UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA.

PROCESO DE TITULACIÓN

JUNIO 2023 – OCTUBRE 2023

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA PRUEBA PRÁCTICA

PREVIO A LA OBTENCIÓN DEL TÍTULO DE:

INGENIERO EN SISTEMAS DE INFORMACIÓN

TEMA:

ANÁLISIS DE LOS DIFERENTES TIPOS DE ATAQUES CIBERNÉTICOS QUE SON UTILIZADOS A TRAVÉS DE LOS SMS

ESTUDIANTE:

KEYLA ARISA ALARCON TOMALA

TUTOR:

ING. NARCISA MARIA CRESPO TORRES

AÑO 2023

ÍNDICE

RESUMEN

En la actualidad, la tecnología avanza rápidamente, lo que ha llevado al aumento de ataques cibernéticos a través del SMS, lo que representa una amenaza para la seguridad de los usuarios y la pérdida de información empresarial.

En esta investigación sobre los ataques cibernéticos a través de los SMS, se manejará un enfoque metodológico que combina diversas técnicas de compilación y análisis de datos. El objetivo principal es analizar los diferentes tipos de ataques cibernéticos más comunes que utilice SMS comprender en profundidad los diferentes tipos de ataques cibernéticos y su impacto en la seguridad de los usuarios de mensajería SMS.

Este estudio de caso utilizará una investigación exploratoria y descriptiva. La investigación exploratoria ayudará a identificar los diferentes tipos de ataques cibernéticos, mientras que la investigación descriptiva suministrará una visión detallada de cada tipo de ataque y sus características. Se llevarán a cabo entrevistas con estudiantes graduados y profesionales donde se analizarán las posibles víctimas de ataques cibernéticos a través de SMS. Estas entrevistas ayudarán a obtener información cualitativa valiosa sobre las estrategias utilizadas por los atacantes y el impacto en las personas y las organizaciones.

Para abordar este problema, es crucial realizar un análisis de los diferentes tipos de ataques cibernéticos y educar a los usuarios sobre la seguridad de su información. El desarrollo de Internet ha revolucionado la forma en que se intercambia información en diversos sectores, y la seguridad en el ciberespacio es vital para proteger a los usuarios y activos de las organizaciones.

Palabras claves: Ataques cibernéticos, seguridad informática, mensaje de texto.

ABSTRACT

Today, technology is advancing rapidly, which has led to the increase in cyber attacks through SMS, posing a threat to user security and loss of business information.

In this research on cyber attacks through SMS, a methodological approach will be used that combines various data compilation and analysis techniques. The main objective is to analyze the different types of most common cyber attacks that SMS uses to understand in depth the different types of cyber attacks and their impact on the security of SMS messaging users.

This case study will use exploratory and descriptive research. Exploratory research will help identify the different types of cyber attacks, while descriptive research will provide a detailed view of each type of attack and its characteristics. Interviews will be carried out with graduate students and professionals where possible victims of cyber attacks via SMS will be analyzed. These interviews will help obtain valuable qualitative information about the strategies used by attackers and the impact on people and organizations.

To address this issue, it is crucial to conduct an analysis of the different types of cyber attacks and educate users about the security of their information. The development of the Internet has revolutionized the way information is exchanged in various sectors, and security in cyberspace is vital to protect users and organizational assets.

Keywords: Cyber attacks, computer security, text message.

PLANTEAMIENTO DEL PROBLEMA.

En la actualidad, la tecnología avanza cada días más, donde se desarrollan nuevos dispositivos y el aumento alarmante de ataques cibernéticos a través del SMS, tomado lugar como el principal a las amenazas a la seguridad de la información en la actualidad en Ecuador, estos ataques son cada vez más frecuentes, y simbolizan un riesgo significativo para los usuarios mostrando inseguridad, pérdidas de información en las empresas, las organizaciones gubernamentales, y la vulnerabilidad en sus dispositivos móviles debido a la cantidad de SMS que recibe.

El aprendizaje sobre ciberseguridad en Ecuador es aún insuficiente, muchas personas no son consecuentes de los riesgos de los ataques cibernéticos a través de SMS, y no saben cómo protegerse de ellos. Sin embargo, existen diferentes tipos de herramientas que cumplen las funciones de enviar SMS maliciosos a los usuarios, provocando daño a los dispositivos móviles en la resistencia del sistema, retraso en el procesamiento e interrupción del funcionamiento normal de los dispositivos móviles.

En el Ecuador los ataques cibernéticos a través de los SMS representan una serie de problemas que amenazan la seguridad de los usuarios y la integridad de las empresas, es decir, suplantan las identidades para obtener la información personal, afecta el lado financiero que son recibidos a través de los SMS y falta de conocimientos de los usuarios los hace vulnerables al mundo de la tecnología.

