, obtenido de https://www.spellman.edu.ec/index.php/joomla-pages-2/2016-11-28-17-09-06/mision-y-vision

1.1.3. Visión

La figura 3, muestra la visión de la UESCS.

Visión.

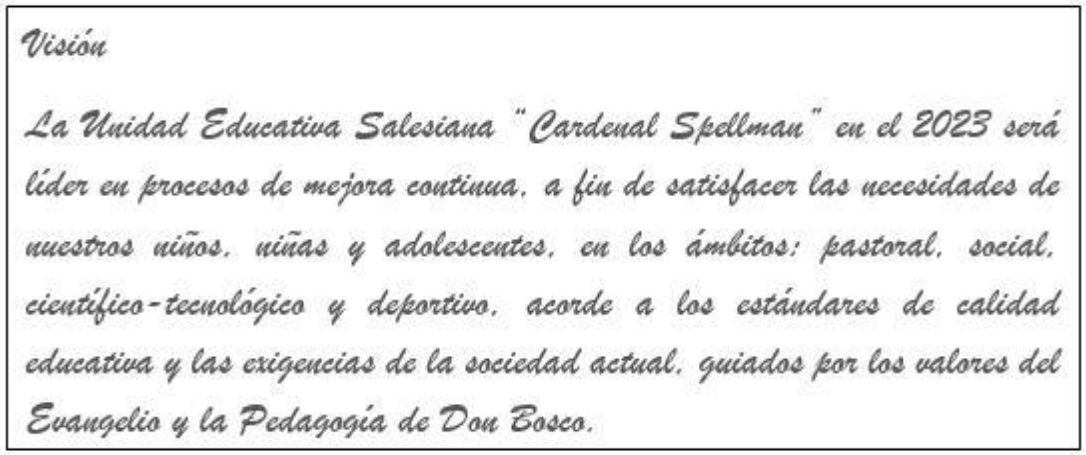


Figura 3. Visión de la Unidad Educativa Salesiana Cardenal Spellman.
Fuente: *(Spellman, Misión y Visión, 2016)*, obtenido de https://www.spellman.edu.ec/index.php/joomla-pages-2/2016-11-28-17-09-06/mision-y-vision

1.1.4. Estructura jerárquica

Dentro de la página web de la institución se encuentra la estructura jerárquica de la UESCS, que se muestra en la figura 4.

Estructura jerárquica.

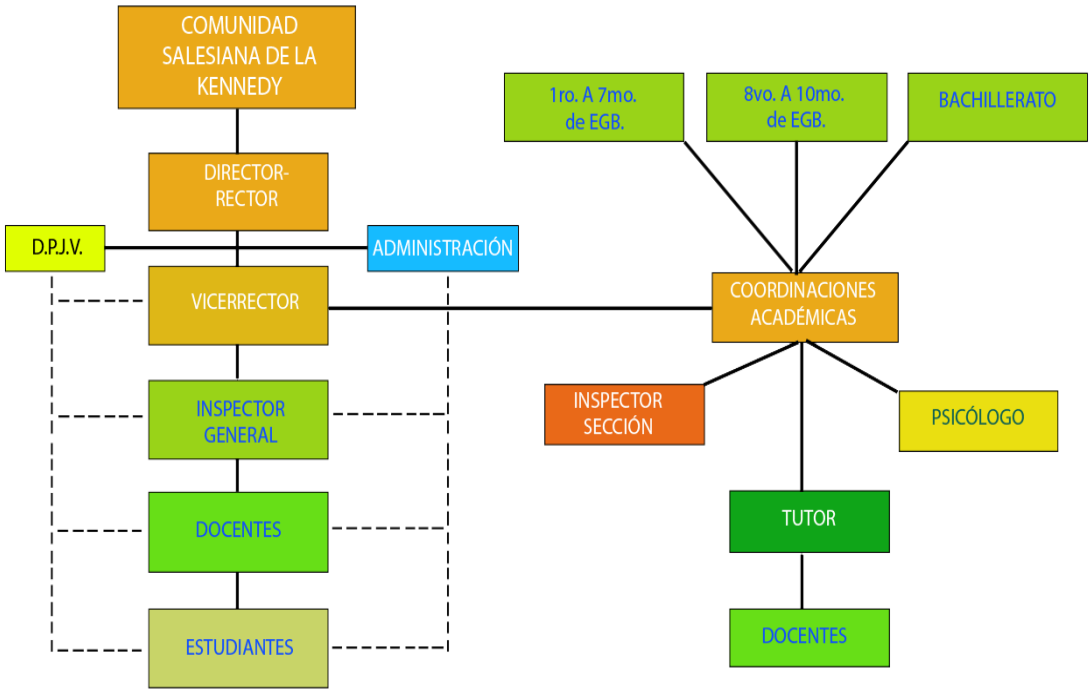


Figura 4. Estructura jerárquica de la Unidad Educativa Salesiana Cardenal Spellman. Fuente: *(Spellman, Estructura jerárquica, 2016)*, obtenido de https://www.spellman.edu.ec/index.php/joomla-pages-2/organigrama

1.1.5 Estructura de la red de la UESCS

La UESCS, tiene una infraestructura sólida, y brinda varios servicios, para que el trabajo de sus usuarios sea lo más eficiente posible, en donde los usuarios intercambian, procesan y conservan información, todo esto se lo realiza en redes de datos, equipos informáticos y de almacenamiento, pero no se asegura el riesgo de que estos sistemas informáticos estén sometidos a riesgos potenciales de seguridad, ya sea dentro de la propia organización como fuera de ella.

1.1.5.1. Equipos

En la institución se encuentran 3 marcas de switch que permiten la comunicación entre edificios, por cuestión de seguridad la tabla 13 que se encuentra en los anexos muestra la información completa acerca de los equipos instalados en la institución.

- 3COM con un periodo de vida superior a 8 años.
- HP con un periodo de vida de más de 5 años.
- Mikrotik con un periodo de vida de más de 3 años.

También cuentan con un switch capa 3 HP la que realiza tareas de enrutamiento y un switch capa 2 Mikrotik para el acceso de dispositivos a la red.

En el departamento de sistemas se encuentra el NOC principal (Network Operations Centers), este es el núcleo de la red LAN y en donde se encuentra la red hacia internet, con un Firewall Fortinet como frontera, el cual recibe un enlace dedicado de 200 Mb de la red CEDIA, a continuación, se detallan los equipos dentro de la institución.

Tabla 1.
Equipos instalados en la red de la UESCS.

Equipos	Cantidad
Switch capa 2/3/4 48 puertos 10/100/1000 4 puertos SFP GE Capacidad de Conmutación 192 Gbps. Arquitectura Non-Blocking	1
Switch capa 2/3/4 24 puertos GE SFP 8 puertos 10/100/1000	1
Switch capa 2 24 puertos 10/100/1000 2 puertos SFP Capacidad de Conmutación 136 Gbps.	3
Switch capa 2/3 48 puertos 10/100/1000 2 puertos SFP Capacidad de Conmutación 176 Gbps.	1
Switch L2 24 puertos 10/100 4 puertos SFP GE.	3
Switch L2 48 puertos 10/100 2 puertos SFP GE.	4
Switch L2 24 puertos 10/100 2 puertos SFP GE.	1
Switch L2, L3 24 puertos 10/100 2 puertos SFP GE.	1
Firewall Proxy, DNS, VPN 2 DMZ 2 enlaces WAN	1
Servidor en Rack Velocidad DIMM Hasta 2666 MT/s, Tipo de memoria UDIMM 4 ranuras UDIMM RAM máxima UDIMM 64 GB.	1
Wireless Access Point UAP 2.4 Ghz.	15
Equipos escritorio	198
Equipos portátiles	98
Total	328

Nota: La tabla muestra los equipos que se encuentran en la UESCS, la tabla 13 en la sección de anexos muestra la información completa.
Elaborado por: Los autores, a partir de la entrevista al departamento de sistemas de la UESCS.

1.1.5.2. Topología de la red

La UESCS maneja una topología tipo estrella, con un equipo frontera Fortinet como principal y un switch capa 3 HP, estos son los encargados de la comunicación entre edificios, dentro de los cuales se localizan los enlaces de fibra óptica.

La red de la UESCS es plana, posee un bloque extenso de direcciones, además no cuenta con una segmentación a través de VLANS para una óptima administración.

Los equipos de interconectividad de la institución son administrados remotamente, cuenta con una dirección IP identificada y su acceso es mediante telnet y acceso web, cuentan con su usuario y contraseña correspondiente.

Topología lógica.

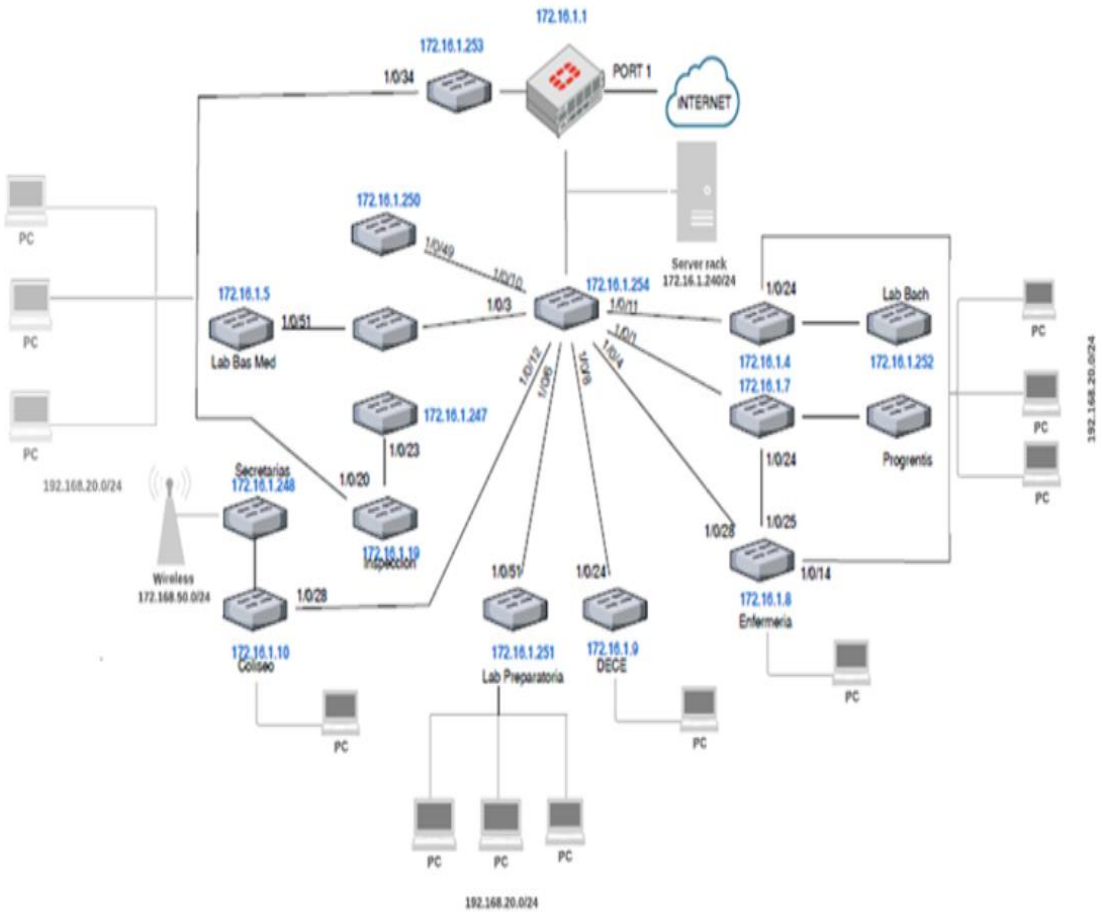


Figura 5. Topología lógica de la red de la Unidad Educativa Salesiana Cardenal Spellman.
Elaborador por: Los autores, a través de la plataforma del firewall de la UESCS.

Tabla 2.
Direccionamiento IPv4.

Área	Dirección IPv4
Administrativos	172.16.1.0/24
Laboratorios	192.168.20.0/24
Docentes	192.168.1.0/24
Equipos Wireless Unifi	192.168.50.0/24

Nota: La tabla muestra las direcciones IPv4 de la red de la UESCS.
Elaborado por: Los autores, a partir de la entrevista al departamento de sistemas de la UESCS.

La UESCS cuenta con una red inalámbrica con equipos Unifi, estos se encuentran distribuidos en los edificios de la institución en puntos específicos como: oficinas, salas de profesores y auditorios, cuentan con su propia red y son manejados desde la consola propia del equipo.

Topología física.

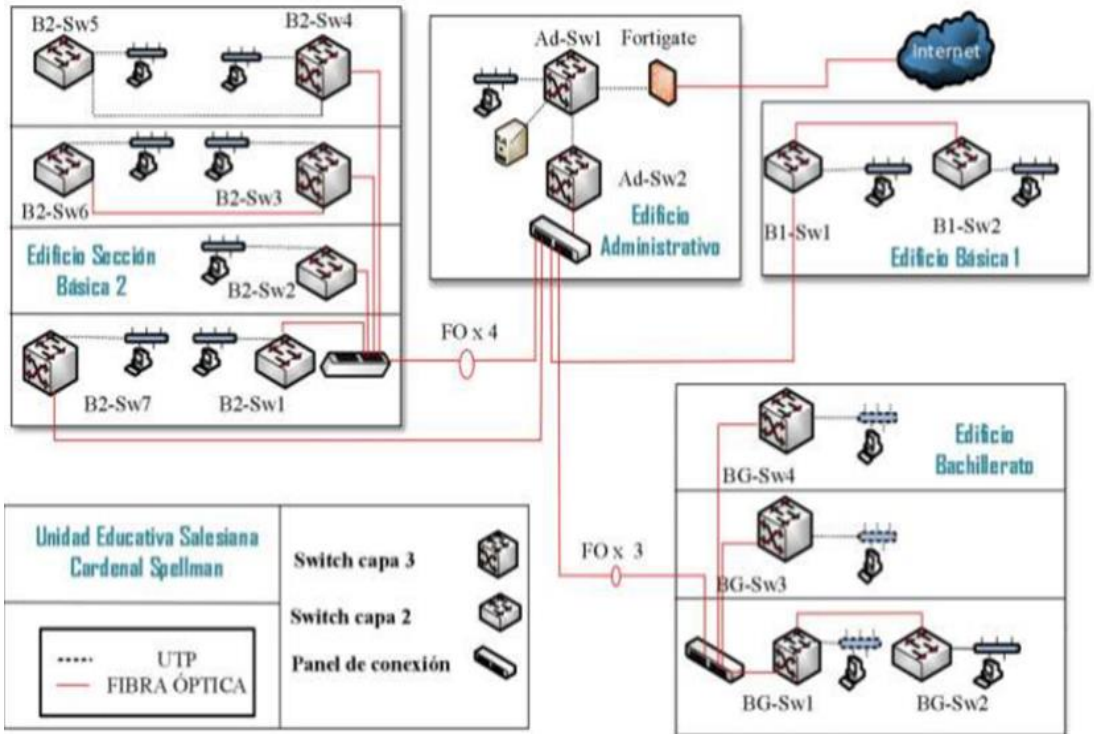


Figura 6. Topología física de la red de la Unidad Educativa Salesiana Cardenal Spellman.
Elaborador por: Los autores, a través de la plataforma del firewall de la UESCS.

Los equipos que se encuentran en la red de la unidad educativa, buscan solventar los requerimientos de conectividad, para asegurar los servicios que ofrece la institución, y la conectividad entre aulas, laboratorios, oficinas dentro del campus.

Los enlaces de fibra óptica multimodo está en el backbone de cada edificio, y en el NOC, que es el lugar de donde se origina todo el cableado para la institución, están interconectados por cable par trenzado y enlaces de fibra óptica.

- UTP (Unshield Twisted Pair) categoría 5e y 6e.
- Fibra óptica 0M2 multimodo.

Se encuentra un enlace adicional de fibra óptica OM2, para los laboratorios de computación, cada laboratorio posee su propio switch, sus características: fibra multimodo MM 50/125, instancia máxima: 550 m., ventana operativa: 850 nm., atenuación: 3,5 dB/km, ancho de banda: 500 MHz.

1.1.5.3. Servicios

El departamento de sistemas manifiesta que la red de la UESCS presta servicios internos con varias aplicaciones para todo el personal de la institución, los cuales se encuentran detallados en la tabla 3.

Tabla 3.
Servicios de la UESCS.

Equipo	Servicios	Aplicación	Descripción
Hosting externo	Página Web	Joomla	Página informativa de la institución.
NAS Asustor	Almacenamiento de documentos, archivos	ADM Asustor	Repositorio de archivos que permite la transferencia de información.
Servidor externo	Plataforma institucional educativa	Esemtia Moodle	Registro de datos del alumnado junto a sus calificaciones, aula virtual.
Nube	Correo institucional y servicios de ofimática	Office 365	Administra los correos de la institución, y brinda servicios de ofimática.
Servidor DELL	Sistema contable	VMWare SAFI	Permite el procesos de contabilidad, presupuestos, depreciaciones, recursos humanos y autorización de pagos.
Nube	Antivirus	ESET	Consola web que administra antivirus brindando seguridad a los datos corporativos.
Firewall Fortinet	Administración y seguridad	Fortinet APP	Administración de la seguridad de la red.
Servidor DELL	Creación de usuarios, equipos y grupos para administrar	VMWare Active Directory	Manejo de máquinas de los laboratorios, creación de usuarios cuentas zoom.
Servidor DELL	Acceso de Ingresos	VMWare ESUMAN	Se encarga de administrar los accesos de los empleados de la UESCS.

Nota: La tabla muestra los diferentes servicios de internos de la UESCS.
Elaborado por: Los autores, a partir de la entrevista al departamento de sistemas de la UESCS.

La población estudiantil oscila los 1800 alumnos, distribuidos en diferentes secciones, el personal que labora en la institución es de 150 personas, divididas en administrativos, docentes, autoridades y personal de apoyo.

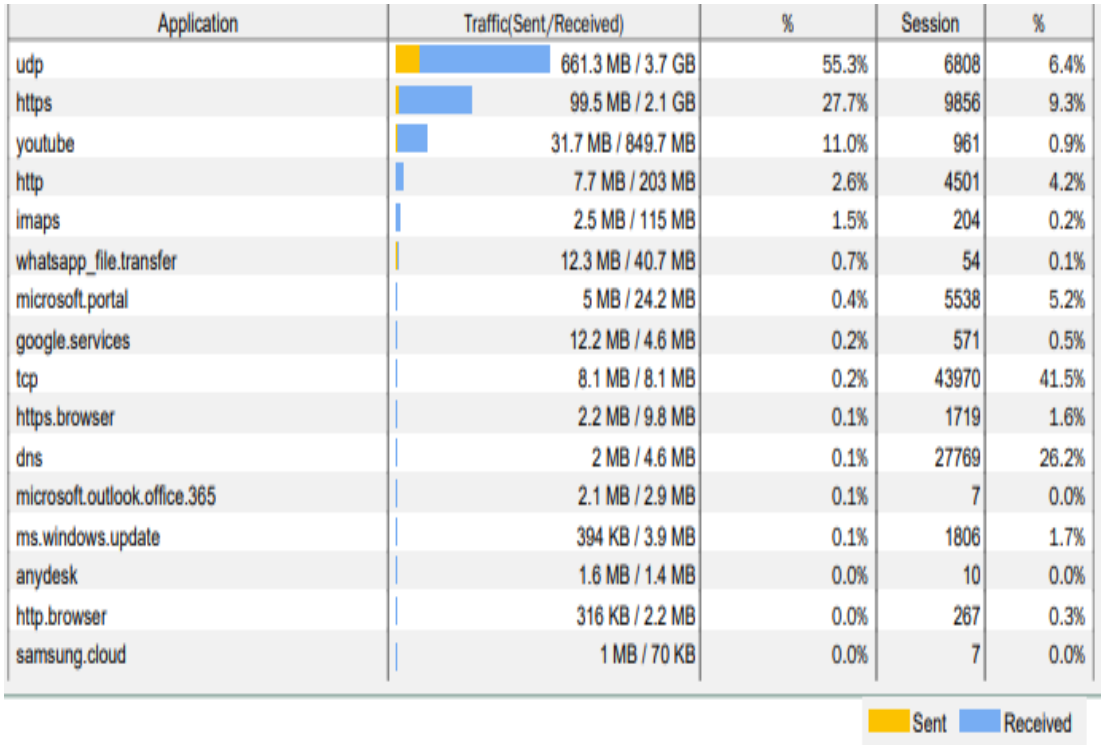
En la UESCS, los usuarios finales utilizan sistemas operativos Windows con sus licencias respectivas, también se maneja el paquete de office con sus licencias respectivas.

Para el manejo de servidores se utiliza Windows Server, instalado en el servidor DELL el cual se encuentra virtualizado con la plataforma VMware, este no cuenta con una licencia oficial.

1.1.5.4 Análisis de protocolos de la UESCS

Para el análisis de protocolos, se utilizó el firewall Fortinet, como resultado se evidenció que, los protocolos que corren en la red de le UESCS son los siguientes: UDP, TCP, HTTPS, HTTP, IMAPS, DNS, STUN, SSL, SSH.

Análisis de protocolos de la UESCS.



Application	Traffic(Sent/Received)	%	Session	%
udp	661.3 MB / 3.7 GB	55.3%	6808	6.4%
https	99.5 MB / 2.1 GB	27.7%	9856	9.3%
youtube	31.7 MB / 849.7 MB	11.0%	961	0.9%
http	7.7 MB / 203 MB	2.6%	4501	4.2%
imaps	2.5 MB / 115 MB	1.5%	204	0.2%
whatsapp_file.transfer	12.3 MB / 40.7 MB	0.7%	54	0.1%
microsoft.portal	5 MB / 24.2 MB	0.4%	5538	5.2%
google.services	12.2 MB / 4.6 MB	0.2%	571	0.5%
tcp	8.1 MB / 8.1 MB	0.2%	43970	41.5%
https.browser	2.2 MB / 9.8 MB	0.1%	1719	1.6%
dns	2 MB / 4.6 MB	0.1%	27769	26.2%
microsoft.outlook.office.365	2.1 MB / 2.9 MB	0.1%	7	0.0%
ms.windows.update	394 KB / 3.9 MB	0.1%	1806	1.7%
anydesk	1.6 MB / 1.4 MB	0.0%	10	0.0%
http.browser	316 KB / 2.2 MB	0.0%	267	0.3%
samsung.cloud	1 MB / 70 KB	0.0%	7	0.0%

Figura 7. Protocolos que corren en la red de la Unidad Educativa Salesiana Cardenal Spellman.
Elaborador por: Los autores, a través de la plataforma del firewall de la UESCS.

1.1.6. Resumen del estado actual de la seguridad de la red de la UESCS

En base a las respuestas obtenidas por la entrevista realizada al personal del departamento de sistemas de la UESCS y después del análisis de la información

brindada, se recopiló la siguiente información expuesta en la tabla 4, además, sobre los usuarios se puede decir lo expuesto en la tabla 5. (La guía de entrevista consta en los anexos.)

Tabla 4.
Estado actual de la seguridad de la red de la UESCS.

Hardware	Switch	Obsolescencia de los equipos. Sin soporte de la marca. Incompatibilidad. Falta de mantenimiento. Desperdicio de ancho de banda. Localización – exposición a daños.
	Cableado	Cableado deteriorado. Falta de mantenimiento Inadecuada seguridad del cableado.
Software	Sistema Operativo	Sin soporte oficial. Exposición de contraseñas. Falta de actualizaciones. Falta de parches de seguridad.
	Programas	Instalación / desinstalación no controlada Instalación programas maliciosos. Falta de documentación. Control inadecuado de versiones. Pruebas de software insuficientes.

Nota: La tabla muestra el estado actual de la seguridad de la red de la UESCS.
Elaborado por: Los autores, a partir de la entrevista al departamento de sistemas de la UESCS.

Tabla 5.
Falencias encontradas acerca de los usuarios de la red de la UESCS.

Usuarios	Falta de conciencia de seguridad.
	Falta de capacitación.
	Falta de políticas, normas, procedimientos.
	Contraseñas predeterminadas no modificadas.
	Clasificación inadecuada de la información.
	Respaldo inapropiado o irregular.
	Falta de información y conciencia sobre seguridad
	Inadecuada gestión y protección de contraseñas.
	Falta de política de acceso o política de acceso remoto.
	Falta de documentación interna.

Nota: La tabla muestra las falencias encontradas con respecto a los usuarios de la UESCS.
Elaborado por: Los autores, a partir de la entrevista al departamento de sistemas de la UESCS.

CAPÍTULO 2

2.1 Fundamento teórico

2.1.1. Definición de ingeniería social

En el ambiente de la seguridad, se debe tomar en cuenta todas las amenazas en contra de la red, por lo tanto, estas amenazas se convierten en un riego latente a la información de las organizaciones tanto públicas como privadas.

La ingeniería social, no es exclusivamente un campo de estudio en la seguridad de redes, esta ha sido estudiada desde muchos años atrás, en diferentes áreas, tanto políticas, sicológicas, etc. (Granger, 2001)

Kevin Mitnick, califica a la ingeniería social como el punto débil en la seguridad de la información, el autor considera que el factor determinante en la seguridad de las redes, no es el software o el hardware que se implemente en la organización, sino la capacidad de los usuarios en interpretar y cumplir las políticas de seguridad. (Mitnick, 2001)

Según Daniel Huerta en su libro "Ingeniería Social", define a la ingeniería social como el uso de técnicas y tareas planeadas con anticipación que permiten manejar las acciones de las diferentes personas para conseguir que realicen acciones que no realizarían normalmente. (Huerta, 2010)

2.1.2. Historia

En 1984, en el ensayo redactado por J.C. Van Marken, se comenzó con el uso del término, pero es en 1909 que W.H. Tolman lo introdujo en los Estados Unidos, para detallar el trabajo que realizaba el ingeniero social como un mediador para la resolución de problemas en las empresas.

Karl Popper, en el año de 1945, introduce esta expresión para llevar a cabo e implementar métodos críticos y racionales, en la ingeniería y ciencias sociales. (Huerta, 2010)

Desde la década de los 40 en que el término tomó notoriedad, hasta la fecha actual, la utilización de esta técnica para cometer ataques, que en un principio se realizaron como una impersonalización a través de llamadas telefónicas, hoy en día el atacante busca ser imperceptible para la víctima, usando técnicas y medios digitales. (redes sociales, correo electrónico, SMS, etc.)

2.1.3. Principios básicos de la ingeniería social

Según Mitnick, existen cuatro principios básicos de la ingeniería social (Mitnick, 2001):

Principios básicos.

Figura 8. Principios básicos de la Ingeniería Social.
Elaborado por: Los autores, a través de la información obtenida de (Mitnick, 2001).

La ingeniería social, parte del estudio del comportamiento humano, esto supone que, si se establece una relación de forma adecuada con la víctima, apelando a su ingenuidad, se puede obtener la información necesaria. (Iglesias, 2017)

2.1.4. Tipo de hackers

La clasificación general está compuesta por tres tipos: Hackers de sombrero blanco, sombrero negro y sombrero gris, pero a través de los años se ha ido encontrando nuevos tipos hasta instituir una amplia lista. (Astudillo, 2013; Espinosa, 2012)

Tabla 6.
Tipo de hackers.

Hackers sombrero blanco	Son expertos en seguridad, se los conoce como hackers éticos, utilizan sus conocimientos para realizar pruebas de penetración en busca de brechas de seguridad y la aplicación de metodologías para garantizar que las redes y sistemas de información sean seguros. A diferencia de otro tipo de hacker, estos cuentan con el permiso de los propietarios, así que sus actividades se vuelven legales.
Hackers sombrero negro	Comúnmente conocidos como hackers o crackers, a diferencia de los de sombrero blanco, estas personas penetran en redes o computadores, utilizando diversos métodos para realizar actos delictivos, su motivación es el beneficio tanto personal como económico.
Hackers sombrero gris	Realizan actividades similares que los hackers de sombrero blanco y negro, a diferencia de estos, estas personas buscan vulnerabilidades con o sin el consentimiento de los dueños, al momento de encontrar alguna novedad, suelen comunicarse con los administradores de la red, en algunos casos solicitan una recompensa, por ubicar la brecha de seguridad, y resolver el problema.
Script Kiddies	Son personas que están comenzando en este mundo, utilizan programas automatizados escritos por otros para realizar ataques a sistemas informáticos, redes, páginas web, generalmente tienen poca o ninguna comprensión de los diferentes conceptos, su motivación es la de impresionar a sus pares.
Hacktivistas	Son personas que usan su conocimiento como una forma de protesta a través de la red, su trabajo consiste en utilizar la tecnología para enviar su mensaje (social, político, religioso, etc.).
Hackers patrocinados por el estado	Son personas o grupos que son entrenados y/o financiados por un gobierno, su principal objetivo es el espionaje y la guerra cibernética, tienen un presupuesto y tiempo ilimitado para realizar ataques a personas, organizaciones u otros gobiernos.
Hackers espía	Estas personas son contratadas para realizar espionaje e infiltrarse de forma física o a través de la red, en compañías u organizaciones para obtener secretos comerciales, su única motivación es servir a los deseos de sus empleadores.
Informantes	Son personas dentro de una empresa, que filtran información sensible, utilizando el acceso obtenido previamente, en general estas personas tienen malas intenciones y rencor, su objetivo es el de lucrar con la información obtenida o conseguir un empleo mejor en una empresa rival.
Ciberterroristas	Estos hackers, son personas con motivaciones políticas y/o religiosas, su principal objetivo es el de crear caos y generar miedo al alterar los sistemas de información críticos, por ejemplo, el sistema de una torre de control.

Nota: La tabla muestra los tipos de hackers que se encuentran en la actualidad.
Elaborado por: Los autores, a través de la información obtenida de (Astudillo, 2013; Espinosa, 2012).

2.1.5. Técnicas de ataques de ingeniería social

Las técnicas de ataques de ingeniería social dependen en la facilidad que se tenga parar poder realizarlas, se dividen en dos grandes grupos:

2.1.5.1. Ataques de ingeniería social personales

Busca obtener información a través de las interacciones sociales, el atacante establece una relación con la víctima de manera directa, estos ataques se aprovechan del miedo, la ingenuidad o el simple hecho de ayudar. (García, 2017; Hinojosa, 2010)

Tabla 7.
Ataques personales de ingeniería social.

Llamadas telefónicas	Este es uno de los primeros ataques de ingeniería social conocidos, el atacante se comunica con la víctima, suplantando la identidad de una persona, con el fin de recolectar información, utilizando engaños, amenazas, falsos reportes, etc.
Relaciones basadas en engaños	La víctima siente que la persona con la cual se está comunicando, tienen afinidad alguna, los mismos intereses o quieren lo mismo en la vida, esto favorece que se cree una relación fuerte, mientras la víctima entrega información que se necesita para acceder a la red.
Ingeniería social inversa	El atacante utiliza la red de la empresa para crear el problema y luego que la víctima ha encontrado el problema, el atacante mismo soluciona el problema.
Buscar en la basura	Otra de las formas en que se puede obtener información, aunque suene algo bizarro, y que sigue en uso, es buscar entre la basura de las personas, todas ellas a la final crean desechos, como por ejemplo el correo, documentos varios con información personal, implica el estar metido entre los tachos de basura, en la mayoría de casos la información encontrada no es trascendental, pero en ocasiones revelan mucho más de lo que parece.
Acceso físico	Los atacantes suelen evitar el lugar en el cual realizaran el ataque, pero en algunos casos visitan las organizaciones, para obtener información que facilite el acceso, para esto utilizan la suplantación de identidad de algún empleado de la misma, así poder transitar de manera más tranquila en las instalaciones.
Engaño mediante escenarios ficticios	El atacante crea un escenario ficticio para persuadir a la víctima de que entregue información o que esta realice una acción, para esto se utiliza información antes conseguida (fecha de nacimiento, saldo de la cuenta, información familiar), para establecer confianza.
Mirar sobre el hombro	Esta técnica consiste en observar a la víctima de manera indirecta, sin levantar sospechas, por lo general esta técnica ocurre en las oficinas al momento que el atacante observa lo que la víctima está tecleando, en ese momento puede estar ingresando información confidencial como una contraseña.
Seguir de cerca	En las diferentes organizaciones existen, medios de seguridad físicos como, por ejemplo, puertas con acceso biométricos o con tarjeta, las cuales llevan a lugares estratégicos para el atacante, para esto siguen de cerca a las personas mientras dejan abiertas las puertas, en algunos casos el atacante se aprovecha del desconocimiento de las personas para que le permitan el acceso.
Suplantación de identidad	Los atacantes se hacen pasar por autoridades de alto rango de las organizaciones que son el blanco del ataque, y así obtener acceso a lugares con información clasificada y sensible. Aunque el término dicta, de que se trata de un ataque personal, la suplantación de identidad en la actualidad a evolucionado a la par de la tecnología, se aprovechan en muchos casos de las vulnerabilidades de las víctimas para obtener información de las mismas, a través de correos electrónicos, redes sociales o medios de mensajería instantánea.

Nota: La tabla muestra los tipos de ataques personales de ingeniería social.
Elaborado por: Los autores, a través de la información obtenida de (García, 2017; Hinojosa, 2010).

2.1.5.2. Ataques de ingeniería social tecnológicos

Estas agresiones usan la tecnología para crear el vínculo entre el delincuente y su objetivo, buscando no tener interacción directa, con el atacado. (Cordero, 2018; García, 2017; Hinojosa, 2010)

Tabla 8.
Ataques tecnológicos de ingeniería social.

Baiting	Esta técnica es una de las más usadas por los hackers más experimentados, en la cual dejan USB infectada, en lugares públicos, en empresas, con la esperanza de que sea utilizada. En la actualidad la evolución de esta técnica está en toda la red, por ejemplo, en un enlace de descarga, una página de publicidad engañosa.
Correos electrónicos	Los correos electrónicos son una herramienta simple y poderosa a la vez para la comunicación con varias víctimas a la vez, el alto volumen de correo que se maneja, hace que no se preste la atención necesaria al remitente o al contenido, creando así un vector de contagio, todo esto facilita el trabajo del atacante.
Farming	El objetivo de este ataque es el de mantener el engaño el mayor tiempo posible, para conseguir el mayor volumen de información, para esto se recurre al uso de granjas de identidades, obtenidas con anticipación. Este tipo de ataque también depende del pretexting, recreando un escenario lo altamente creíble y confiable, que ayude a que el engaño dure lo más posible.
Phishing	Esta práctica, siendo una de la más comunes en ingeniería social, consiste en enviar un mensaje a través de un medio electrónico, el cual hace creer a la víctima que es de una institución de confianza, sin conocer el verdadero objetivo, la víctima es redirigida hacia una página en la cual, se le solicita información personal y sensible.
Pretexto	Es un escenario recreado por parte del atacante, con el fin de crear una relación con la víctima, el objetivo este ataque es el de extraer la mayor cantidad de información posible, estas situaciones apelan a la tendencia de las personas de recibir un servicio gratuito, recibir un premio o ayudar a un tercero. Hacen uso de llamadas telefónicas, mensajería instantánea y/o correo electrónico.
Spear Phishing	Es una práctica relacionada con el phishing, pero en este caso está más relacionada a una organización que a una sola víctima, por lo cual esto requiere un mayor esfuerzo de la parte del atacante, quien debe obtener un volumen más alto de información, una vez obtenida la información se procede al envío de mensajes a través de todo medio electrónico, que resulten relevantes, que logre persuadir a las víctimas de revelar información sensible acerca de la organización.
Vishing	El atacante usando llamadas telefónicas, o recreando el sistema de voz interactiva de las organizaciones bajo ataque, intenta engañar a los empleados para que revelen información sensible de carácter personal, financiero, etc.
Hunting	Es la unión de un grupo de ataques, por ejemplo, baiting, phishing, vishing, todo esto con el propósito de extraer tanta información de la víctima o a la organización bajo ataque, con la menor interacción posible.

Nota: La tabla muestra los tipos de ataques tecnológicos de ingeniería social.
Elaborado por: Los autores, a través de la información obtenida de (Cordero, 2018; García, 2017; Hinojosa, 2010).

2.1.6. Herramientas de ingeniería social

La persona al escuchar ingeniería social, inmediatamente lo relaciona con actos delictivos, sin embargo, estas herramientas y técnicas son utilizadas por los analistas de seguridad para examinar la red de una organización. (Astudillo, 2013; Haro & Parra, 2016)

Tabla 9.
Herramientas de ingeniería social.

Social-Engineer Toolkit (SET)	Es un marco de pruebas de penetración de código libre para Linux como para MacOS, diseñado por David Kennedy de la compañía TrustedSec, tiene una serie de vectores de ataques que pueden ser personalizados, permiten crear diversos ataques y pruebas rápidamente y sobre todo creíbles. Algunos de los ataques que vienen dentro de este framework son por ejemplos el Phishing y el Spear Phishing, que utilizan el correo electrónico como vector de contagio con el objetivo de manipular a la víctima para conseguir información. Además, incorpora un cosechador de credenciales, el cual permite obtener credenciales de varios usuarios por diferentes métodos, por ejemplo, clonando una página web en la cual se soliciten información de identidad y contraseña.
Saint	Es un generador de spyware para Windows escrito en lenguaje java por Tiago Lampert, permite crear un archivo ejecutable que, al infectar una computadora, da como resultado recibir información de qué está tecleando la víctima, a través de un correo electrónico, además permite que se tomen capturas de pantalla, fotos a través de la cámara web del computador, y crear persistencia. Este spyware necesita que la máquina víctima tenga instalado Java JRE, caso contrario no funcionará.
Metasploit framework	Es una herramienta o más bien un conjunto de programas que permiten desarrollar y ejecutar exploits contra sus objetivos para tomar el control remoto de sus equipos, es usado ampliamente en pruebas de penetración orientadas a la seguridad, esto permite que el administrador de red conozca si su red es vulnerable y/o tiene brechas de seguridad que pueden ser utilizadas en su contra. Antes de utilizar este framework, se necesita de algún otro programa de detección como Nessus o Openvas.
Resource hacker	Esta herramienta creada por Angus Johnson en lenguaje Objeto Pascal, se usa para modificar varios elementos de un S.O. o un programa, por ejemplo, recursos ejecutables, enlaces dinámicos, librerías y ejecutables. También ofrece las opciones para compilar y descompilar otros recursos desde su línea de comandos.
SFX compiler	Esta herramienta desarrollada por Uticasoft, permite compilar tantos archivos dentro de un único fichero ejecutable, una vez que se ejecute este ejecutable, todo lo que se encuentra dentro se guardará en el disco, que mantiene la estructura original.

Nota: La tabla muestra las herramientas de ingeniería social.
Elaborado por: Los autores, a través de la información obtenida de (Johnson, 2019; Lampert, 2017; OffSec, s.f.).

2.2. Ciberhigiene

El término ciber higiene, acuñado por el Dr. Vinton Cerf, quién utilizó por primera vez esta expresión en su presentación ante el Comité de economía del Congreso de los Estados Unidos. (Cerf, 2000)

Extracto de la Presentación del Dr. Cerf.

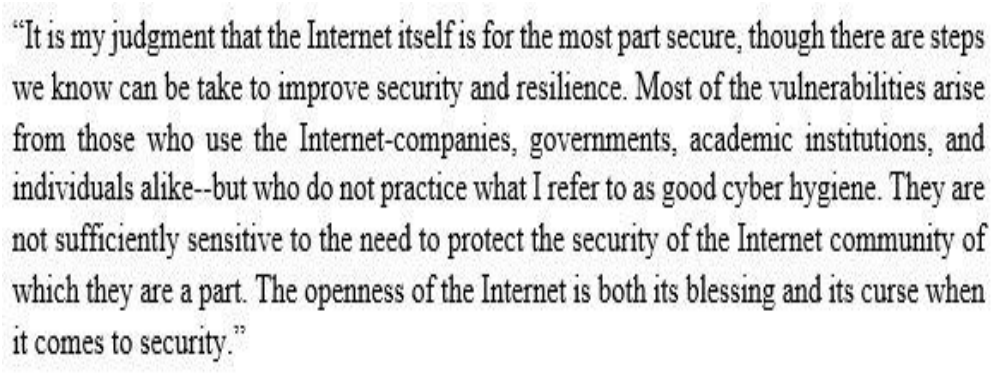

"It is my judgment that the Internet itself is for the most part secure, though there are steps we know can be take to improve security and resilience. Most of the vulnerabilities arise from those who use the Internet-companies, governments, academic institutions, and individuals alike--but who do not practice what I refer to as good cyber hygiene. They are not sufficiently sensitive to the need to protect the security of the Internet community of which they are a part. The openness of the Internet is both its blessing and its curse when it comes to security."

Figura 9. Extracto de la presentación Dr. Vinton Cerf con respecto a la ciber higiene al congreso de los EEUU.
Fuente: *(Cerf, 2000)*, obtenido de https://www.jec.senate.gov/archive/Documents/Hearings/cerf22300.html

La higiene cibernética detalla las buenas prácticas y acciones que los administradores y usuarios de la red deben efectuar, para mantener en estado óptimo a los equipos y sistemas, y así, mejorar la seguridad de la red. (Brook, 2018)

Esto consiste en la capacitación de los usuarios de la red, para que piensen de forma dinámica acerca de la seguridad informática, así como lo hacen con su higiene personal, para hacer frente a las diferentes amenazas informáticas, una vez que estas prácticas se consoliden debidamente en la institución, serán simples rutinas diarias, buenas prácticas y revisiones ocasionales para garantizar la seguridad de la red. (Ciberseguridad, 2019)

Fomentar la práctica de la higiene cibernética en la institución, es beneficioso por dos grandes razones: mantenimiento y seguridad.