Además, los atacantes invisibles (los emisores) son los que envían mensajes de texto engañosos que alientan al destinatario (los receptores) a tomar medidas, como hacer clic en un enlace o llamar a un número de teléfono.

Los mensajes pueden contener enlaces o archivos adjuntos maliciosos que, cuando se abren o descargan, infectan el dispositivo móvil del destinatario como: robando información, controlan el dispositivo o realizan actividades astutas sin el conocimiento del usuario.

El principal problema que conlleva el estudio del caso es en como la información de los usuarios está siendo trastada a las página en línea, pero no es tan malo pasar la información al sistema porque les facilita a las personas autorizadas de cada empresa en los datos de sus usuarios realizar procesos por contratos empresarial o a su vez el proceso de cualquier trámite legal, donde los usuarios al realizar actualización o registrar su información personal, se ubican a un punto muy fijo para que al llegar a un límite más como cuyo nombre HACKER obtengan con facilidad engañar a los usuarios con SMS a nombre de las empresas llegando a lo más profundo de toda la información.

Por una pronta y posible solución que nos lleva a cabo la siguiente pregunta: ¿Cómo un análisis de los diferentes tipos de ataques cibernéticos puede contribuir al Ecuador a guiar a los usuarios y enseñándoles a conocer más de la seguridad que son estafados por notificaciones falsas a través del SMS y disminuir la vulnerabilidad de los dispositivos?

JUSTIFICACIÓN

Los usuarios son los principales afectados por estos ataques. Al analizar los diferentes tipos de ataques cibernéticos que se utilizan a través de los SMS, se puede identificar las tácticas empleadas por los ciberdelincuentes para engañar a los usuarios y robar su información personal o dañar sus dispositivos. Con esta información, es posible en el Ecuador plantar enseñanzas a los usuarios y concienciarlos sobre los peligros potenciales, ayudándoles a tomar medidas preventivas para protegerse.

Las empresas también son objetivos de los ataques cibernéticos a través de los SMS, los delincuentes pueden intentar obtener acceso no autorizado a información confidencial o emplear técnicas de ingeniería social para estafar a los empleados. Al analizar los ataques utilizados, las empresas pueden fortalecer sus sistemas de seguridad y desarrollar políticas para proteger su información.

Se justifica el presente estudio de cado que el Ecuador es un país en desarrollo con una creciente población digital, para así conocer los tipos de ataques utilizados a través de los SMS permite a las empresas y a los usuarios tomar medidas proactivas para evitarlos o mitigar su impacto. Se pueden implementar soluciones de seguridad adecuadas, como autenticación de dos factores, cifrado de datos y sistemas de detección de intrusiones, para reducir la probabilidad de éxito de los ataques.

En el Ecuador existen regulaciones y leyes que exigen que las organizaciones para así proteger adecuadamente los datos de sus usuarios y clientes, uno de ellos es la ley de protección de los datos personales y la firma electrónica, comercio electrónico y lo que corresponde a los mensajes de texto.

OBJETIVOS.

Objetivo General:

Analizar los diferentes tipos de ataques cibernéticos más comunes que se llevan a cabo a través de los SMS.

Objetivos Específicos:

- Examinar los tipos comunes de ataques cibernéticos en SMS para comprender sus características, impactos y posibles contramedidas de seguridad.
- Identificar los daños ocasionados por los ataques cibernéticos a través de los SMS, en términos a la pérdida de información.
- Determinar las herramientas que realiza los ataques cibernéticos a través de SMS, con el fin de conocer más de ellos.

LÍNEAS DE INVESTIGACIÓN.

En base a la línea de investigación, está enfocado en el presente caso de estudio es la siguiente: Sistemas de información y comunicación, emprendimiento e innovación, de tal manera el estudio de los ataques cibernéticos puede ayudar a identificar las nuevas oportunidades innovadoras en el ámbito en la seguridad informática.

Y en la sub línea de la investigación es la siguiente: Redes tecnologías inteligentes de software y hardware, aquí se lleva a cabo la ayuda a utilizar para la prevención los ataques cibernéticos y protección a la información.

El presente estudio de caso aporta al siguiente tema; Soporte y Monitoreo de la Red y Correctivo y Preventivo de la “GOBERNACION DE LO RIOS” realizado en las prácticas pre profesionales en el Ecuador – Los Ríos - Babahoyo en el periodo de Noviembre 2021 – Marzo 2022 de parte de la Universidad Técnica de Babahoyo y proceso a los estudiantes preparándose en la vida profesional, desempeñando las destrezas y enseñanzas a lo aprendido durante el periodo estudiantil, para así fluir el tema del presente estudio de caso Análisis De Los Diferentes Tipos De Ataques Cibernéticos Que Son Utilizados A Través De Los SMS.