El mantenimiento en los equipos y programas es necesario para que estos se ejecuten de forma óptima, al mantener esta rutina la posibilidad de revelar problemas aumenta, y esto ayuda a impedir que se originen problemas más graves, ya que una red bien mantenida es menos probable que sea vulnerable a riesgos de ciberseguridad.

La seguridad es la razón más importante para integrar una rutina de higiene cibernética, en la actualidad las amenazas se encuentran en constante cambio, por esto es imprescindible usar una rutina de higiene cibernética, para evitar que los hackers, virus, etc., accedan y comprometan la seguridad de la red. (RSI, 2019)

La higiene cibernética es responsabilidad de todos, tanto de usuarios y de administradores, para esto existen varias prácticas recomendadas para garantizar que su higiene sea lo mejor posible, los seis pasos esenciales son:

2.2.1. Asegurar que los enrutadores y cortafuegos estén instalados y configurados.

Los enrutadores y cortafuegos actúan como la primera línea de defensa de la red, ya que estos evitan que usuarios ajenos a la red accedan a los servidores y otras fuentes de información. (Brook, Digital Guardian, 2018)

Antes de nada, el administrador de red debe cambiar la configuración predeterminada de los equipos, especialmente la contraseña, ya que estas se pueden encontrar fácilmente a través de una simple búsqueda en Google, mantener la configuración predeterminada de fábrica facilita el trabajo al hacker para entrar a los dispositivos, además, se debe asegurar que se habilitaron y configuraron los servicios de protección de los dispositivos.

Los cortafuegos deben ser capaces de escanear todo el tráfico, esto requiere más que una inspección de paquetes, se debe escanear los puertos y protocolos, además

debe permitir la creación de políticas de forma simple y flexible, por ejemplo, debe garantizar el acceso a una aplicación en particular, en el departamento de comunicación se debe permitir el acceso a redes sociales para llevar a cabo campañas de publicidad, caso contrario con un empleado del departamento financiero. (Axis, s.f.)

Los enrutadores también ofrecen seguridad a la red, ya que permiten conocer quien está conectado, conocer las páginas accedida por cada equipo, y bloquear usuarios no deseados.

2.2.2. Instalar software antivirus y software anti malware.

Son desarrollados para analizar, buscar y eliminar virus, malware, etc., los cuales pueden exhibir la red a varios ataques, son una pieza valiosa en la higiene cibernética. (Brook, CyberSecurity Forum, 2018)

Entre sus diferentes funciones, los antivirus son efectivos ante amenazas, a través del correo electrónico, escanea si estos traen virus maliciosos y otras amenazas, en las últimas actualizaciones, estos traen nuevas funciones que operan directamente en un conjunto determinado, por ejemplos datos financieros, esto bloqueará tentativas de acceso no autorizado, impidiendo que se extraiga la información. (Brook, CyberSecurity Forum, 2018)

2.2.3. Establecer contraseñas robustas

Es una buena práctica el establecer contraseñas seguras, esto evitará que los usuarios malintencionados las descubran. Una contraseña segura por ejemplo debería ser mayor a 12 caracteres entre mayúsculas y minúsculas.

Las contraseñas no deben ser compartidas, deben ser cambiadas regularmente y no utilizar las mismas al cambiar. (Brook, Digital Guardian, 2018)

Las contraseñas de firmware, ayudan como controles adicionales en los equipos, estas permiten evitar que otras personas usen el computador, que se reinicie o se restablezca.

Entre las fallas de seguridad de los usuarios, estos utilizan como contraseñas, dato que les sea fácil recordar, por ejemplo, fechas de cumpleaños, nombres de familiares, lugares conocidos, etc., esto facilita al atacante conseguir las contraseñas de los usuarios. (Brook, CyberSecurity Forum, 2018)

2.2.4. Emplear encriptación en las comunicaciones y dispositivos.

La encriptación oculta la información a través de un proceso, que hace a la información inaccesible a terceros. Esta práctica ha demostrado que existe una mayor protección de la información en la red. (Brook, Digital Guardian, 2018)

Se debe asegurar que al menos se esté utilizando uno de los protocolos de autenticación como son HTTP y HTTPS, esto nos asegura que toda la información esté encriptada antes de ser enviada a través de la red, reducen la posibilidad de ser víctimas de algún ataque, por ejemplo, de espionaje, en el cual el código malicioso escucha transmisiones sin cifrar.

Mantener todos los datos de usuario y de aplicaciones de usuario separados, de misma forma con los datos personales de los comerciales, aplicando un cifrado seguro (AES-256 o superior) con contraseñas seguras para todos los datos sensibles y confidenciales, incluidos, los datos financieros. (Axis, s.f.)

Considere un servicio de correo electrónico seguro, con cifrado de extremo a extremo para garantizar que su contenido permanezca privado.

2.2.5. Autentificación multifactor

Esta práctica ofrece una seguridad adicional a la protección en la red, esta autenticación requiere que se envíen dos o más códigos de verificación para tener el acceso correcto, por ejemplo, la contraseña y un código adicional que puede llegar a través de un correo o un mensaje de texto. (Brook, CyberSecurity Forum, 2018)

Para conseguir esto se recomienda utilizar la autenticación de dos factores (2FA) o la autenticación multifactor (MFA), que agrega una capa de seguridad adicional a las contraseñas, siempre y cuando esto sea práctico, especialmente en datos financieros, personales, y otros datos confidenciales. 2FA y MFA aumentan la seguridad al garantizar la contraseña con información adicional, por ejemplo, con un pin único, datos biométricos (huellas dactilares), dispositivos secundarios (teléfono móvil). (Axis, s.f.)

2.2.6. Actualizar software regularmente

INCIBE, exhorta actualizar habitualmente las aplicaciones, navegadores web y sistemas operativos, con esto se asegura que se encuentran instalados los parches de seguridad actuales, cuales enmendaran problemas existentes en versiones anteriores, además de siempre elegir la opción de actualizaciones automáticas esté disponible. (Izquierdo, 2018; OSI, s.f.)

En general las actualizaciones incluyen parches de correcciones para mejorar la seguridad de los equipos, por esta razón, se debe considerar que el software antiguo es susceptible de ser atacado, ya que los atacantes han tenido más tiempo para encontrar y descubrir las diferentes vulnerabilidades. (INCIBE, s.f.)

2.3. FUNDAMENTO METODOLÓGICO

2.3.1. Proyecto piloto

Es un esfuerzo temporal que se realiza para comprobar la factibilidad de un resultado exclusivo del trabajo propuesto. Temporal representa que, el trabajo tiene una fecha final; exclusivo expresa que, el resultado final del trabajo es diferente al resultado de otras soluciones del trabajo propuesto. (Emanuelli A., 2014)

La figura 10 muestra el ciclo de vida de un proyecto piloto, el cual está conformado por las siguientes etapas: (Emanuelli A., 2014)

Ciclo de vida.

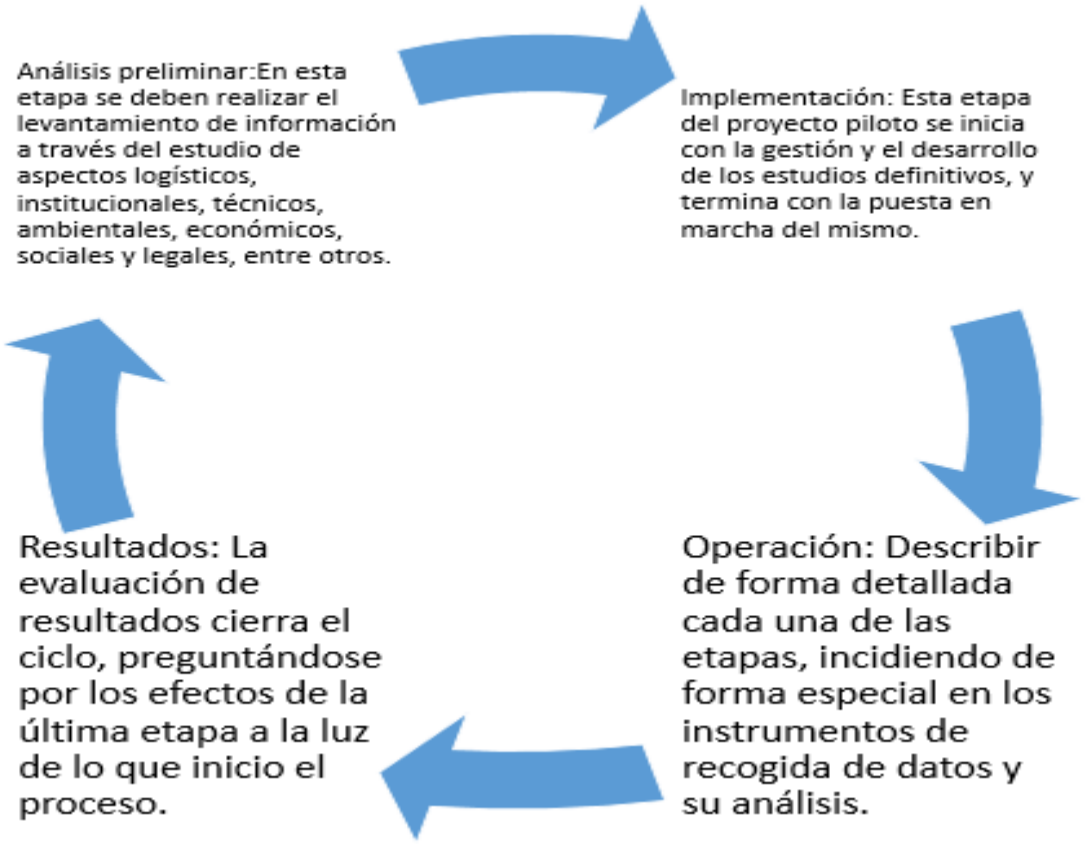


Figura 10. Ciclo de vida Proyecto Piloto.
Elaborado por: Los autores, a partir de la información obtenida de (Emanuelli A., 2014).

CAPÍTULO 3

3.1. Diseño de los escenarios de investigación

3.1.1. La cadena de ataques cibernéticos (The Cyber Kill Chain)

Es un modelo de defensa y seguridad que se basa en investigación, recopilación de información e inteligencia para la identificación y prevención de ataques informáticos, establece pasos que deben seguir los atacantes, con el fin de lograr su meta (Catota, 2010; Hospelhorn, 2020), en la figura 11 se muestran las siete etapas que dicta este modelo, está ligada a una determinada actividad dentro de un ataque informático, este no diferencia si se trata de un ataque interno o externo. (Martin, s.f.)

Etapas de la cadena de ataques cibernéticos.

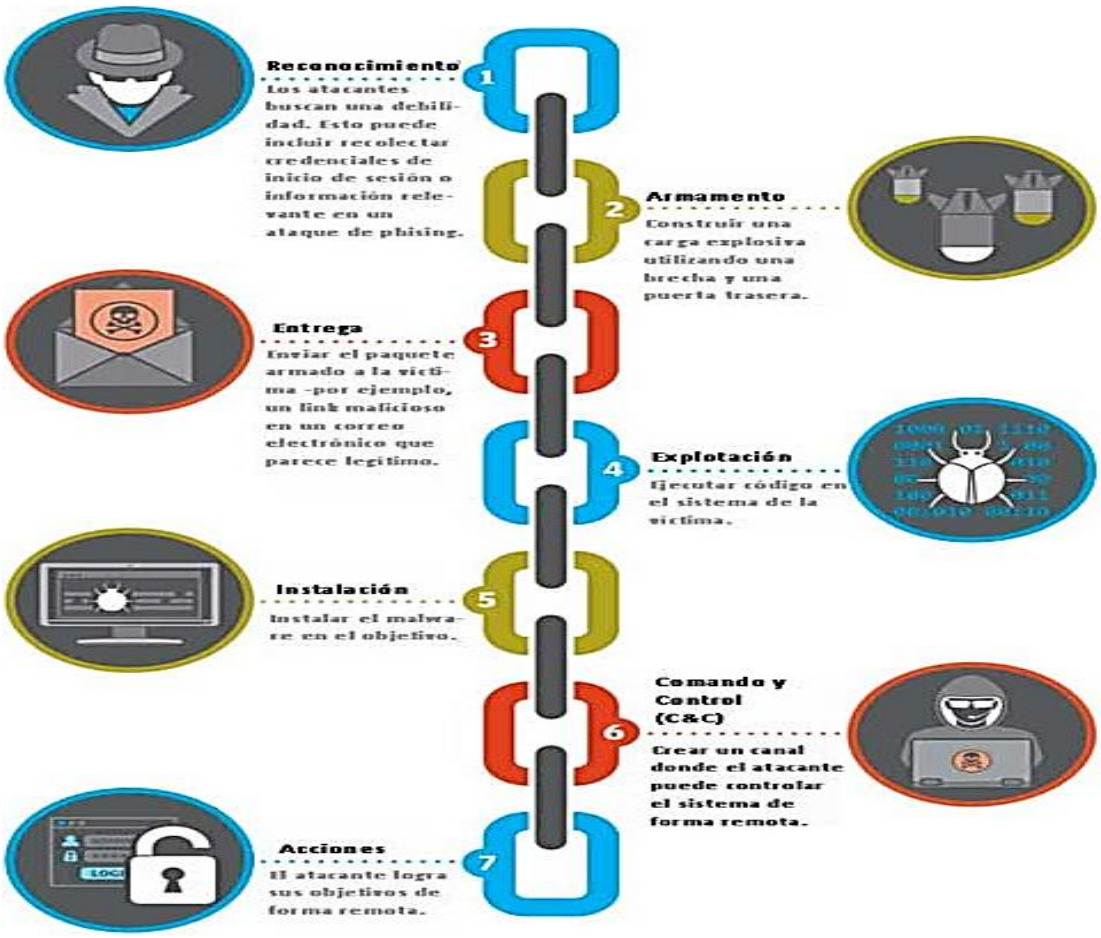


Figura 11. Etapas de Cyber Kill Chain.
Fuente: (Martin, s.f.), obtenido de https://www.lockheedmartin.com/en-us/capabilities/cyber.html

En base en el modelo Cyber Kill Chain, siguiendo los pasos expuestos en la figura 11, se desarrollarán los escenarios de investigación.

Para la creación de los escenarios de investigación, se tomó en cuenta el estado actual de la seguridad de la red de la UESCS, sobre todo las falencias encontradas en relación a sus usuarios, además de la investigación acerca de las técnicas y herramientas de ingeniería social.

Se escogió la herramienta SET (Social-Engineering Toolkit), la cual está diseñada para realizar ataques contra el usuario, además permite automatizar labores, desde el envío de correos electrónicos, mensajes de texto falsos, a clonar una página web para realizar ataques en pocos minutos.

3.1.2. Escenario 1 – Spoofing – clonación de página

Para el desarrollo de este escenario, se aplicará la técnica de Spoofing, utilizando el correo institucional como medio de propagación, además de la plataforma SET, que se encargará de crear la página web clonada para la recolección de datos.

Dentro del correo electrónico, se notifica que se realizará una conexión entre la plataforma Esemtia y las cuentas de correo institucional, para esto se le solicita ingresar el usuario al enlace incluido dentro del correo, que lo dirigirá hacia una página web maliciosa.

Cabe recalcar que la intención es conocer las vulnerabilidades en el ámbito de usuarios y observar la respuesta hacia el ataque, más no a nivel tecnológico.

3.1.2.1. Identificación de víctimas

Para el desarrollo de este escenario, se aplicó el ataque a 10 funcionarios administrativos, que cuentan con acceso a la red interna, además manejan un volumen

alto de información sensible y confidencial de la institución, siendo la parte administrativa más accesible a estos ataques.

Direcciones de correo.

Figura 12. Direcciones de correo electrónicos del personal del departamento administrativo.
Elaborado por: Los autores, a través de la plataforma de correo.

3.1.2.2. Desarrollo del escenario

Para la creación del escenario, en primer lugar, se creó una cuenta de correo ficticia, con usuario dapuente@gmail.com, la finalidad de que se asemeje a una cuenta real, es para ganar la confianza de los usuarios.

Después se creó la página web clonada utilizando SET dentro de Kali Linux, las imágenes a continuación muestran el paso a paso.

Para la clonación de la página web se ha escogido, la página de acceso a la plataforma de Esemtia, siendo una de las más ocupadas dentro de la institución, con la

IP 172.1.16.100, que es la IP de la máquina atacante en la cual se alojará la página creada.

Para ingresar a la plataforma SET dentro de Kali, es cuestión de abrir una consola y escribir setoolkit en la línea de comando.

Acceso a SET.

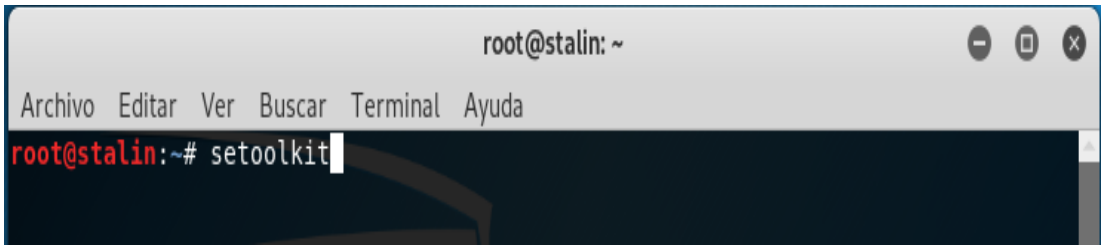


Figura 13. Como ingresar a la herramienta SET.
Elaborado por: Los autores, a través de la herramienta SET (Social-Engineering Toolkit).

Pantalla principal SET.

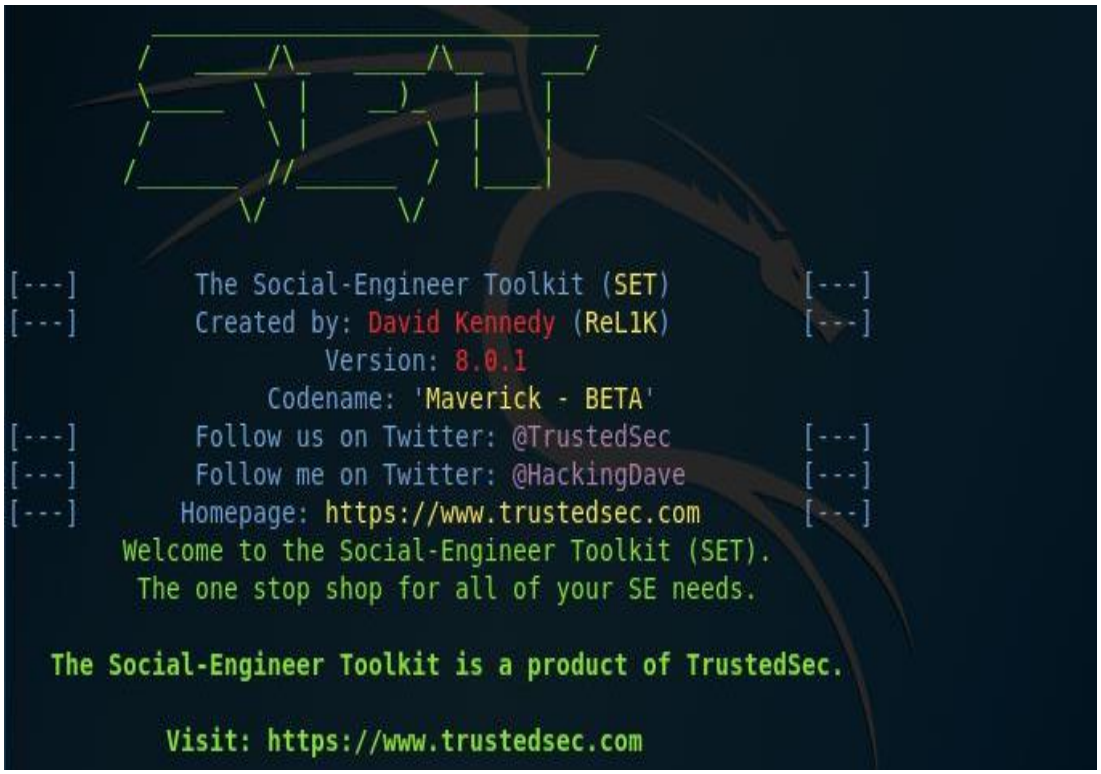


Figura 14. Pantalla principal de la herramienta SET (Social-Engineering Toolkit).
Elaborado por: Los autores, a través de la herramienta SET (Social-Engineering Toolkit).

Dentro de SET, se escogió la opción 1, Social – Engineering Attacks.

Social – Engineering Attacks.

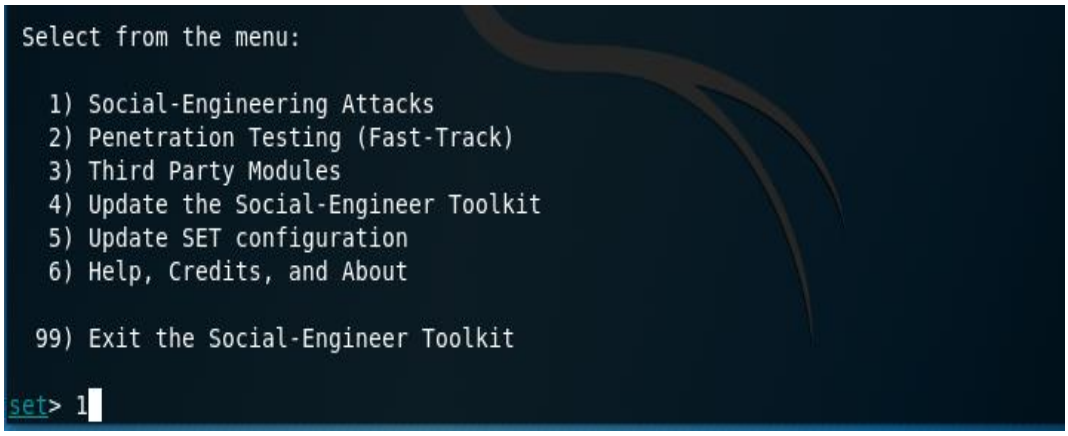


Figura 15. Selección opción Social – Engineering Attacks en la herramienta SET.
Elaborado por: Los autores, a través de la herramienta SET (Social-Engineering Toolkit).

La plataforma SET mostró un nuevo menú, en el que cual se seleccionó la opción 2, Website Attack Vectors.

Website Attack Vectors.

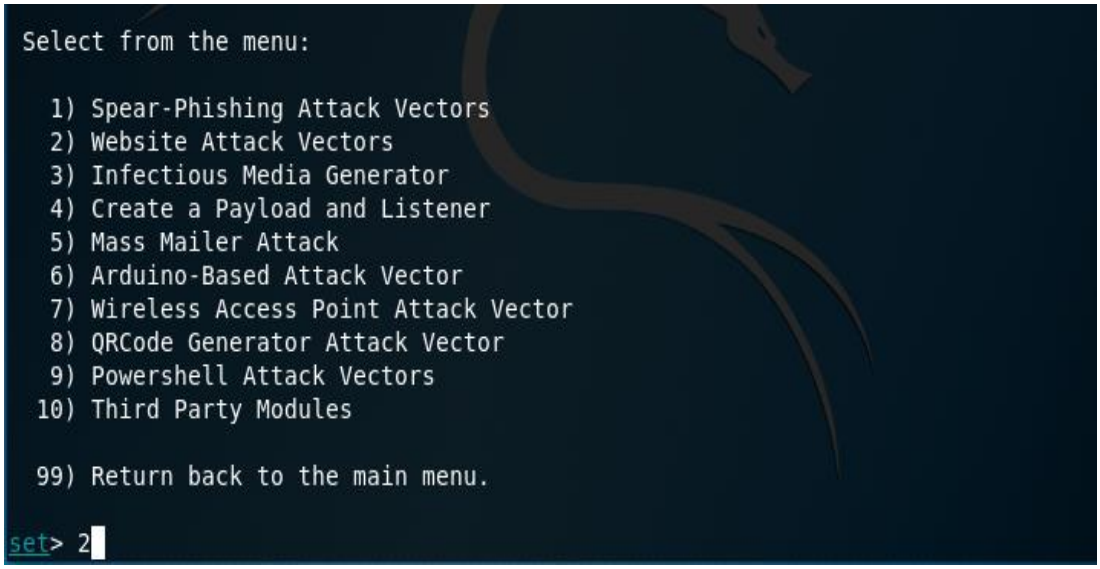


Figura 16. Selección opción Website Attack Vectors en la herramienta SET.
Elaborado por: Los autores, a través de la herramienta SET (Social-Engineering Toolkit).

SET mostró un nuevo menú, con más opciones, para lo cual se eligió la opción 3, Credential Harvester Attack Method.

Credential Harvester Attack Method.

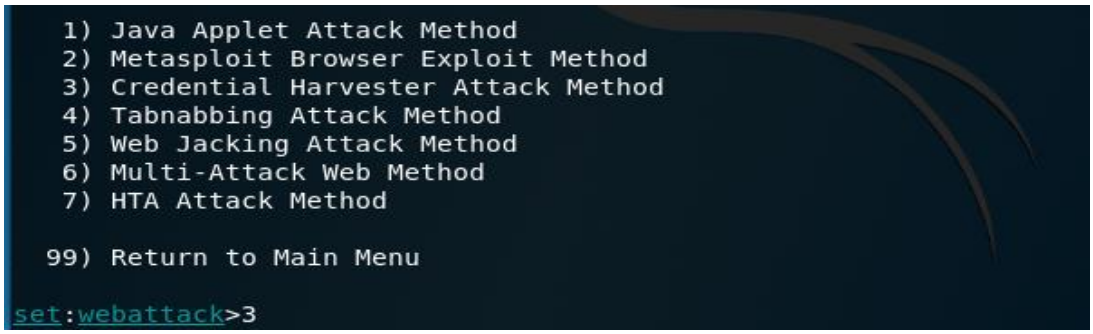


Figura 17. Selección opción Credential Harvester Attack Method en la herramienta SET.
Elaborado por: Los autores, a través de la herramienta SET (Social-Engineering Toolkit).

Y, por último, la plataforma mostrará 3 opciones, para este escenario se va a utilizar la opción 1 Web Templates y la opción 2 Site Cloner, la diferencia entre estas opciones es, la primera opción permite a SET, importar páginas web predefinidas, caso contrario a la segunda opción, la cual realizará la clonación de una página web completa, se recomienda que la página a clonar tenga campos para ingreso de credenciales como usuario y contraseña.

Opción para método de recolección de información.

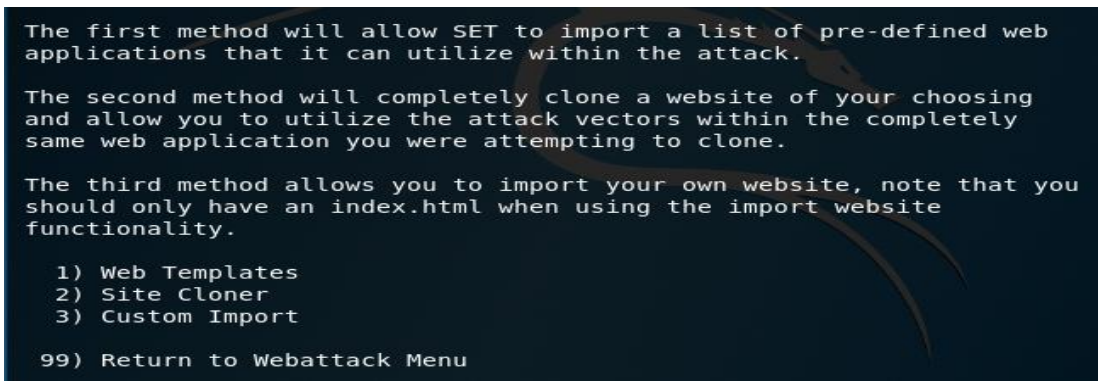


Figura 18. Selección opción Web Templates – Site Cloner en la herramienta SET.
Elaborado por: Los autores, a través de la herramienta SET (Social-Engineering Toolkit).

Primera Opción – Web Templates

Dentro de esta opción, SET solicita que se ingrese la IP de la máquina atacante.

IP máquina atacante.

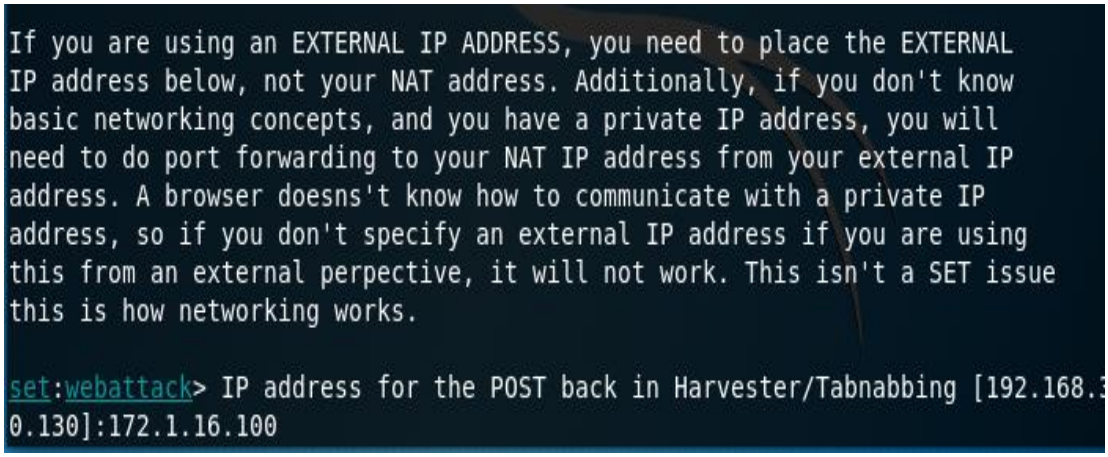


Figura 19. Ingreso IP de la máquina atacante en la herramienta SET, primera opción
Elaborado por: Los autores, a través de la herramienta SET (Social-Engineering Toolkit).

Después de que se ingresó la IP, se desplegó un menú con tres opciones, se seleccionó la opción 2, Google.

Opción Google.

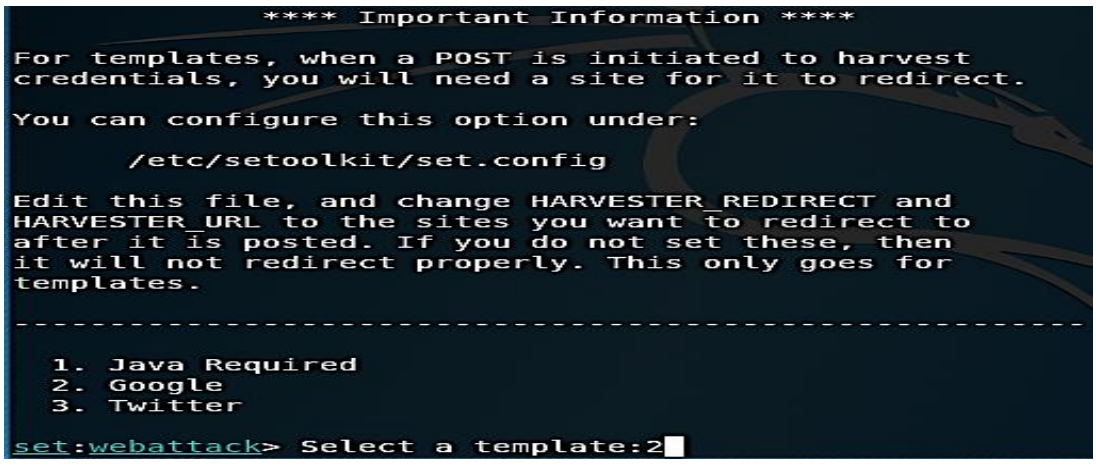


Figura 20. Selección opción Google en la herramienta SET.
Elaborado por: Los autores, a través de la herramienta SET (Social-Engineering Toolkit).

SET precederá a clonar la plantilla y guardarla en la máquina atacante. Para comprobar que la página se ha guardado correctamente, utilizando un navegador web, se debe escribir la IP para visualizar los resultados.

Acceso Google.

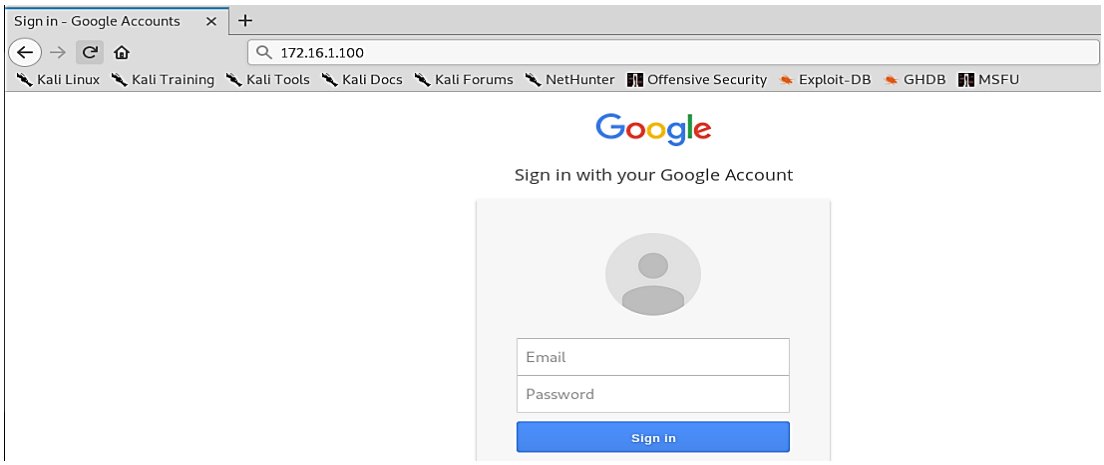


Figura 21. Página de acceso a la plataforma Google clonada.
Elaborado por: Los autores, a través de la herramienta SET (Social-Engineering Toolkit).

Segunda Opción – Site Cloner

Al escoger esta opción, SET realizará la clonación de la página de Esemtia, con la cual se realizará este ataque, como en la primera opción, se ingresa la IP de la máquina atacante.

IP máquina atacante.

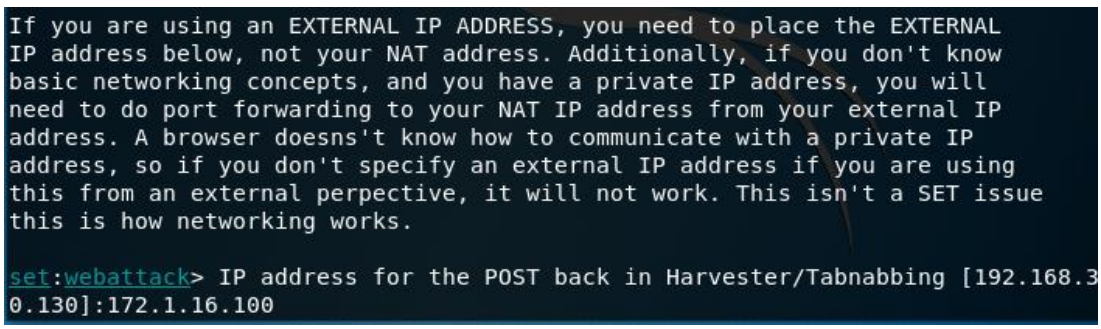


Figura 22. Ingreso IP máquina atacante en la herramienta SET, segunda opción.
Elaborado por: Los autores, a través de la herramienta SET (Social-Engineering Toolkit).

Dirección página Esemtia.

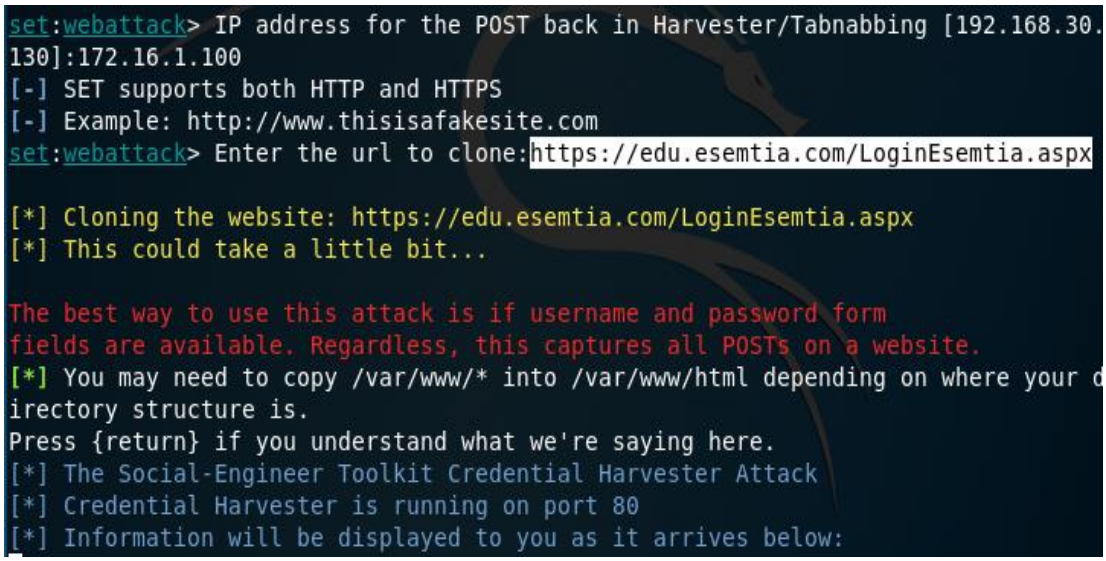


Figura 23. Ingresar la dirección IP de la página web a clonar en la herramienta SET.
Elaborado por: Los autores, a través de la herramienta SET (Social-Engineering Toolkit).

Para comprobar que la página se ha guardado correctamente, utilizando un navegador web, se debe escribir la IP para visualizar los resultados.

Página Esemtia.

Figura 24. Página a la que será el usuario redirigido.
Elaborado por: Los autores, a través del navegador web.

SET al crear un escenario, en este caso Google, guardó la página en la máquina atacante, pero al utilizar la segunda opción de clonación de sitios web, SET realiza el procedimiento, pero no sobrescribe la nueva página clonada, esto da como resultado que después de que se ingresaron los datos, el usuario sea redirigido hacia la página web real de Esemtia, es por esto que al utilizar las dos opciones aumenta la credibilidad del ataque.

3.1.2.3. Entrega del escenario

Para realizar la entrega del enlace de la página clonada maliciosa, se enviará un correo electrónico a los empleados seleccionados.

Cuerpo del correo electrónico.

Figura 25. Correo electrónico enviado a las víctimas, a través de una cuenta ficticia.
Elaborado por: Los autores, a través de la plataforma de correo electrónico.

3.1.2.4. Resultados

Para realizar la recopilación de información, se dejó levantado el servidor por varios días, esperando recibir datos por parte de los empleados, en las siguientes imágenes se muestran la información de los empleados que entraron al enlace e ingresaron sus credenciales.

Credenciales recuperadas.

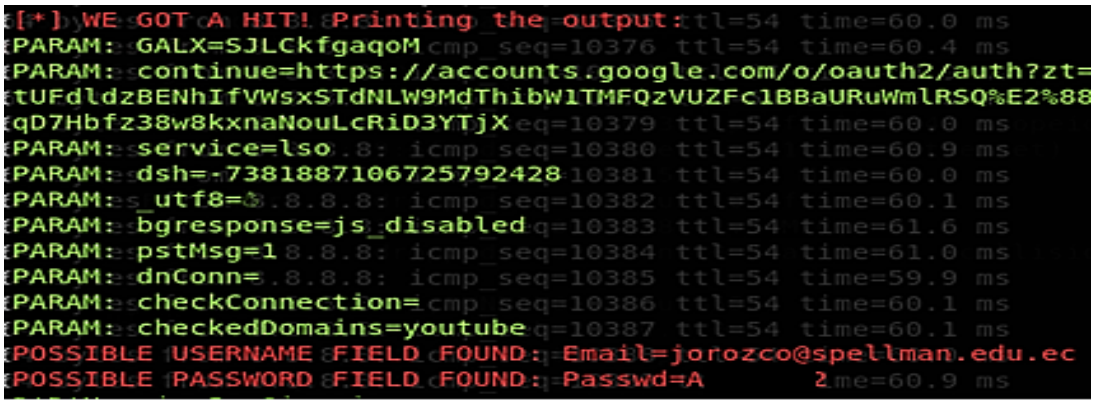


Figura 26. Credenciales primera víctima en la herramienta SET.
Elaborado por: Los autores, a través de la herramienta SET (Social-Engineering Toolkit).

Credenciales recuperadas.