MARCO CONCEPTUAL

SISTEMA DEL SMS (MENSAJE DE TEXTO)

Los SMS (SHORT MESSAGE SERVICE) Servicio de Mensaje Corto son vistos en todos los dispositivos móviles del más avanzado hasta el más sencillo. El servicio de los SMS siendo hoy en día está siendo popular. Manejando el módem portátil y una tarjeta SIM celular, permitiendo al sistema el envío y recepción proyectada de SMS a teléfonos móviles. En general, los SMS con mensajes motivacionales y generales fueron todos bien recibidos. (Condori, Menacho Alvirio, Pérez-Lu, & Cavagnaro, 2019)

TEORÍA SISTEMA DEL SMS

En los últimos años, una nueva generación de académicos se ha acercado a los textos que se ha presentado interpretaciones que van más allá de las lecturas tradicionales. Es decir, los soportes livianos como el papiro se pueden encontrar en dos maneras: mientras que en Israel fue utilizado por grupos religiosos y respaldó una disposición cultural al tiempo. El sistema de comunicación SMS se anticipa a la obsesión actual por la información y las constantes interrupciones por la llegada de mensajes que, acaban por hacer claro en primer lugar el proceso de comunicación e intercambio de información que este medio promueve. (Scolari, 2022)

ATAQUES CIBERNÉTICOS

El avance de Internet fue el primer paso para alcanzar el nivel actual de intercambio de información. Comunicaciones, hospitales, centrales hidroeléctricas, bancos, escuelas, comercio, industria, gobiernos, en definitiva, prácticamente todos los sectores dependen en alguna medida de las tecnologías de la información y la comunicación (TIC).

El conjunto de recursos, políticas, conceptos de seguridad, medidas de seguridad, políticas, metodologías de gestión de riesgos, medidas, investigación y desarrollo, capacitación, mejores prácticas, garantías y tecnologías que se pueden utilizar para garantizar la disponibilidad, integridad, autenticación, confidencialidad y no -confidencialidad. (GIRALDO PORTILLO, 2022)

Existen 2 tipos de ataques pasivos y activos, a continuación, su definición:

Ataque pasivo: Es una amenaza que no puede ser descubierta de ninguna manera, afectando principalmente a la confiabilidad de la información.

Ataques activos: Es aquí donde si es detectado, además de afectar a la confidencialidad, también amenazan la integridad y disponibilidad de los datos y servicios. (Fernando, 2020)

INGENIERÍA SOCIAL

Desarrollar las opciones múltiples en el internet para tener redes sociales que actualmente se han desarrollado con nuevas actualizaciones como es Instagram, Facebook, Twitter, entre otras, es directamente conforme a la necesidad humana de consumir servicios como este, compartir datos personales y publicarla es de lo que se aprovechan los ciberdelincuentes.

Los ataques de la ingeniería social han ido desarrollándose día a día y mejor resultado. Es importante decir, que la ingeniería social puede mostrar de dos formas: una interactuando con máquinas y software u otra basada en humanos. (Romero D. , 2019)

ROLES

Cuando se trata de ingenieros sociales, se suele asociar a los hackers, pero la realidad es más compleja. (Romero J. E., 2019)

Hackers: Son encargados de desarrollar software más seguras y robustas en busca de nuevas modalidades para logar su objetivo.

Probadores de seguridad: Aquí utilizan las técnicas de los hackers para entrar a los diferentes sistemas.

Espías: Ellos buscan la información siguiendo los pasos y atreviéndose a lo imposible.

Ladrones de identidad: Es un delito cibernético que tiene graves consecuencias para las víctimas y que presenta desafíos en su investigación y prevención.

Artistas del timo utilizan tácticas manipuladoras para explotar la avaricia de las personas y atraerlas hacia situaciones que parecen "oportunidades" lucrativas.

Agentes de recursos humanos: Su tarea va más allá de simplemente obtener información de los entrevistados, y el potencial de los candidatos encajan con el lugar de trabajo y las necesidades de la empresa.

Vendedores: Es un proceso complejo que implica diversas habilidades y estrategias para lograr que un producto o servicio satisfaga las necesidades de un cliente potencial.

La gente de cada día: es un fenómeno que va más allá de profesionales específicos y se puede observar en diversos ámbitos de la vida cotidiana.

VULNERABILIDAD DE LOS DISPOSITIVOS MÓVILES

Los dispositivos móviles son cada vez más vulnerables a los ataques cibernéticos para los mensajes maliciosos pueden causar daño al procesador de los teléfonos móviles de varias maneras. Un tipo de daño común es la sobrecarga del procesador. Esto puede hacer que el teléfono funcione con lentitud o incluso se bloquee (Garcia, 2020)

Esto se debe a una serie de factores:

La creciente popularidad de los dispositivos móviles: Son cada vez más traídos para acceder a la información y realizar transacciones en línea convirtiéndolo en un objetivo para los ciberdelincuentes.

La falta de seguridad de los dispositivos móviles: Suelen ser menos seguros que las computadoras de escritorio o laptops. Esto se debe a que los dispositivos móviles suelen tener sistemas operativos y aplicaciones más vulnerables en la seguridad.

La falta de conocimiento de los usuarios sobre la seguridad cibernética: Muchos usuarios de dispositivos móviles no son conscientes de los riesgos de seguridad a los que están expuestos. (López Sempere, 2022)

TÁCTICAS EMPLEADAS POR LOS CIBERDELINCUENTES.

Los ciberdelincuentes traen una variedad de tácticas para engañar a los usuarios y robar su información personal o dañar sus dispositivos. Estas tácticas se basan en la psicología humana y en la explotación de nuestras vulnerabilidades. (Alzas Hernandez, 2023)

Algunas de las tácticas más comunes empleadas por los ciberdelincuentes incluyen:

Engaño: Utilizan técnicas de engaño para crear una sensación de urgencia o de confianza. Por ejemplo, pueden enviar mensajes de texto que parecen ser de una fuente conocida, como un banco o una empresa de servicios públicos.

Presión: Es aquí donde obligar a las víctimas a actuar. Por ejemplo, pueden amenazar a las víctimas con revelar información confidencial o con dañar sus dispositivos si no siguen sus instrucciones.

Llamada a la acción: Utilizar mensajes de texto que contienen una llamada a la acción clara. Por ejemplo, pueden pedir a las víctimas que hagan clic en un enlace, que abran un archivo adjunto o que proporcionen información personal.

TIPOS DE DAÑO QUE OCASIONA LOS ATAQUES CIBERNÉTICOS A TRAVÉS DE LOS SMS A LOS USUARIOS

- **Robo de Información Personal y Financiera:** Los ataques SMS pueden transportar al robo de información personal y financiera, como números de tarjetas de crédito, contraseñas, números de seguridad social y otra información confidencial.
- **Compromiso de Cuentas en Línea:** Si los usuarios revelan información de inicio de sesión en respuesta a mensajes falsificados. Esto permite a los atacantes manipular o robar datos y realizar acciones no consideradas en nombre del usuario. (Molina Castaño, 2021)
- **Fraude y Estafas:** Los atacantes pueden utilizar ataques SMS para llevar a cabo fraudes y estafas. Pueden solicitar pagos no autorizados, prometer recompensas falsas o engañar a los usuarios para que compartan información financiera.

- **Pérdida de Datos Sensibles:** Los ataques SMS pueden resultar en la pérdida de datos sensibles y confidenciales almacenados en dispositivos móviles, y a la ves consecuencias financieras, legales y de reputación para los individuos. (Magne Quispe, 2020)
- **Daño a la Reputación:** Si los atacantes utilizan mensajes SMS falsos para difamar a individuos o empresas, esto puede dañar su reputación y credibilidad en línea.
- **Violación de la Privacidad:** Los ataques SMS pueden resultar en la violación de la privacidad de los usuarios al obtener acceso a sus mensajes, contactos, fotos y otros datos personales.
- **Interrupción del Servicio:** Al inundar a los usuarios con mensajes SMS maliciosos o al realizar ataques de denegación de servicio (DDoS) a través de mensajes, los atacantes pueden interrumpir las comunicaciones y el funcionamiento normal de los dispositivos. (Balderas Méndez & Alvarez Monjaraz, 2023)

CIBERSEGURIDAD

Son responsables de la seguridad general de la empresa y ofrecen una gama de servicios que van desde protección básica contra virus y ataques de cibernéticos hasta gestión de errores.

Al subcontratar la protección de la ciberseguridad a expertos, las organizaciones pueden garantizar la protección general de su infraestructura de red. Los proveedores de servicios gestionados permiten a las organizaciones confiar en profesionales experimentados para abordar aspectos críticos de la ciberseguridad, desde el monitoreo continuo de amenazas hasta medidas proactivas para garantizar la integridad y confidencialidad de los datos. (Rodriguez Canfranc, Villar Garcia, Farin Quiros, & Blachez Sora, 2022)

IMPORTANCIA DE LA SEGURIDAD INFORMÁTICA DE LOS USUARIOS

No cabe duda que la seguridad de los sistemas informáticos de una empresa se ha transformado en uno de los pilares más sensibles, vulnerables y es imperioso buscar componentes para fortalecerla. La técnica de la seguridad se cambia a una herramienta fundamental en el método de la información, el beneficio de los recursos técnicos, el desarrollo de nuevas aplicaciones y tecnologías para la organización de los sistemas más avanzados. También en los temas como estrategias de análisis de riesgos y equipos de detección sin olvidar el análisis de posibles impactos en el sistema y los equipos para estos análisis políticas de seguridad y herramientas para detectar estos factores y establecer estas políticas (Palacios, 2020)