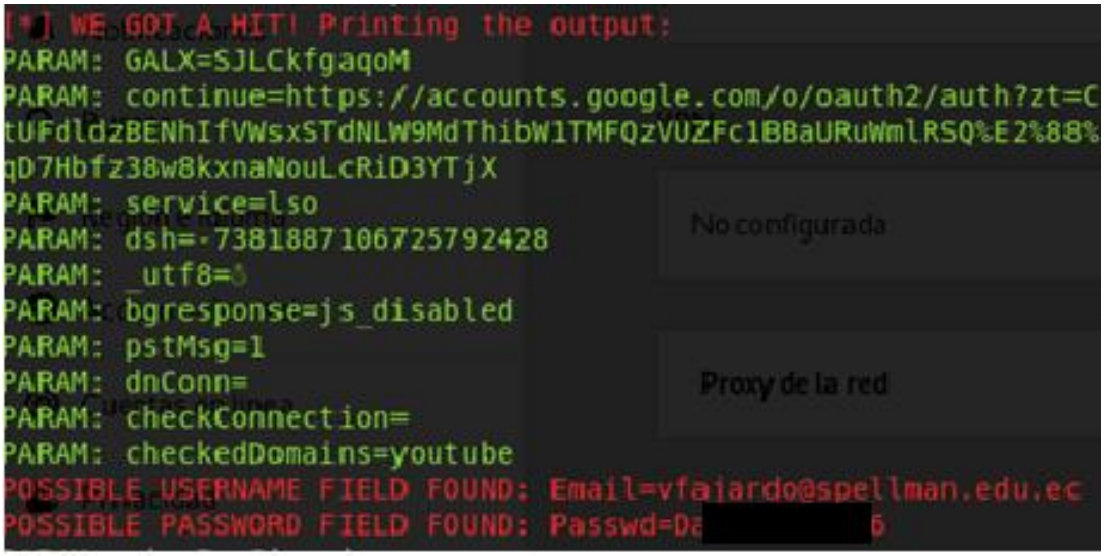


Figura 27. Credenciales segunda víctima en la herramienta SET.
Elaborado por: Los autores, a través de la herramienta SET (Social-Engineering Toolkit).

Credenciales recuperadas.

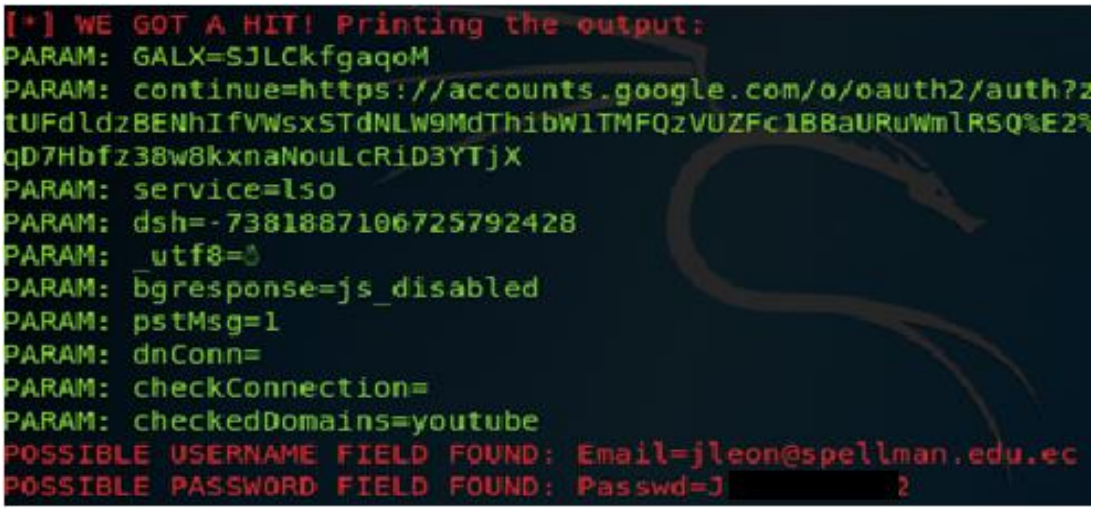


Figura 28. Credenciales tercera víctima en la herramienta SET.
Elaborado por: Los autores, a través de la herramienta SET (Social-Engineering Toolkit).

Credenciales recuperadas.

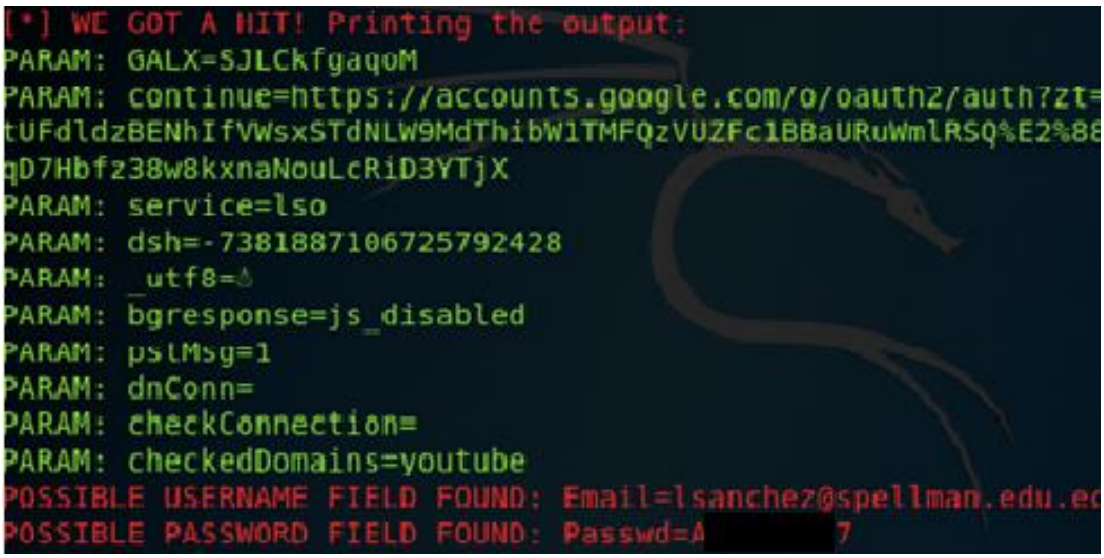


Figura 29. Credenciales cuarta víctima en la herramienta SET.
Elaborado por: Los autores, a través de la herramienta SET (Social-Engineering Toolkit).

Con los resultados, se evidenció que 4 empleados ingresaron al enlace, siguiendo las instrucciones del correo, en las siguientes imágenes se observará las cuentas institucionales de las víctimas, a las que se accedió utilizando la información recopilada en el ataque.

Información personal.

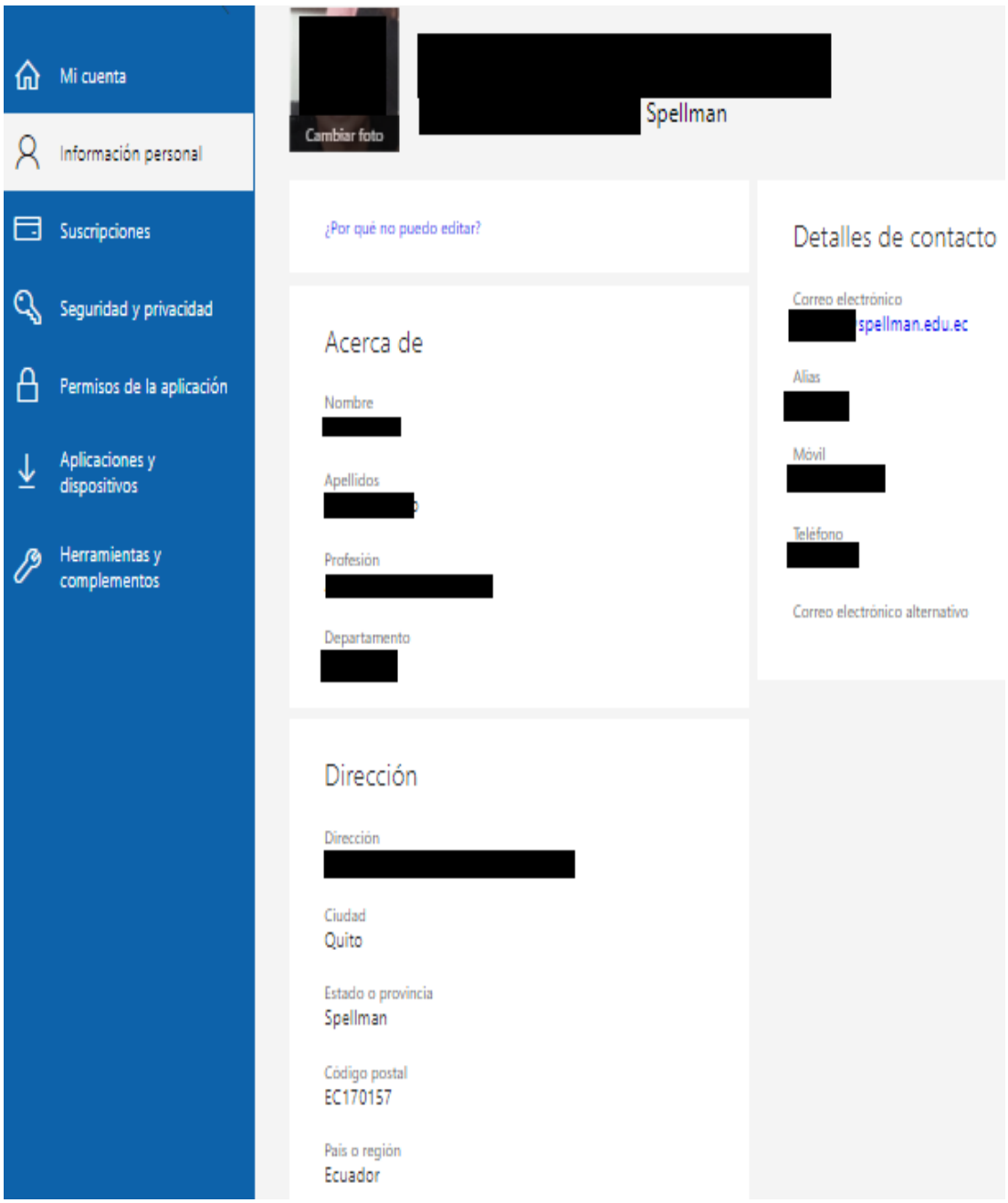


Figura 30. Información personal primera víctima en la plataforma Office 365.
Elaborado por: Los autores, a través de la plataforma Office 365.

En la figura 30 se observa que, al ingresar a la cuenta de la víctima, se obtuvo su información personal, como su dirección, teléfonos de contacto, además, en la opción de seguridad y privacidad se podría cambiar la contraseña de acceso, como se observa en la figura 31.

Cambio de contraseña.

Figura 31. Cambio de contraseña primera víctima en la plataforma Office 365.
Elaborado por: Los autores, a través de la plataforma Office 365.

Con las credenciales de la segunda víctima, se ingresó a su cuenta institucional, como se muestra en la figura 32, se evidencian los documentos en su poder.

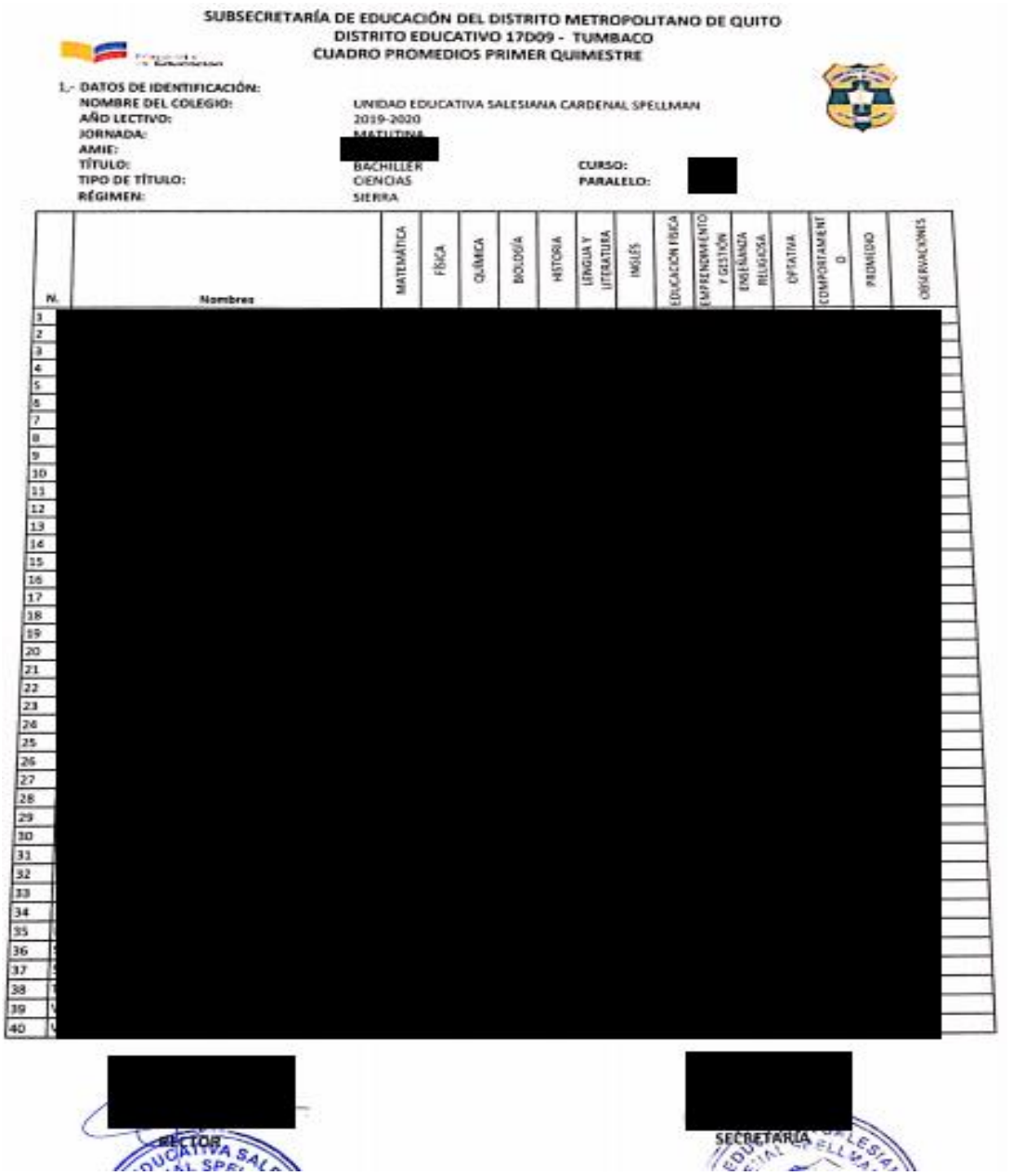
Documentos personales.

Figura 32. Documentos personales segunda víctima en la plataforma Office 365.
Elaborado por: Los autores, a través de la plataforma Office 365.

Al ingresar a uno de estos documentos, se encontró información sensible como los nombres y firmas del rector y secretaria de la institución, como se muestra en la

figura 33, cabe aclarar que el procedimiento realizado con las dos primeras víctimas, se puede realizar con todas, ya que usan la misma plataforma.

Documento con nombres y firmas de autoridades.



SUBSECRETARÍA DE EDUCACIÓN DEL DISTRITO METROPOLITANO DE QUITO
DISTRITO EDUCATIVO 17D09 - TUMBACO
CUADRO PROMEDIOS PRIMER QUIMESTRE

1.- DATOS DE IDENTIFICACIÓN:
NOMBRE DEL COLEGIO: UNIDAD EDUCATIVA SALESIANA CARDENAL SPELLMAN
AÑO LECTIVO: 2019-2020
JORNADA: MATUTINA
AMIE: [redacted]
TÍTULO: BACHILLER
TIPO DE TÍTULO: CIENCIAS
RÉGIMEN: SIERRA
CURSO: [redacted]
PARALELO:

N.	Nombres	MATEMÁTICA	FÍSICA	QUÍMICA	BIOLOGÍA	HISTORIA	LENGUA Y LITERATURA	INGLÉS	EDUCACIÓN FÍSICA	EMPRENDIMIENTO Y GESTIÓN	ENSEÑANZA RELIGIOSA	OPTATIVA	COMPORTAMIENTO	PROMEDIO	OBSERVACIONES
1	[redacted]														
2															
3															
4															
5															
6															
7															
8															
9															
10															
11															
12															
13															
14															
15															
16															
17															
18															
19															
20															
21															
22															
23															
24															
25															
26															
27															
28															
29															
30															
31															
32															
33															
34															
35															
36															
37															
38															
39															
40															

[redacted]
RECTOR

[redacted]
SECRETARIA

Figura 33. Documentos personales segunda víctima en la plataforma Office 365.
Elaborado por: Los autores, a través de la plataforma Office 365.

Con las credenciales de las dos últimas víctimas se ingresó a sus cuentas, en la figura 34 se observa la bandeja de entrada de correo de la tercera víctima, en la figura

35 se observa el acceso a la cuenta, con el correo enviado, el cual tiene el enlace hacia la página maliciosa.

Bandeja de entrada.

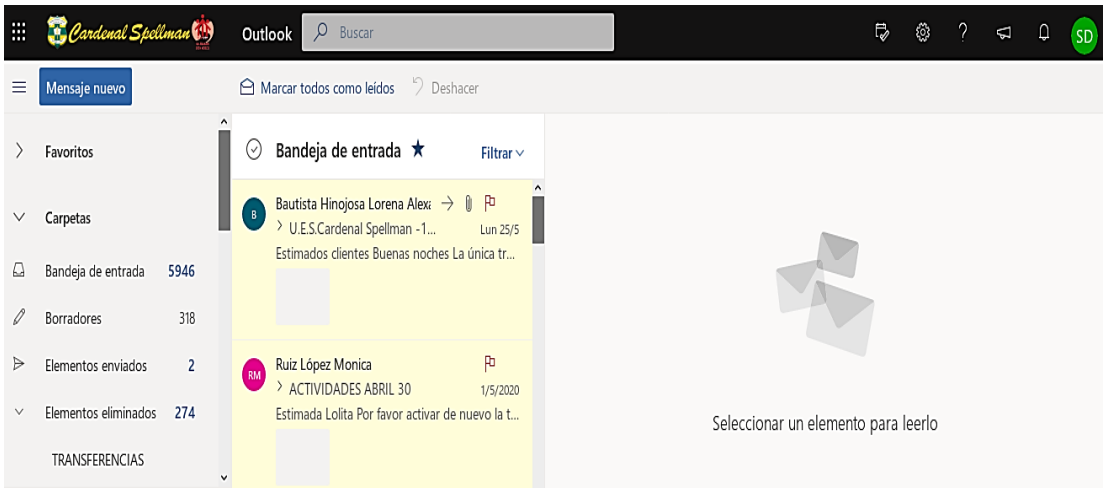


Figura 34. Bandeja de entrada tercera víctima en la plataforma Office 365.
Elaborado por: Los autores, a través de la plataforma Office 365.

Correo evidencia.

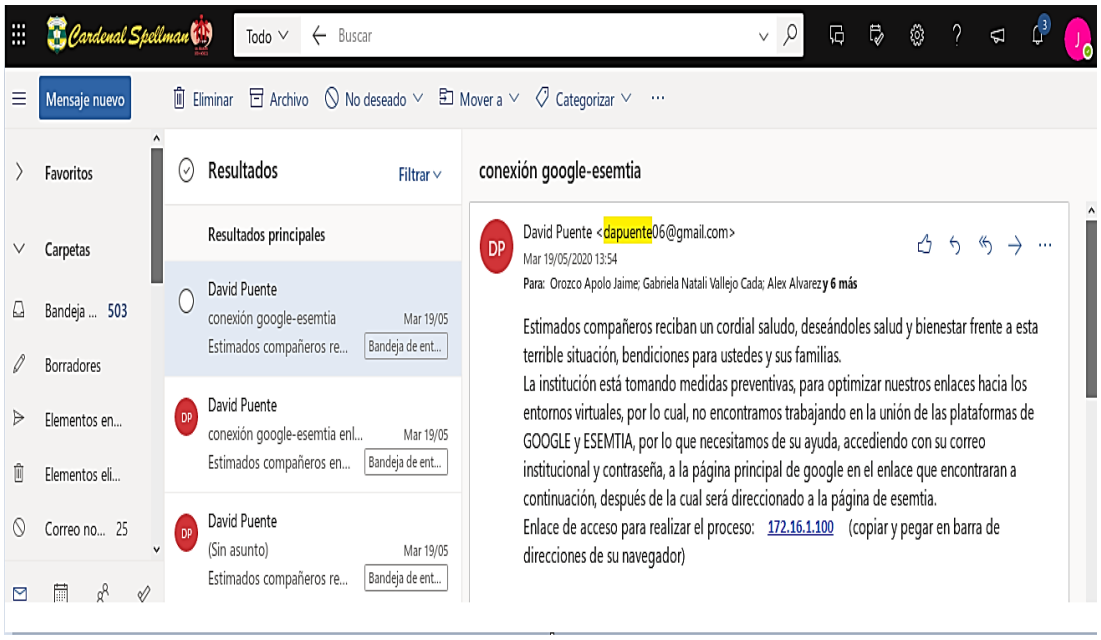


Figura 35. Bandeja de entrada cuarta víctima, evidenciando el correo recibido en la plataforma Office 365.
Elaborado por: Los autores, a través de la plataforma Office 365.

3.1.3. Escenario 2 – Spoofing – Pretexting

Para el desarrollo de este escenario, se aplicó la técnica de Spoofing, utilizando el correo institucional como medio de propagación, con la ayuda de Google Forms, que se encargó de recolectar los datos, además se utilizó la técnica de Pretexting con la plataforma de mensajería instantánea WhatsApp.

3.1.3.1. Identificación de víctimas

Se aplicó el ataque a 54 docentes, a los cuales se les envió el mensaje a través del correo electrónico institucional y a 25 docentes se les envió el mensaje a través de WhatsApp, en algunos casos, a varios docentes les llegó el mensaje por ambos medios.

Se le notificó al cuerpo de docentes acerca de capacitaciones virtuales gratuitas, para lo cual debieron entrar al enlace adjunto, que los dirigió hacia el formulario de Google, en el cual se le solicitó información personal para realizar su registro.

Direcciones de correo electrónico.

Figura 36. Direcciones de correo del personal docente de la UESCS en la plataforma Gmail.
Elaborado por: Los autores, a través de la plataforma Gmail.

3.1.3.2. Desarrollo del escenario

Para la creación del escenario, en primer lugar, se creó una cuenta de correo ficticia, con usuario autoeducationec@gmail.com, que simula ser una empresa de capacitaciones asociada a un centro universitario ficticio, la finalidad de que se asemeje a una cuenta real, es para ganar la confianza de los usuarios.

De misma manera se creó un perfil de WhatsApp, con una imagen y nombre del centro universitario ficticio que permita ser lo más creíble posible.

Perfil WhatsApp

Figura 37. Perfil ficticio en WhatsApp, con el que se enviaran los mensajes.
Elaborado por: Los autores, a través de la plataforma WhatsApp.

Para la creación del mensaje se tomaron en cuenta algunos aspectos, como el logotipo de la universidad ficticia, que los cursos ofrecidos sean reales, pero sobre todo que las capacitaciones son gratuitas.

Cuerpo del correo electrónico.

Figura 38. Correo enviado a las víctimas a través de la plataforma Gmail.
Elaborado por: Los autores, a través de la plataforma Gmail.

Mensaje enviado por WhatsApp.

Figura 39. Mensaje enviado a las víctimas a través de la plataforma WhatsApp.
Elaborado por: Los autores, a través de la plataforma WhatsApp.

Además, utilizando la plataforma Google Forms, se desarrolló el formulario en el cual se le solicitó a la víctima que ingrese su información personal para realizar su supuesta inscripción en las capacitaciones.

Formulario de registro

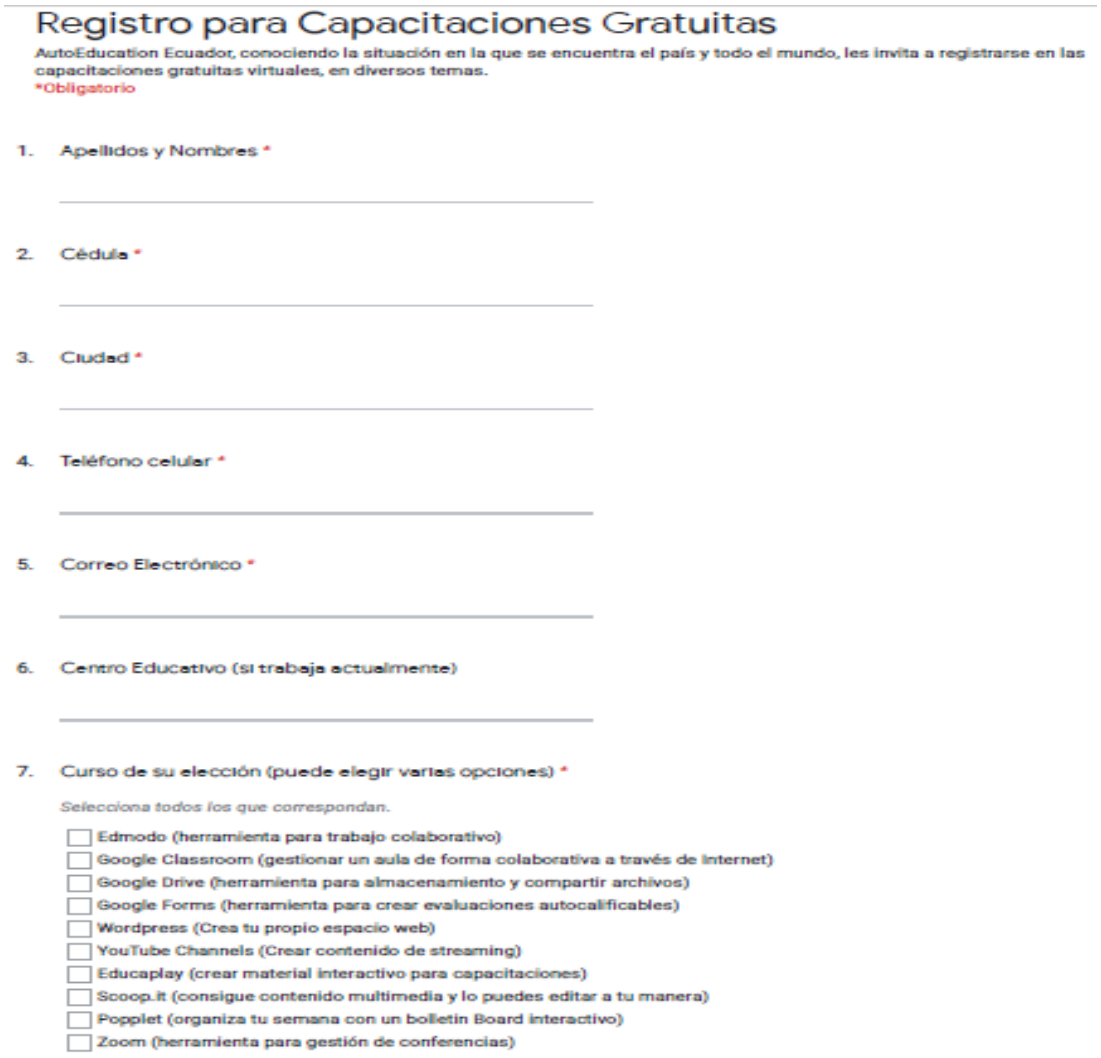


Figura 40. Formulario de registro a las capacitaciones gratuitas en la plataforma Google Forms.
Elaborado por: Los autores, a través de la plataforma Google Forms.

En el formulario se les solicitó a los empleados, que ingresen sus nombres y apellidos, cédula de identidad, ciudad, correo electrónico, centro educativo en el que trabaja y que escojan que capacitaciones le interesa.

3.1.3.3. Entrega del escenario

Para la entrega del enlace al formulario, se utilizó tanto el correo electrónico como mensajes a través de WhatsApp.

El texto del mensaje fue lo más auténtico posible para crear una atmósfera de confianza.

3.1.3.4. Resultados

Para realizar la recopilación de información, es cuestión de dejar abierto el formulario para que las personas que accedan a través del enlace y comiencen a llenar los campos, la tabla 10 muestra la información de los empleados que entraron al enlace e ingresaron sus credenciales.

Tabla 10.
Información obtenida a través de Google Forms.

Apellidos y Nombres	Cédula	Ciudad	Teléfono	Correo electrónico
APU[redacted]NDO	17[redacted]7	QUITO	97[redacted]4	a[redacted]@hotmail.com
Guz[redacted]ndra	17[redacted]3	Quito	99[redacted]0	dori[redacted]ucero@gmail.com
COLOM[redacted] NOEMÍ	17[redacted]5	Quito	98[redacted]9	sc[redacted]pellman.edu.ec
Cab[redacted]mar	17[redacted]2	Quito	99[redacted]3	pr[redacted]@hotmail.com
GALLEGO[redacted] MARLENE	17[redacted]0	Quito	99[redacted]9	vg[redacted]pellman.edu.ec
[redacted]	17[redacted]8	Quito	99[redacted]9	fc[redacted]pellman.edu.ec
Agu[redacted]mela	17[redacted]1	Quito	99[redacted]3	k[redacted]pellman.edu.ec
Morale[redacted]xandra	17[redacted]8	Quito	99[redacted]7	A[redacted]es@hotmail.es
[redacted]	17[redacted]0	Quito	99[redacted]6	Carm[redacted]guilar@gmail.com
DÁVILA [redacted]EXANDRA	17[redacted]9	QUITO	98[redacted]8	srta.va[redacted]ndra@hotmail.com
P[redacted]rto	17[redacted]3	Quito	99[redacted]1	jos[redacted]o@hotmail.com
[redacted]	18[redacted]7	Quito	99[redacted]1	sar[redacted]dav@gmail.com
[redacted]	17[redacted]7	Quito	99[redacted]4	a[redacted]@hotmail.com
ANDR[redacted]ARIAS	17[redacted]7	QUITO	98[redacted]0	and[redacted]azuri@gmail.com
Ta[redacted]ián	17[redacted]7	Quito	99[redacted]1	ata[redacted]spellman.edu.ec
Ta[redacted]ián	17[redacted]7	Quito	99[redacted]1	ata[redacted]spellman.edu.ec
PICHU[redacted]DRIGO	17[redacted]9	QUITO	98[redacted]8	pp[redacted]spelman.edu.ec
PICHU[redacted]DRIGO	17[redacted]9	QUITO	98[redacted]8	ppi[redacted]spellman.edu.ec

Nota: Por cuestiones de seguridad no se muestran la información completa.
Elaborado por: Los autores, a partir de la información recogida de Google Forms.

Para proporcionar evidencias, se seleccionó una cédula de identidad al azar, para conocer hasta qué punto se podría conocer más información acerca de la persona.

Se quiere conocer la dirección de domicilio de la víctima, para eso se procede a consultar, por el medio de la plataforma de avalúos del municipio, para conocer si tiene alguna propiedad registrada.

Consulta de avalúos en el Municipio.

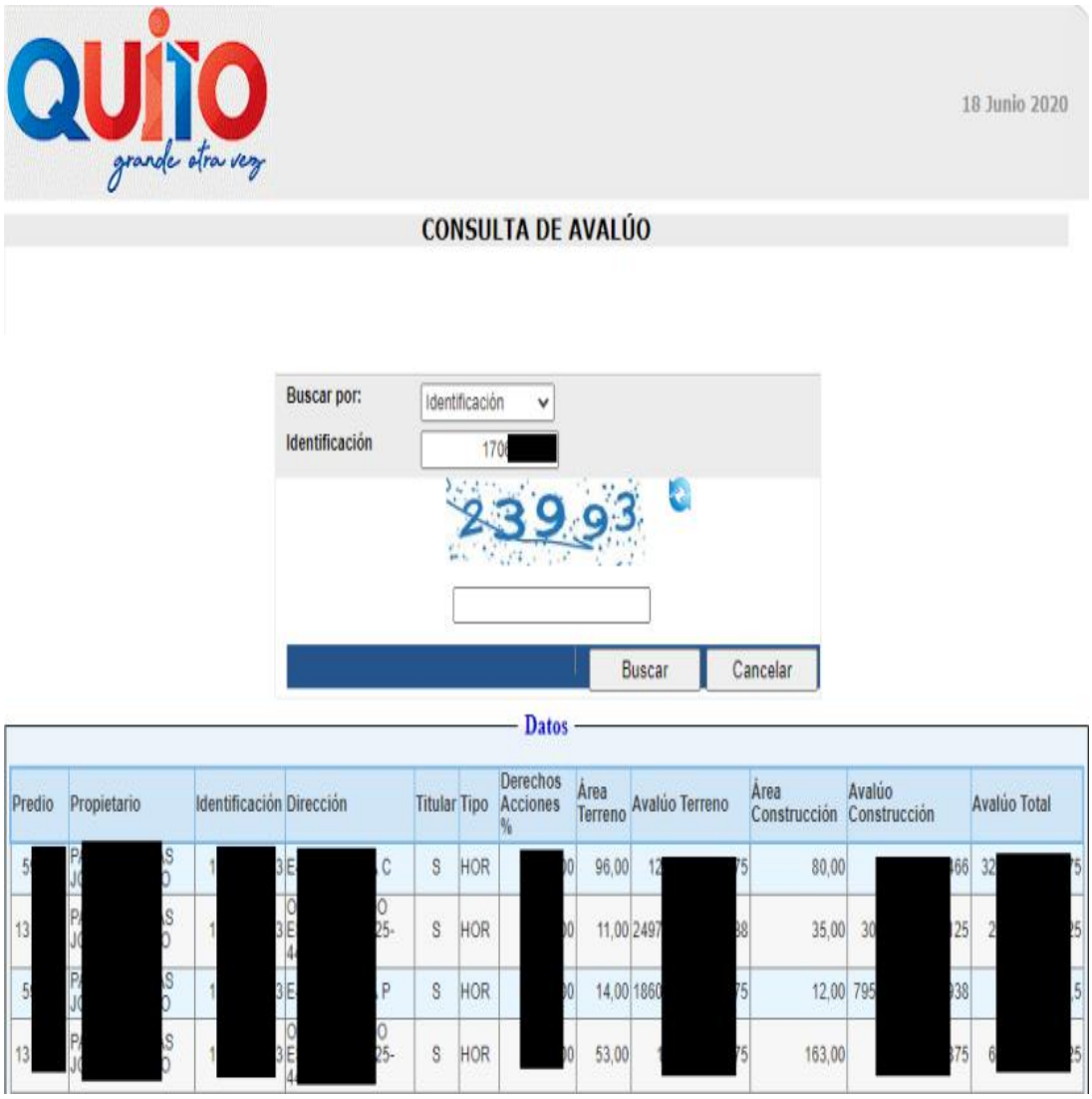


Figura 41. Información de avalúos de la víctima en la plataforma del municipio de Quito.
Elaborado por: Los autores, a través de la plataforma de avalúos del municipio de Quito.

En la figura 41, la cédula ingresada muestra que, si existen propiedades registradas, ahora tomando el número de predio, se consulta, la dirección en la que se encuentra.

Para realizar la consulta de la dirección, se debe acceder a la página de informe de regulación metropolitana, donde se ingresó el número de predio.

Consulta de información de predio.

Figura 42. Consulta del IRM de la víctima en la plataforma de predios del municipio de Quito.
Elaborado por: Los autores, a través de la plataforma de predios del municipio de Quito.

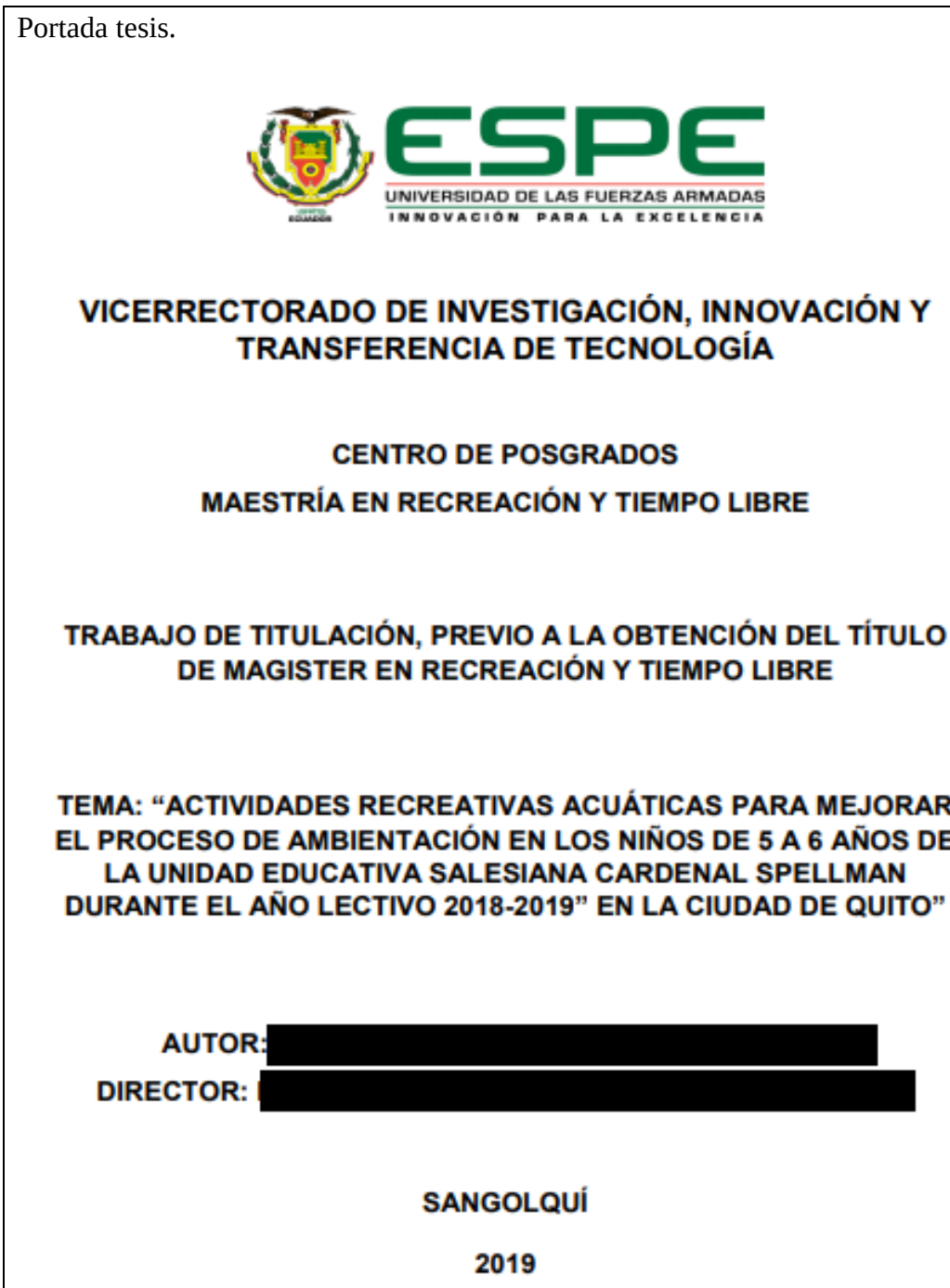
En la figura 42, se ingresó el número de predio, como resultado la página muestra la dirección exacta de la víctima, con un croquis del predio.

Resultado.

Figura 43. Información de la víctima, dirección y croquis en la plataforma de predios del municipio de Quito.
Elaborado por: Los autores, a través de la de plataforma de predios del municipio de Quito.

Para obtener más evidencia, se tomaron los nombres, apellidos y número de cédula de otra víctima, se ingresó esta información en el buscador, el cual devolvió como resultado, el documento del proyecto final para la obtención del título universitario.

Portada tesis.



ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y TRANSFERENCIA DE TECNOLOGÍA

CENTRO DE POSGRADOS

MAESTRÍA EN RECREACIÓN Y TIEMPO LIBRE

TRABAJO DE TITULACIÓN, PREVIO A LA OBTENCIÓN DEL TÍTULO DE MAGISTER EN RECREACIÓN Y TIEMPO LIBRE

TEMA: "ACTIVIDADES RECREATIVAS ACUÁTICAS PARA MEJORAR EL PROCESO DE AMBIENTACIÓN EN LOS NIÑOS DE 5 A 6 AÑOS DE LA UNIDAD EDUCATIVA SALESIANA CARDENAL SPELLMAN DURANTE EL AÑO LECTIVO 2018-2019" EN LA CIUDAD DE QUITO"

AUTOR: [redacted]

DIRECTOR: [redacted]

SANGOLQUÍ

2019

Figura 44. Portada de la tesis de la víctima encontrada en el repositorio digital dspace.
Elaborado por: Los autores, a partir del repositorio digital dspace.

En la página de autoría de responsabilidad, se encontró la firma de la víctima, la cual se podría escanear y utilizar para fines delictivos.

Página tesis.

UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y TRANSFERENCIA DE TECNOLOGÍA

CENTRO DE POSGRADOS

AUTORÍA DE RESPONSABILIDAD

YO, [redacted], con cedula de ciudadanía nº [redacted], declaro que el contenido, ideas y criterios del trabajo de titulación: "ACTIVIDADES RECREATIVAS ACUÁTICAS PARA MEJORAR EL PROCESO DE AMBIENTACIÓN EN LOS NIÑOS DE 5 A 6 AÑOS DE LA UNIDAD EDUCATIVA SALESIANA CARDENAL SPELLMAN DURANTE EL AÑO LECTIVO 2018-2019" EN LA CIUDAD DE QUITO" es de mi autoría y responsabilidad, cumpliendo con los requisitos teóricos, científicos, técnicos, metodológicos y legales establecidos por la Universidad de las Fuerzas Armadas ESPE, respetando los derechos intelectuales de terceros y referenciados las citas bibliográficas.

Consecuentemente el contenido de la investigación mencionada es veraz.

Sangolquí, Mayo 2019

Firma:
[redacted]

CI.[redacted]

Figura 45. Página de autoría tesis de la víctima en el repositorio digital dspace.
Elaborado por: Los autores, a partir del repositorio digital dspace.

Además, en la página de dedicatoria, se descubrió información familiar, como los nombres de los padres, hermanos y amigos, los cuales podrían ser utilizados como información para una estafa, amenazas y demás delitos.