SEGURIDAD DE LOS USUARIOS:

En los usuarios es necesario mantener sus dispositivos seguros y no descuidarse en las actualizaciones que le solicite en su dispositivo móvil, como sabemos cada usuario guarda cantidad de información personal como son es la información financiera, las redes sociales o proceso legar de una empresa, o personal. (Garcia Garcia, 2020)

Como recomendación Antivirus y Anti-Malware es una aplicación para los dispositivos móviles, ayuda a disminuir los ataques y la vulnerabilidad. A continuación, veremos unos puntos que nos ayuda a proteger nuestros dispositivos móviles:

1. **Uso de contraseñas:** Es aquí donde los usuarios deben colocar contraseñas seguras al menos de 13 caracteres que incluya número, letras y símbolos.
2. **Actualizado el software:** Ayuda en proteger los dispositivos y disminuir la vulnerabilidad, es recomendable instalar software de seguridad como: AVL Pro es un antivirus que se lo puede descargar en Play Store.

SEGURIDAD EMPRESARIAL:

Es que las estrategias tradicionales de seguridad pueden quedar obsoletas en el contexto de la movilidad y la rápida evolución tecnológica. El sistema de seguridad empresarial no se trata solo de tecnología y protocolos, sino de un enfoque holístico, que va desde la capacitación y el compromiso de los gerentes hasta la implementación efectiva de medidas de seguridad en todos los niveles de la organización. (Cuéllar Fernández, 2023)

Para las empresas se recomienda el uso de la aplicación Gestor de Contraseñas, actualización del software y VPN, ayudara a las empresas estén seguras y menos infiltraciones en el robo de información. A continuación, se mencionará seis áreas principales para un entorno móvil seguro para las empresas a los usuarios:

1. **Gestión de la movilidad empresarial:** Esta es una estrategia que engloba herramientas y tecnologías para gestionar de manera efectiva los dispositivos móviles y portátiles utilizados en las operaciones de una organización.
2. **Seguridad del correo electrónico:** Dado que el correo electrónico es una de las principales vías de ataque cibernético y se enfoca en salvaguardar los datos contra amenazas que se propagan a través del correo electrónico, como malware, phishing y robo de identidad.
3. **Protección de puntos finales:** Con la proliferación de tecnologías como dispositivos móviles y el Internet de las cosas (IoT), los puntos finales se han diversificado y expuesto a más riesgos. El objetivo es proteger los dispositivos conectados y los datos que almacenan de posibles amenazas.

4. **VPN:** Una VPN es una herramienta que permite a una organización extender su red privada de manera segura sobre una red pública. Esto se logra mediante la creación de túneles encriptados que protegen la comunicación entre los usuarios y los recursos de la red.
5. **Gateways de seguridad:** Es un punto de conexión protegido que vincula diferentes tipos de dispositivos o usuarios a la red. Aplica políticas de seguridad y cumplimiento consistentes a todos los usuarios, independientemente de su ubicación o dispositivo.
6. **Agente de acceso a la nube:** El CASB actúa como intermediario entre los usuarios y los proveedores de servicios en la nube. Supervisa la actividad en la nube y aplica políticas de seguridad y cumplimiento para garantizar que el uso de recursos basados en la nube cumpla con las normativas y estándares establecidos.

TIPOS DE ATAQUES CIBERNETICOS MÁS COMUNES UTILIZANDO LOS SMS:

Un ciberataque es un acto malicioso que intenta acceder, cambiar o destruir información confidencial. Donde información personal obtenida en ataques cibernéticos para realizar transacciones fraudulentas, cometer otros delitos o incluso robar las identidades de las víctimas. También pueden dañar o destruir los datos almacenados en el dispositivo.

- **Smishing (SMS Phishing):** Es un ataque dirigido a dispositivos móviles en el que el atacante envía mensajes de texto a la víctima que contienen enlaces maliciosos y el atacante busca robar datos confidenciales del usuario, como información de cuentas bancarias, contraseñas, credenciales de usuario, información de tarjetas de crédito, etc. a través de este mensaje. (Mishra & Devpriya, 2019)

- **Características:** Similar al phishing, los atacantes envían mensajes SMS con enlaces maliciosos o números de teléfono falsificados. El objetivo es que los usuarios hagan clic en los enlaces o respondan a los mensajes con información sensible.
- **Consecuencias:** Los usuarios pueden verse expuestos, robo de información personal y compromiso de la seguridad de sus dispositivos.
- **Medidas de Seguridad:** Se debe evitar hacer clic en enlaces desconocidos y no compartir información confidencial a través de mensajes SMS.

1. **Phishing a través de SMS:** Es una investigación eficaz en la que varios investigadores proporcionan métodos para detectar mensajes de smishing. (Sonowa, 2020)

- **Características:** Los atacantes envían mensajes SMS que aparentan ser de fuentes legítimas, como bancos, empresas o servicios populares. Solicitan a los destinatarios que revelen información confidencial, como contraseñas o números de tarjetas de crédito.
- **Consecuencias:** La divulgación de información personal y financiera puede llevar a fraudes, robo de identidad y pérdidas financieras.
- **Medidas de Seguridad:** Los usuarios deben verificar la autenticidad del remitente, no hacer clic en enlaces sospechosos y no proporcionar información confidencial en respuesta a mensajes SMS no solicitados.

2. **Spoofing de SMS:** Estos ataques permiten, a través de la interceptación de comunicaciones, obtener información suficiente y necesaria para emular, lo que significa violar el sistema. (Roldán Álvarez & Vargas Montoya, 2020)

- **Características:** Falsificación de Identidad, engaño al destinatario con el objetivo principal es engañar al destinatario para que crea que el mensaje y técnica de ingeniería social

- **Consecuencias:** Robo de información, fraude o estafas y compromiso de la seguridad si los destinatarios siguen las instrucciones en el mensaje falso, pueden involuntariamente comprometer la seguridad de sus cuentas, dispositivos o información personal.
- **Medidas de Seguridad:** Verificación de fuentes, no compartir información sensible, desconfiar de mensajes urgentes, es recomendable las aplicaciones de mensajería segura y educación y concienciación.

3. **Malware a través de SMS:** También conocido como código malicioso, es cualquier tipo del software que intencionalmente realiza actividades maliciosas en un sistema informático sin el conocimiento del usuario. Se utiliza técnicas de ingeniería social pasando por una persona o empresa de confianza en un mensaje aparentemente oficial o algún tipo de sistema de mensajería instantánea, redes sociales SMS/MMS. (Chambi Machaca, 2020)

- **Características:** Los atacantes envían mensajes SMS con enlaces o archivos adjuntos maliciosos.
- **Consecuencias:** Los dispositivos pueden quedar infectados con malware que roba información o daña la funcionalidad.
- **Medidas de Seguridad:** No abrir enlaces ni archivos adjuntos de fuentes no confiables y mantener actualizados los dispositivos con soluciones de seguridad.

HERRAMIENTAS QUE REALIZA LOS ATAQUES CIBERNÉTICOS A TRAVÉS DE SMS

Como punto principal el sistema operativo más conocido, tenemos al Kali Linux que nos muestran un sin número de herramientas, es una distribución de Linux especializada en seguridad informática y pruebas de ingenio.

Se utiliza principalmente para realizar pruebas éticas de seguridad en sistemas y redes, incluyendo la investigación y la prevención de ataques cibernéticos, como aquellos que se llevan a cabo a través de SMS.

Como herramienta tenemos las siguientes:

SPOOFING:

Es la suplantación de identidad en mensajes SMS implica ocultar o cambiar el número de teléfono del remitente real en un mensaje de texto, de modo que parezca provenir de un dispositivo diferente. Es un atacante crea un entorno que parece ser auténtico con el fin de engañar a una víctima. Dentro de este entorno falso, la víctima toma decisiones perjudiciales sin darse cuenta de las verdaderas consecuencias de sus acciones. A menudo, las acciones que parecen lógicas en el entorno falso pueden tener implicaciones legales en el mundo real para la víctima. Esta técnica se utiliza comúnmente para llevar a cabo estas actividades engañosas. (MEDINA, 2022)

MALWARE:

Los ataques a través de mensajes de texto implican la creación y distribución de software malicioso diseñado para atacar los dispositivos móviles de las víctimas. Estos programas maliciosos, conocidos como troyanos, tienen la capacidad de realizar llamadas o enviar mensajes de texto sin autorización del usuario. Estas llamadas y mensajes se dirigen a servicios de mensajería SMS o números con tarifas especiales utilizados por ciberdelincuentes para obtener beneficios económicos. Para proteger tus dispositivos móviles contra troyanos que realizan ataques SMS y llamadas no autorizadas, puedes instalar un software antimalware efectivo. Kaspersky Mobile Security, por ejemplo, ofrece una sólida protección para teléfonos Android,

mientras que Kaspersky Tablet Security brinda seguridad para tablets, asegurándote que estén protegidos contra troyanos y otros tipos de malware. (Fernández, 2019)

MARCO METODOLÓGICO

Método de investigación.

El método de investigación utilizado para este estudio de caso fue el método deductivo, siendo un método de investigación que parte de generalizaciones para llegar a conclusiones específicas. En este caso, la investigación se basó en la revisión de libros sobre los diferentes tipos de ataques cibernéticos que son utilizados a través de los SMS.

Tipos de investigación.