Página tesis.

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y TRANSFERENCIA DE TECNOLOGÍA

DEDICATORIA

Mi tesis la dedico con todo mi amor y cariño a mis amados [redacted] por darme la energía, la motivación e inspiración suficiente de seguir prosperándome, por su sacrificio, esfuerzo y por creer en mí.

A mi hermano [redacted] que es mi motor a seguir, mi ejemplo de vida, que me enseña a no decaer y siempre seguir adelante, que me regaña pero siempre dice que me ama, a [redacted] que siempre están ahí para brindarnos un gran abrazo y un consejo.

A mi amiga Incondicional [redacted] por siempre estar en los momentos más difíciles, por darme un consejo, por regañarme y por brindarme su tiempo para jugar fútbol, hacer deporte y por salidas maniáticas que tenemos.

Figura 46. Página dedicatoria tesis de la víctima en el repositorio digital dspace.
Elaborado por: Los autores, a partir del repositorio digital dspace.

CAPÍTULO 4

En este capítulo se analizan los resultados obtenidos después de aplicar las pruebas a los empleados y las vulnerabilidades encontradas en la red, además de las medidas preventivas para no volver a ser víctima de la ingeniería social.

4.1. Resultado de los escenarios

4.1.1. Primer escenario

Gráfica circular de víctimas en el primer escenario.

$$x = \frac{4 * 100\%}{10} = 40\%$$

Figura 47. Porcentaje resultante de víctimas en el primer escenario.
Elaborado por: Los autores, a partir de los resultados obtenidos en el primer escenario.

Con los resultados obtenidos en el primer escenario, se evidenció que, de los 10 integrantes atacados del área administrativa con acceso a la red interna de la institución como se lo explica en él apartado 3.1.2.1., se obtuvo 4 credenciales (figuras 26 – 29), siendo esto el 40% de éxito de la prueba, con las cuales se pudo ingresar a la

plataforma de la institución, se encontró información personal y laboral, como se observa en las figuras 30 - 35.

4.1.2. Segundo escenario

Gráfica de barras de víctimas en el segundo escenario.

$$x = \frac{54*100}{100} = 29.6\% \qquad y = \frac{2*100}{25} = 8\%$$

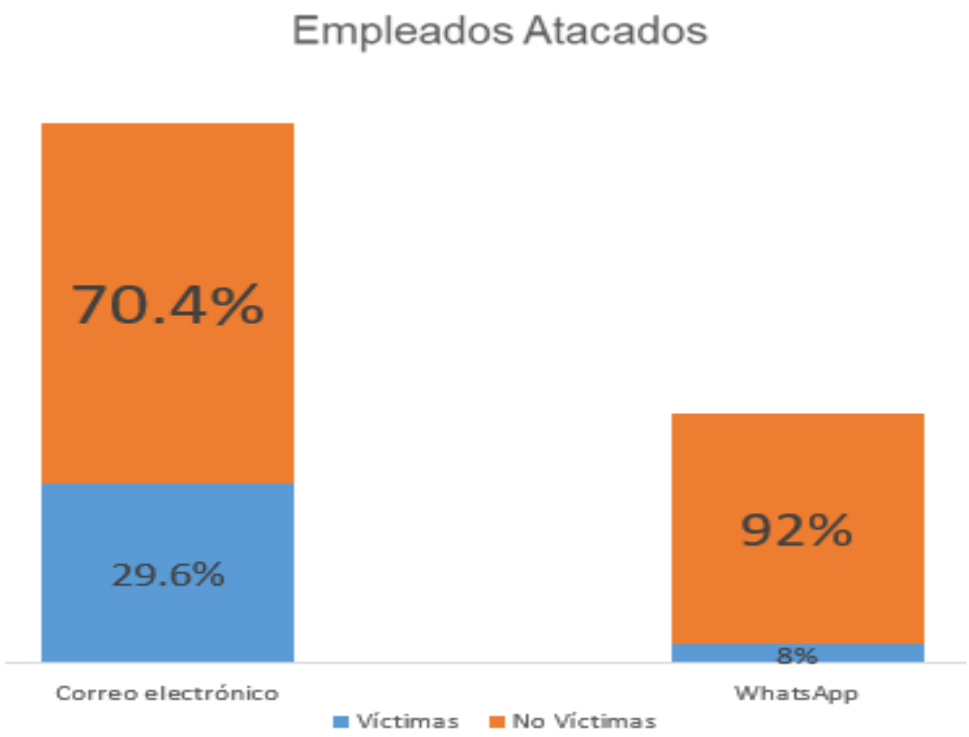


Figura 48. Porcentaje resultante de víctimas en el segundo escenario.
Elaborado por: Los autores, a partir de los resultados del segundo escenario.

A diferencia del primer escenario, en este caso como vectores de contagio se utilizó tanto el correo electrónico de la institución y mensajes a través de WhatsApp como se observa en la figura 39, con los resultados obtenidos, se comprobó con los cálculos realizados, que se obtuvo un 29.6% de éxito al utilizar el correo electrónico, en comparación al 8% de éxito que se obtuvo a través de WhatsApp.

Con la información recolectada mostrada en la tabla 10, se logró obtener información sobre que hacen, su información laboral y familiar, además de su lugar de residencia, como se puede evidenciar en las figuras 41 – 46.

La diferencia de éxito entre los dos vectores de contagio, se debe a la confianza que existe al recibir la información por medio de la plataforma de la institución, en comparación de recibir un mensaje de un número desconocido, cabe recalcar que el texto del mensaje en ambos casos es el mismo.

Con los resultados obtenidos en los dos escenarios, se elaboró la tabla 11 que muestra la vulnerabilidad a la que está expuesta seguridad de la red en relación a la confidencialidad, integridad y disponibilidad.

Tabla 11.
Vulneración de confidencialidad, integridad y disponibilidad.

Confidencialidad	Revelación de información confidencial y sensible de la institución.
Integridad	Cambio y eliminación de información en el sistema académico. Cambio y eliminación de información en el sistema financiero.
Disponibilidad	Ataques de denegación de servicios. Ataques de rescate de información (Wannacry).

Nota: La tabla muestra las vulnerabilidades de confidencialidad, integridad y disponibilidad, encontradas en la red de la UESCS, por parte de los usuarios.
Elaborado por: Los autores, a partir de los resultados obtenidos en las pruebas.

4.2. Vulnerabilidades encontradas en la red

Las vulnerabilidades presentadas en la tabla 11 y las falencias en los usuarios que se muestran en la tabla 5, elaboradas a partir de la información obtenida en la entrevista realizada al departamento de sistemas, exponen que las vulnerabilidades presentadas en la tabla 12 son las que más incidencia presentan en la seguridad de la red, y tienen un grado alto de exposición a un ciberataque.

Tabla 12.
Vulnerabilidades encontradas en la seguridad de la red de la UESCS.

Problema	Descripción	Solución	Relevancia
Medio de intercomunicación	Disminución de prestaciones de la red	Conexión directa de la fibra a los equipos mediante módulos SFP	Alto
Equipos	Velocidad de transferencia 100 Mbps	Renovar equipos que operan con velocidades de transferencia 10/100 La institución cuenta con un ancho de banda alto , y con estos equipos se lo está desperdiciando	Medio
Direccionamiento estático	Administración compleja	Se maneja pocos rangos de ips para la institución, Se manejan varias secciones y varios equipos, con poca administración.	Medio
Red plana	Bloque extenso de direcciones	No se cuenta con la división de áreas , para mayor administración y seguridad implementar una segmentación de Vlan	Alto
Seguridad	Equipos sin contraseña ni dirección para administración	Cambiar claves para acceso por consola, telnet y interfaz web Falta de educación a usuarios finales con respecto a la entrega de la información.	Alto

Nota: La tabla muestra las vulnerabilidades encontradas en la seguridad de la red de la UESCS.
Elaborado por: Los autores, a partir de los resultados obtenidos en las pruebas.

4.3. Medidas legales

Es necesario la implementación de un reglamento para la creación de políticas de seguridad de la información, para evitar que la red de la institución y sus elementos no sean víctimas de ciberataques, para conocer los procedimientos a seguir antes, durante y después de un ataque.

Estas políticas deben ser elaboradas junto con la institución y las acciones legales correspondientes.

4.4. Medidas preventivas

- La Institución debe dar continuamente capacitaciones, establecer un cronograma de las mismas para todo el año lectivo y para todo el personal de la institución, acerca de las últimas novedades y noticias de la seguridad informática y de la información, con el fin de cultivar una cultura de protección para la institución y para los usuarios y así se convertirán en aliados para la ciberseguridad del colegio.
- Se debe socializar que el papeleo que ya no vale y contienen información valiosa se lo destruir de una forma adecuada, ya que es una brecha de recolección fácil para gente maliciosa.
- Las contraseñas y claves de acceso deben ser cambiadas periódicamente, además se recomienda la utilización de firmas digitales, métodos de autentificación, técnicas criptográficas y de encriptación para la protección de información para garantizar la seguridad del usuario.
- Se debe definir límites y roles para los usuarios, ya sea por áreas, procesos o niveles, para tener un control de los datos los que puede acceder, por ejemplo:

a los datos estratégicos y confidenciales solo pueden acceder las autoridades de la institución.

- Proponer un E-learning, para optimizar tiempos y los usuarios puedan participar constantemente, creando una intranet con información relacionada con ciberseguridad de la organización, en donde también podrán interactuar con preguntas, dudas y sugerencias.
- Prohibir la utilización de unidades externas en los equipos de la institución para evitar el ingreso de malware; la nube se podría utilizar como alternativa de los dispositivos de almacenamiento.
- Se recomienda adoptar el estándar internacional ISO 27001, que permite la implementación de un sistema de gestión de seguridad de la información, cual proporciona la seguridad necesaria a la información sensible y confidencial.
- Realizar periódicamente ataques de ingeniería social para verificar el estado de la seguridad de la red y de los usuarios, así comprobar si los protocoles están funcionando, y establecer buenas prácticas de seguridad.
- Informar a los usuarios de no compartir datos fácilmente, para que después puedan ser usados para un ataque, ya que se pone en riesgo a la institución y a la persona, por lo que debe asegurarse de la fuente de donde le solicita dicha información, y si es el caso consultar con personas con más conocimiento en este caso será el departamento de Sistemas.
- La institución y sus usuarios deben mantener sus equipos siempre actualizados con sistemas operativos actuales, antivirus y con licencias originales, y así asegurar los equipos.
- Las contraseñas son el primer obstáculo de seguridad de los usuarios, para proteger su información, es por eso que la contraseña debe tener combinaciones

alfanuméricas, superior a 8 dígitos, agregar caracteres especiales como #$%&/, manejar diferentes contraseñas y usuarios para sistemas bancarios, correo electrónico y redes sociales, cambiar regularmente las contraseñas, no recordar las contraseñas en los navegadores, no guardar las contraseñas en lugares visibles y no escribirlas en ningún lado.

- Evitar los enlaces sospechosos, ya que estos son los más utilizados por los atacantes para dirigir a las víctimas a páginas maliciosas, por lo tanto, se debe evitar dar clic en estos, generalmente estos provienen a través de correo electrónico o servicios de mensajería instantánea.
- Revisar los remitentes en los correos electrónicos, ya que pueden tratarse de correos maliciosos, estos pueden llegar a la suplantación de la identidad del personal de la institución, con el único fin de recolectar información.
- Evitar proporcionar datos personales, usuarios, contraseñas en correos sospechosos o mensajes a través de servicios de mensajería instantánea.
- Se deberá restringir el acceso a todas las redes sociales y páginas que no se relaciones a la labor de los empleados, esto impedirá que delincuentes roben información privada de la institución médica o del personal.
- Se recomienda la implementación de políticas y procesos que permitan la correcta administración de la información de la institución.
- Nunca descargar software enviado por correo electrónico o páginas sospechosas, ya que se puede dar una brecha para el robo de información y ser víctimas de un ataque de ciberseguridad.
- Realizar siempre copias de seguridad de la información, configuraciones, ya sean manuales o automáticas, ya que los equipos siempre son vulnerables a un ataque y no se sabe cuándo podrían ser víctimas de uno de ellos.

- Al momento de detectar alguna amenaza se deberá informar de inmediato al departamento de sistemas, que procederá a su inmediata eliminación y a reconfigurar el dispositivo en caso de ser necesario.

CONCLUSIONES

- Con la información obtenida al analizar la entrevista realizada al personal del departamento de sistemas, se logró conocer el estado de la situación actual de la seguridad de la red de la UESCS, se observó que existen equipos con algún grado de obsolescencia, sin soporte de la marca y que necesitan un cambio a corto plazo, por lo que serían un riesgo de seguridad, como lo alerta la INCIBE.
- Como resultado de la investigación acerca de las herramientas y técnicas de ingeniería social, la herramienta Social-Engineering Toolkit (SET), fue usada para el desarrollo del primer escenario, para clonar una página web, con la cual se capturaron credenciales sensibles del personal administrativo para realizar un ataque de suplantación de identidad, para lo cual se evidenció una vulnerabilidad que existe en la organización, y ofreciendo una ayuda accesible a través de un enlace malicioso para que las víctimas ingresen sus credenciales institucionales. En el segundo escenario se utilizaron las técnicas de Phishing y Pretexting, con las cuales se capturaron datos personales privados de los docentes, que junto con redes sociales y servicios de Google se pudo conocer que hacen, su información familiar y hasta su lugar de residencia.
- Al redactar el mensaje con el cual se realizaron los ataques de Spoofing y Pretexting, se tomó en cuenta que, la información llame la atención de las víctimas, para lo cual, se debe crear un ambiente de confianza y credibilidad para no levantar sospechas, por la tanto, se consiguió el acceso a información personal y laboral de las víctimas.
- Desde el punto de vista legal es importante que la institución cuente con una política de seguridad hacia la red y sus usuarios, para prevenir ciberataques y gestionar su tratamiento en caso de ser víctima.

- Los resultados técnicos obtenidos en este trabajo de titulación, alertan la necesidad de tomar medidas preventivas y correctivas, por lo cual es importante fomentar medidas de protección establecidas por la institución y su departamento técnico, para mitigar estas vulnerabilidades encontradas.

RECOMENDACIONES

- Se recomienda realizar un análisis de riesgos de los activos de la información junto con un plan de contingencias, para formalizar la actuación frente a un incidente de seguridad.
- Se deben crear normas de seguridad que engloben todo lo referente a la ingeniería social, deben ser claras y apoyarse en las técnicas usadas por estos delincuentes.
- Se debe clasificar la información y mantener un control sobre qué usuarios tienen acceso a esa información dentro de la institución, para impedir que un reducido número de personas tengan acceso a toda la información y sea objetivo de un ataque.

GLOSARIO DE TÉRMINOS

Atacante: Se hacen pasar por otra persona y convencen a la víctima para entregar información sensible de la organización o sus contraseñas. (Rodríguez Rincón, 2018)

Ataque: Es un intento organizado e intencionado causado por una o más personas para ocasionar daño o problemas a un sistema informático o red. (Rodríguez Rincón, 2018)

E-learning: es un espacio virtual de aprendizaje orientado a facilitar la experiencia de capacitación a distancia, para instituciones educativas. (Samaniego, 2018)

Farming: es lo contrario al hunting, en este caso el objetivo es mantener el engaño el mayor tiempo posible, para exprimir al máximo el conocimiento, recursos o posición de la víctima. (Iglesias, 2017)

Firewall o cortafuego: Hardware o software de seguridad que impide el acceso de personas no autorizadas a una red interna desde el exterior (como puede ser Internet). (Espinosa, 2012)

Hacker: experto de programación, sistemas, redes en general, Internet, computadoras y no tiene intenciones malas a diferencia de lo que se escucha comúnmente. Le gusta acceder a lugares prohibidos por diversión, alimento de ego y demostrar que para él, los sistemas más costosos son vulnerables. (Espinosa, 2012)

Hardware: hace referencia a los aspectos físicos o materiales que conforman un sistema informático. (Haro & Parra, 2016)

Hunting: son aquellos ataques que buscan información específica del objetivo con la menor exposición posibles. (Iglesias, 2017)

Ingeniería social: técnicas y métodos utilizados para engañar a las personas y conseguir información valiéndose de su ignorancia e inocencia. (Espinosa, 2012)

Pretexting: se define como la práctica de presentarse como alguien más para obtener información privada. (Wilhelm, 2013)

Phishing: es una técnica de ingeniería social utilizada por los delincuentes para obtener información confidencial como nombres de usuario, contraseñas y detalles de tarjetas de crédito haciéndose pasar por una comunicación confiable y legítima. (Wilhelm, 2013)

Redes sociales: se refieren al conjunto de grupos, comunidades y organizaciones vinculados unos a otros a través de relaciones sociales. Esto fue el resultado de la convergencia de los medios, la economía política de los mismos y el desarrollo de tecnologías, teniendo como objetivo la interacción de dos o más canales. (Wikipedia, 2017)

Software: Hace referencia al conjunto de operaciones, procesos, instrucciones o algoritmos que determinado programa debe seguir para la ejecución de distintas tareas dentro de un computador. (Haro & Parra, 2016)

Vulnerabilidad: Debilidad del sistema informático que puede ser utilizada para causar un daño. Las debilidades pueden aparecer en cualquiera de los elementos de una computadora, tanto en el hardware, el sistema operativo, como en el software. (Rodríguez Rincón, 2018)

LISTA DE REFERENCIAS

Bibliografía

Astudillo, K. (2013). Hacking Etico 101: Como Hackear Profesionalmente En 21 Dias O Menos. Createspace Independent Pub.

Cordero, W. (2018). Implementación de técnicas de ingeniería social. Málaga, España.

García, C. (2017). Mucho hacker: Más allá de los héroes informáticos o de los delincuentes de la red. Intermedio Editores S.A.S.

Huerta, D. (2010). Ingeniería Social. Córdoba: Cristian Borghello.

Mitnick, K. (2001). The Art of Deception. Hoboken : John Wiley & Sons.

Imágenes

Martin, L. (s.f.). Lockheed Martin. Obtenido de https://www.lockheedmartin.com/en-us/capabilities/cyber.html

Normas

ISO. (2005). ISO/IEC 27001. Ginebra: ISO.

Sitios Web

Axis. (s.f.). NORBAIN. Obtenido de https://norbain.com/wp-content/uploads/2018/02/Axis_Cybersecurity_eBook-1.pdf

Brook, C. (5 de Diciembre de 2018). CyberSecurity Forum. Obtenido de https://cybersecurityforum.com/cybersecurity-faq/what-is-cyber-hygiene.html

Brook, C. (5 de Diciembre de 2018). Digital Guardian. Obtenido de https://digitalguardian.com/blog/what-cyber-hygiene-definition-cyber-hygiene-benefits-best-practices-and-more

Cerf, V. (23 de Febrero de 2000). UNITED STATES CONGRESS. Obtenido de https://www.jec.senate.gov/archive/Documents/Hearings/cerf22300.htm

Ciberseguridad. (13 de Agosto de 2019). ¿Qué es la higiene cibernética y por qué es importante?. Obtenido de: https://ciberseguridad.com/guias/higiene-cibernetica/#:~:text=Cuanto%20mayor%20sea%20tu%20puntuaci%C3%B3n,personales%20y%20otras%20amenazas%20cibern%C3%A9ticas.