El tipo de investigación utilizado para este estudio de caso fue la investigación documental, basándose en la recopilación y análisis de documentos. En este caso, se recopilaron y se analizaron fueron artículos científicos, libros y reportes de investigación sobre los diferentes tipos de ataques cibernéticos que son utilizados a través de los SMS.

Técnicas e instrumentos:

- **Revisión del documento:** Se realizó una revisión de las documentaciones para recopilar información sobre los diferentes tipos de ataques cibernéticos que son utilizados a través de los SMS.
- **Análisis de contenido:** Se utilizó el análisis de contenido para analizar la información compilada a través de la revisión del documento.
- **Entrevistas:** Se utilizó la tabulación de las encuestas con los estudiantes y personal profesional en el área de sistemas y comercio digital.

RESULTADOS

ANÁLISIS DE LOS ATAQUES SMS MÁS COMUNES

El resultado del presente estudio de caso en los ataques SMS como phishing SMS, smishing SMS, Spoofing SMS y malware SMS representan diferentes formas de explotar los mensajes de texto como vector para ataques cibernéticos. Lo que estos ataques tienen en común es que utilizan los mensajes SMS como medio de engaño y manipulación para lograr Exploit. Sin embargo, como lo muestra la tabla 1, este análisis demuestra la necesidad de una mayor inversión en la seguridad cibernética y la educación en el país, con el fin de mitigar los riesgos asociados a los ataques SMS y garantizar la protección de datos personales y sistemas críticos.

Tabla 1 Análisis de los ataques cibernéticos

ANÁLISIS DE LOS ATAQUES SMS MÁS COMUNES		
HERRAMIENTAS	**DESCRIPCIÓN**	**CASOS**
Phishing a través de SMS	Es una forma de engaño en la que los agresores envían mensajes de texto adulterados para conseguir información personal de las víctimas.	En Octubre el 2021, ANT (Agencia Nacional de Tránsito) paso por un ataque cibernético afectando en su sistema.
Smishing (SMS Phishing):	Es aquí donde los mensajes revistan dominar enlaces maliciosos o solicitudes de información personal.	Aunque no se han mencionado casos específicos en este análisis, es una amenaza latente en el panorama de la ciberseguridad.
Spoofing de SMS:	Son involucrar manejo de números de teléfono o el uso de transacciones que permiten remitir mensajes de texto con identidades falsas con enlaces.	Quito, recibió un ataque cibernético el 16 de abril del 2022, el director de Tecnología e Información del municipio de Quito, señala la propagación de un virus que afecto un 20% la información de datos administrativas ha sido afectada.
Malware a través de SMS:	Es aquí donde, si una víctima hace clic en el enlace o a la vez abre el archivo adjunto, se puede instalar malware en su dispositivo	En el 2022 Guayaquil, la Superintendencia de Bancos del Ecuador (SIB) paso por ataques cibernéticos donde 17 han sido detectados y analizando las pérdidas de un valor de USD 10 millones.

Elaborado por: Keyla Alarcon T.

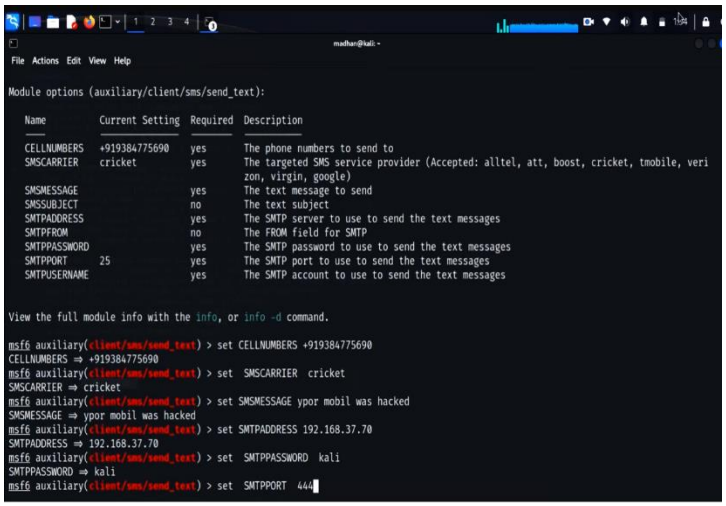
HERRAMIENTA QUE REALIZA ATAQUES CIBERNÉTICOS A TRAVÉS DE LOS SMS.

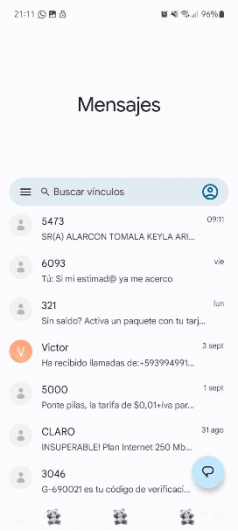
SPOOFING SMS:

Esta es unas herramientas para enviar mensajes anónimos, realiza la entrega de los mensajes de manera rápida, posee un límite de tiempo para enviar un mensaje por día.