Digital, C. (2018). Cambio Digital. Obtenido de https://cambiodigital-ol.com/2018/12/que-es-la-cadena-de-ciberataque/

Emanuelli A., F. M. (2014). Hoja de Ruta de Proyectos Piloto. Obtenido de http://www.reddccadgiz.org/documentos/doc_843564181.pdf

Harley, D. (4 de Mayo de 2015). welivesecurity. Obtenido de https://www.welivesecurity.com/la-es/2015/05/04/evolucion-scams-ingenieria-social-david-harley/

Hospelhorn, S. (29 de Marzo de 2020). VARONIS. Obtenido de https://www.varonis.com/blog/cyber-kill-chain/

Iglesias, P. (13 de Junio de 2017). PabloYglesias. Obtenido de Los 6 principios básicos de la ingeniería social: https://www.pabloyglesias.com/mundohacker-ingenieria-social/

INCIBE. (s.f.). La importancia de las actualizaciones de seguridad. Obtenido de https://www.osi.es/es/actualizaciones-de-seguridad

Izquierdo, R. (9 de Marzo de 2018). EHORUS. Obtenido de https://ehorus.com/es/software-comercial/

Johnson, A. (3 de Enero de 2019). Resource Hacker. Obtenido de http://www.angusj.com/resourcehacker/

Lampert, T. (2017). Github. Obtenido de https://github.com/tiagorlampert/sAINT

Moreira, C. (s.f.). Centro Nacional de Información de Ciencias Médicas. Obtenido de https://instituciones.sld.cu/dnspminsap/files/2013/08/Metodologia-PSI-NUEVAProyecto.pdf

OffSec, L. S. (s.f.). Kali Tools. Obtenido de https://tools.kali.org/information-gathering/set

OSI. (s.f.). Oficina de seguridad del internauta. Obtenido de https://www.osi.es/es/actualizaciones-de-seguridad

PSI. (2010). Metodología de Desarrollo PSI. Obtenido de https://www.uarg.unpa.edu.ar/psi/

RSI, S. (20 de Diciembre de 2019). RSI Security . Obtenido de https://blog.rsisecurity.com/cyber-hygiene-a-complete-guide/

Samaniego, I. (2018). U-planner. Obtenido de https://www.u-planner.com/es/blog/que-es-una-plataforma-de-e-learning

Spellman. (2016). Contactos. Obtenido de https://www.spellman.edu.ec/index.php/contact-sidebar

Spellman. (2016). Estructura jerárquica. Obtenido de https://www.spellman.edu.ec/index.php/joomla-pages-2/organigrama

Spellman. (2016). Misión y Visión. Obtenido de https://www.spellman.edu.ec/index.php/joomla-pages-2/2016-11-28-17-09-06/mision-y-vision

Vidal, J. (30 de Mayo de 2009). ESCUELA POLITÉCNICA NACIONAL. Obtenido de https://es.slideshare.net/lpajaro/sistemas-de-cableado-rutas-y-espacios

Wikipedia. (18 de Octubre de 2017). Wikipedia. Obtenido de https://es.wikipedia.org/wiki/Redes_sociales_en_Internet

Wilhelm, T. (2013). Professional Penetration Testing. Nueva York: Elsevier. Obtenido de Professional Penetration Testing: https://www.social-engineer.org/framework/influencing-others/pretexting/

Tesis

Catota, F. (2010). Análisis de la regulación del riesgo de las tecnologías de la información en el ámbito financiero ecuatoriano (tesis de pregrado). Escuela Politécnica Nacional, Quito, Ecuador.

Espinosa, A. (2012). Ingeniería social y sus niveles de incidencia en la UTPL (tesis de pregrado). Universidad Técnica Particular de Loja, Loja, Ecuador.

Haro, M., & Parra, P. (2016). Aplicación de herramientas de ethical hacking, caso de estudio "Empresa GAPSYSTEM" (tesis de pregrado). Pontificia Universidad Católica del Ecuador, Quito, Ecuador.

Hinojosa, L. (2010). 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 (tesis de pregrado). Universidad Internacional SEK, Quito, Ecuador.

Rodríguez, E. (2018). Metodologías de Ingeniería Social (tesis de maestría). Univesidad Oberta de Catalunya, Catalunya, España.

ANEXOS

Tabla 13.
Equipos usados en la red de la UESCS.

Equipo	Marca	Características	Cantidad
Switch 5120	HP	Switch capa 2/3/4 48 puertos 10/100/1000, 4 puertos SFP GE Capacidad de conmutación 192Gbps Arquitectura Non Blocking	1
Switch A5500	HP	Switch capa 2/3/4 24 puertos GE SFP, 8 puertos 10/100/1000	1
Switch 2530	HP	Switch capa 2 24 puertos 10/100/1000, 2 puertos SFP Capacidad de conmutación 136Gbps	3
Switch 2920	HP	Switch capa 2/3 48 puertos 10/100/1000, 2 puertos SFP Capacidad de conmutación 176Gbps	1
Switch 5500-EI	3COM	24 puertos 10/100 4 puertos SFP GE	3
Switch 4210	3COM	Switch L2 48 puertos 10/100, 2 puertos SFP GE	4
Switch 4210	3COM	Switch L2 28 puertos 10/100, 2 puertos SFP GE	
Switch 4500	3COM	Switch L2, L3 24 puertos 10/100, 2 puertos SFP GE	1
Fortigate 200D	Fortinet	Firewall, proxy, DNS, VPN ,2 DMZ, 2 enlaces WAN	1
Switch CRS125	Mikrotik	Switch L2, L3 24 puertos 10/100/1000, 2 puertos SFP GE	2
Unifi AP	Unifi	Access Point UAP 2.4 Ghz.	15
All in One 520	Lenovo	Equipos Escritorio i5 8va. Gen. 4 Gb. RAM Disco duro 1 Tb.	198
V310	Lenovo	Equipos Portátiles i5 6ta. Gen. 4 Gb. RAM Disco duro 1 Tb.	98
		Total	328

Nota: La tabla muestra la información completa de los equipos de la UESCS.
Elaborado por: Los autores, a partir de la entrevista al departamento de sistemas de la UESCS.

Entrevista al departamento de sistemas de la UESCS

Fecha: 12 de febrero del 2020

Nombre del entrevistado: David Puente

Objetivo: Conocer el estado actual de la seguridad de la red de la UESCS.

1. ¿Cómo está estructurada la red de la UESCS?

   Tiene una infraestructura sólida, y brinda varios servicios, para que el trabajo de sus usuarios sea lo más eficiente posible, en donde los usuarios intercambian, procesan y conservan información

2. ¿Cuáles son los servicios que brinda el departamento de sistemas?

   Navegación Web, almacenamiento de documentos y archivos (NAS), plataforma institucional educativa Esemtia, correo Institucional Office365, sistema contable, antivirus, administración y seguridad, paquete Office 365 en línea.

3. ¿En qué estado se encuentran los equipos de la UESCS?

   Los equipos de escritorio y portátiles que se encuentran en la UESCS, en su gran mayoría han cumplido su vida útil, pero se los ha tratado de mantener para que sigan cumpliendo su trabajo con un mantenimientos preventivos y correctivos.

   Existen maquinas aun con Windows 7, esto lo hacemos porque las maquinas ya no soportan una versión más fuerte de Windows.

4. ¿Cuáles son los problemas con respecto al hardware de la red de la UESCS?

   Existe un alto grado de obsolescencia con respecto a los enrutadores y conmutadores, los cuales ya no cuentan con soporte de fábrica, esto da como resultado un desperdicio de ancho de banda, ya no cuentan con actualizaciones oficiales

5. ¿Cómo está diseñada la red de la UESCS?

   La UESCS maneja una topología tipo estrella, con un equipo frontera Fortinet como principal y un switch capa 3 HP, estos son los encargados de la comunicación entre edificios, dentro de los cuales se localizan los enlaces de fibra óptica.

6. ¿Qué herramientas de software se usan en la UESCS?

   Sistema Contable, Active Directory, sistema biométrico, office365, plataforma educativa ESEMTIA, correo institucional.

7. ¿Qué sistemas operativos utilizan en la UESCS?

   En equipos de escritorio se utiliza Windows 7 y 10, esto es según las condiciones de los equipos se elige el sistema operativo, con sus respectivas licencias.

   Laptops se utiliza Windows 10

   Servidores se usa Windows server 2012

8. ¿Existen restricciones a la hora de usar alguna herramienta o algún software?

   La verdad no se tienen ninguna restricción se utiliza las herramientas o software según requerimientos de la red, de las autoridades o de los administradores si ellos lo ven necesario.

9. ¿Existen problemas con el software que usan en la UESCS?

   Existen varios problemas, pero los que se pueden resaltar son: exposición de contraseñas, falta de actualizaciones y parches de seguridad, instalación/desinstalación no controlada, instalación de programas maliciosos, falta de manuales y documentación, falta de control de versiones y pruebas.

10. ¿La UESCS trabaja con algún tipo de estándar de seguridad de la información?

    No, con ningún tipo de estándar.

11. ¿La UESCS maneja políticas de seguridad de la información?

Con políticas específicamente no se trabaja, ya que no se las tiene, y es por eso que no existe un documento legalmente aprobado y formalmente comunicado sobre políticas de seguridad de la información.

12. ¿La UESCS maneja procesos para la clasificación de la información?

    No, la UESCS no maneja procesos para la clasificación de la información, lo único que se tiene es el servidor NAS en donde se archiva la información por áreas, ya sea la contable, secretarias, y de la administración, y los usuarios son los encargados de realizarla.

13. ¿Cuáles son los procesos que se llevan a cabo para el control de la seguridad en la red de la UESCS?

    No existe un proceso de control de seguridad, los administradores de red lo único que hacemos es de tratar de cuidar la seguridad desde el equipo firewall, con procesos y configuraciones dentro del mismo equipo, para los usuarios se trata de controlar la seguridad con antivirus que también cuenta con su licencia.

    Pero no se cuenta con un proceso definido dentro de la institución.

14. ¿Cuáles son los problemas que existen en la forma de cómo se manipula la información?

    Los usuarios no tienen una cultura para el manejo de la información, en otros casos es falta de conocimiento, lo único que ahora hacen es guardar y archivar en el servidor NAS y en un archivo físico.

15. Con respecto a los usuarios, ¿Cuáles son los problemas que existen?

    Como con toda institución, existen varios problemas con los usuarios, existen una falta de conciencia de seguridad, falta de capacitaciones, así como de políticas, normas y procedimientos. El uso de contraseñas sin una robustez considerable, una inadecuada gestión y protección de las contraseñas, falta de información sobre seguridad, falta de documentación interna.

Existe un grupo de usuarios que ya son adultos mayores y no conocen nada sobre tecnología y menos el manejo de información, es por eso que para el departamento de sistemas es un reto en algunos casos poder crear una cultura informática.

16. Dentro de la UESCS, ¿Existen capacitaciones sobre el uso correcto de la red?

    Existen, pero esto se realiza una vez cada año lectivo, y son muy rápidas y básicas

17. ¿La UESCS, brinda capacitaciones sobre el manejo de la información?

    Se brinda capacitaciones únicamente cuando se implementa alguna herramienta, y es estrictamente sobre la misma.

18. ¿Cómo considera usted la forma en que actualmente se maneja la seguridad de la información?

    Como se dijo anteriormente no existe un manejo adecuado, es muy expuesta los usuarios por momentos hasta se olvidan de archivar en el servidor, y eso ocasiona muchos problemas ya que después existe perdida o modificación de la información

19. ¿Cuáles son los riesgos que usted cree que está expuesta la red de la UESCS?

    En realidad, existen varios riesgos a los que se encuentra expuesta la red, pero en general se pueden exponer los siguientes: los errores humanos, la suplantación de identidad, virus, puertas traseras, acceso no autorizado catástrofes naturales, incendios, accidentes, etc., además de los ataques de denegación, códigos maliciosos, ataques de intrusión, etc.

    Aunque los administradores de red, nos cuidamos de estas amenazas, siempre somos vulnerables para estos tipos de ataques, es por eso que se trata de proteger la red con los recursos que se tiene, hasta la fecha desde el día que nos hicimos cargo de la red nunca hemos tenido amenazas de ser atacados.

Tabla 14.
Configuración Firewall Servicios Temporales

FG200D_Spellman (policy)	
Habilitar software Cambridge name "Ef reverso" srcintf "port3" dstintf "wan2" srcaddr "EF server 1" "EF server 2" "Laboratorios_policy" dstaddr "all" learning-mode enable status disable schedule "always" service "ALL" fsso disable comments "Cambridge_certifications"	Habilitar Servidor NAS red interna y externa name "NAS" srcintf "wan2" "wan1" dstintf "port2" srcaddr "all" dstaddr "PN3T DVR" "NAS_1" "PN3T NAS_1" action accept schedule "always" service "ALL" logtraffic all
Habilitar Puerto 25 Colecturía name "Permitir puerto 25" srcintf "port2" dstintf "wan2" srcaddr "Colexxxx" dstaddr "all" action accept schedule "always" service "SMTP" logtraffic disable fsso disable comments "mail_server" nat enable	Bloquear Puerto 25 para la red interna name "block port 25" srcintf "any" dstintf "wan2" srcaddr "all" dstaddr "all" schedule "always" service "SMTP" logtraffic disable fsso disable next
Habilitar Active Directory laboratorios name "ACtive_lab" srcintf "port3" dstintf "port2" srcaddr "all" dstaddr "all" action accept schedule "always" service "ALL" fsso disable next	Habilitar Active Directory laboratorios name ">Active lab reverse" srcintf "port2" dstintf "port3" srcaddr "all" dstaddr "all" action accept schedule "always" service "ALL" fsso disable next

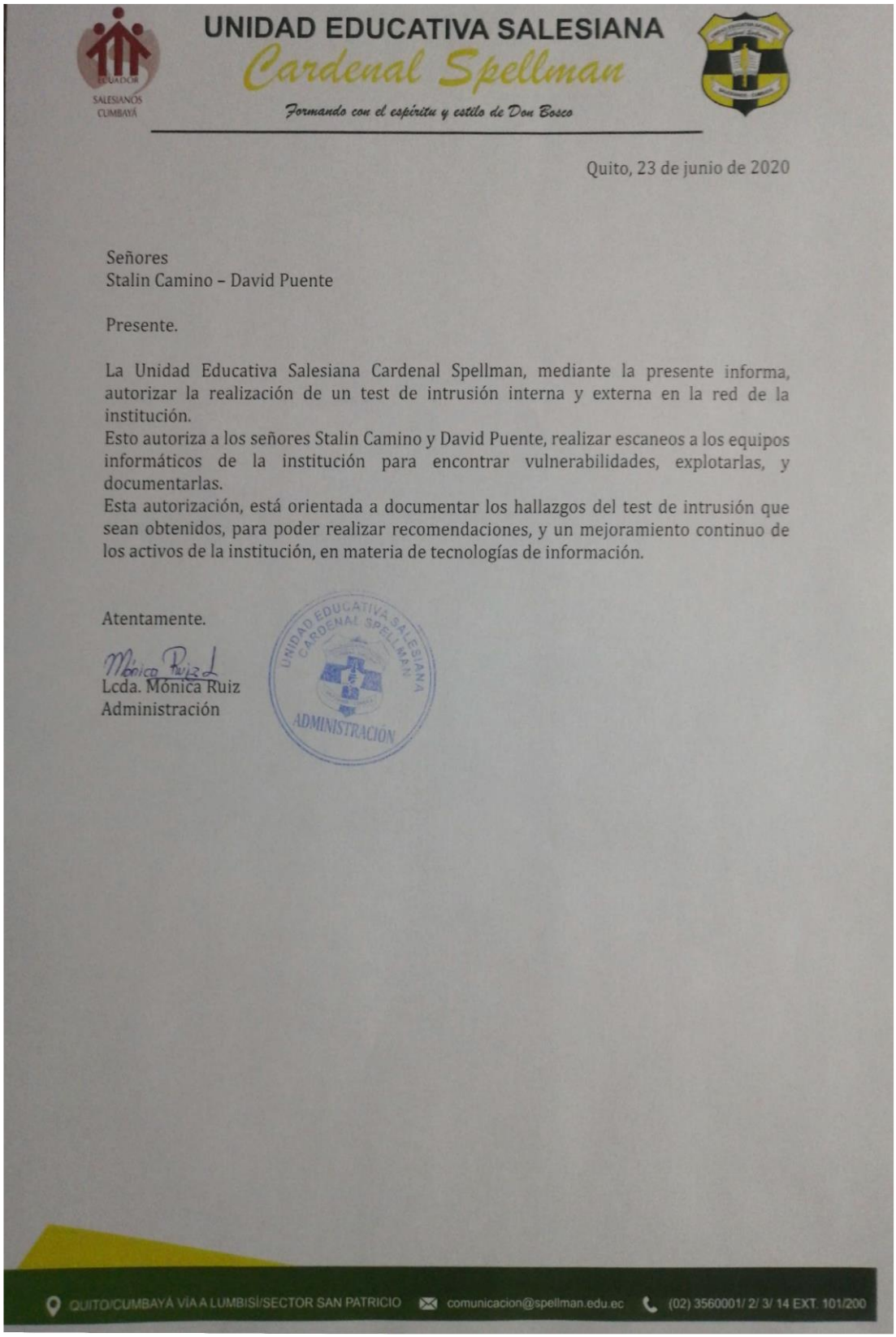
Habilitación antena WIFI name "acceso rucku" srcintf "port2" dstintf "port16" srcaddr "Alxx_Sistemas" dstaddr "all" action accept schedule "always" service "ALL" utm-status enable logtraffic all fsso disable av-profile "default" webfilter-profile "Docentes" dnsfilter-profile "botnets" application-list "Doc_layer7" ssl-ssh-profile "certificate-inspection" nat enable next	Habilitar conexión cámaras Seguridad-NAS name "Bypass" srcintf "port2" "port5" "port14" "port3" dstintf "wan2" "wan1" srcaddr "Lista" "NAS" "cámaras test" dstaddr "all" action accept schedule "always" service "ALL" logtraffic all fsso disable nat enable next
Habilitar WEB docentes name "Docentes" srcintf "port5" dstintf "wan2" srcaddr "all" dstaddr "all" action accept schedule "always" service "ALL" utm-status enable fsso disable av-profile "default" webfilter-profile "Docentes" application-list "Doc_layer7" ssl-ssh-profile "certificate-inspection" nat enable next	Habiltar equipos Wireless name "Unifi-Wireless" srcintf "port14" dstintf "wan2" srcaddr "all" dstaddr "all" action accept schedule "always" service "ALL" utm-status enable logtraffic all fsso disable av-profile "default" webfilter-profile "Docentes" dnsfilter-profile "botnets" application-list "Doc_layer7" ssl-ssh-profile "certificate-inspection" nat enable next

Habilitar acceso total a la red administrativos name "Administrativos" srcintf "port2" dstintf "wan2" "wan1" srcaddr "all" dstaddr "all" action accept schedule "always" service "ALL" utm-status enable logtraffic all fsso disable av-profile "default" webfilter-profile "global_temp" dnsfilter-profile "botnets" application-list "Adm_layer_7" ssl-ssh-profile "certificate-inspection" nat enable next	Habilitar red docentes laboratorios name "Lab docente" uuid 14e1abf0-9100-51e9-d0ab-3c2fb0ab3f5e srcintf "port3" dstintf "wan2" srcaddr "Lab docente" dstaddr "all" action accept schedule "always" service "ALL" utm-status enable fsso disable webfilter-profile "Docentes" dnsfilter-profile "botnets" application-list "Doc_layer7" ssl-ssh-profile "certificate-inspection" nat enable next
Habilitación antena WIFI name "Ruckus 2" srcintf "port16" dstintf "wan2" "wan1" srcaddr "all" dstaddr "all" action accept schedule "always" service "Web Access" utm-status enable logtraffic all fsso disable av-profile "default" webfilter-profile "Docentes" dnsfilter-profile "botnets" application-list "Doc_layer7" ssl-ssh-profile "certificate-inspection" nat enable next	Acceso total a la red Departamento Sistemas name "Control" srcintf "port2" dstintf "any" srcaddr "Alxx_Sistemas" "Daxx_Sistemas" dstaddr "all" action accept schedule "always" service "ALL" fsso disable next

Habilitar consola wireless name "Unifi administración" uuid 9ad5533c-ad27-51e8-186b-f80c373832fc srcintf "any" dstintf "port2" srcaddr "Unifi Adoption list" dstaddr "Alxx_Sistemas" "Daxx_Sistemas" action accept schedule "always" service "ALL" fsso disable next	Habilitación VPN name "VPN" srcintf "ssl.root" dstintf "port2" srcaddr "all" dstaddr "all" action accept schedule "always" service "ALL" users "****" nat enable next
Habilitación VPN name "VPN INTER" uuid 38a72c36-692c-51ea-ebb3-6256d5f38077 srcintf "ssl.root" dstintf "wan2" srcaddr "SSLVPN_TUNNEL_ADDR1" dstaddr "all" action accept schedule "always" service "ALL" users "****" comments "reverse" nat enable	

Nota: la tabla muestra las configuraciones de los servicios temporales de la red de la UESCS.
Elaborado por: Los autores, a partir de la entrevista al departamento de sistemas de las UESCS.

Carta de autorización pentesting.



UNIDAD EDUCATIVA SALESIANA
Cardenal Spellman
Formando con el espíritu y estilo de Don Bosco

Quito, 23 de junio de 2020

Señores
Stalin Camino – David Puente

Presente.

La Unidad Educativa Salesiana Cardenal Spellman, mediante la presente informa, autorizar la realización de un test de intrusión interna y externa en la red de la institución.
Esto autoriza a los señores Stalin Camino y David Puente, realizar escaneos a los equipos informáticos de la institución para encontrar vulnerabilidades, explotarlas, y documentarlas.
Esta autorización, está orientada a documentar los hallazgos del test de intrusión que sean obtenidos, para poder realizar recomendaciones, y un mejoramiento continuo de los activos de la institución, en materia de tecnologías de información.

Atentamente.

Lcda. Mónica Ruiz
Administración

UNIDAD EDUCATIVA SALESIANA CARDENAL SPELLMAN
ADMINISTRACIÓN

QUITO/CUMBAYÁ VÍA A LUMBISÍ/SECTOR SAN PATRICIO comunicacion@spellman.edu.ec (02) 3560001/ 2/ 3/ 14 EXT. 101/200

Figura 49. Carta de autorización para realizar una prueba de penetración a la red de la UESCS.
Elaborado por: Los autores.