Se ingresa al sistema operativo Kali Linux y luego al terminal para iniciar con la práctica.

Ilustración N°1: Ataques cibernéticos con la herramienta Spoofing y bandeja de mensajería de un dispositivo





Elaborado por: Keyla Alarcon T.

- Una vez escrito los comandos se inicia en colocar el número telefónico a nuestro atacante, pero antes abrimos otro terminal para suplantar un sitio web.
- Se ingresa los comandos para de phishing.

- Se selecciona cada paso de para la suplantación del sitio web.

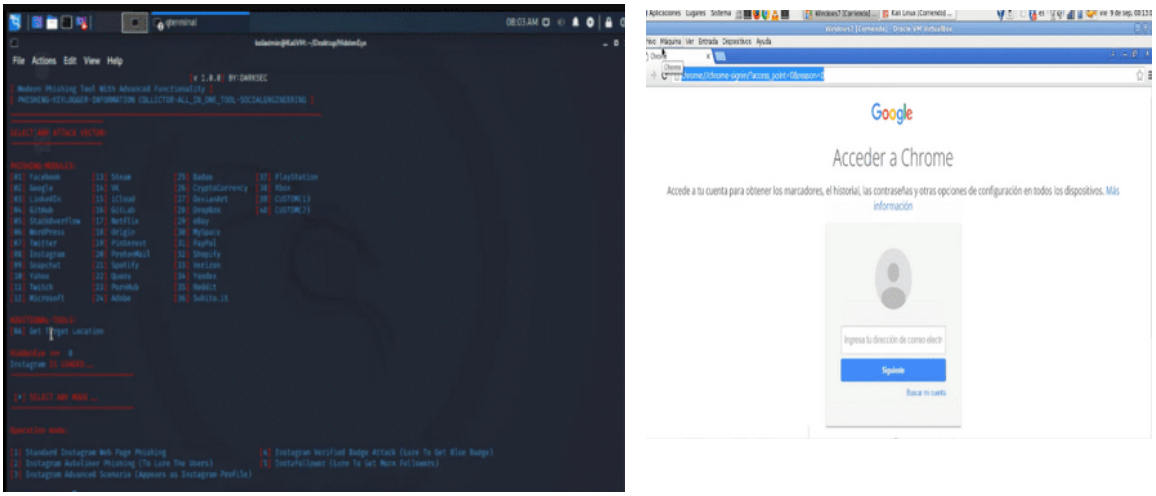


Ilustración N°3: Suplantación de un sitio web

Elaborado por: Keyla Alarcon T.

- Una vez suplantada el sitio se lo selecciona, copia y se lo pega en la primera terminal con el mensaje a la víctima.
- Como resultado esta es nuestra página suplantada y el link del mensaje enviado.

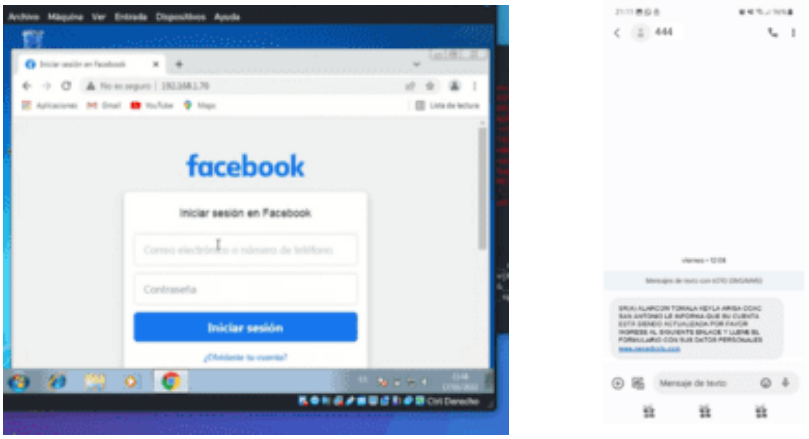


Ilustración N°4: Ataques cibernéticos con la herramienta Spoofing y el mensajes enviado

Elaborado por: Keyla Alarcon T.

TABULACIÓN DE LAS ENCUESTAS

A continuación, se mostrará la cantidad de personas encuestada que son 10 de los estudiantes de la universidad en la carrera de sistemas de información de 8° semestre y 10 profesionales que trabajan en empresas.

Tabla 1: Número de personas encuestadas.

POBLACIÓN	CANTIDAD DE ENCUESTADOS
Estudiantes y trabajadores	**20**

Elaborado por: Keyla Alarcon T.

1. **¿Con qué frecuencia utiliza dispositivos móviles para enviar y recibir mensajes de texto (SMS)?**

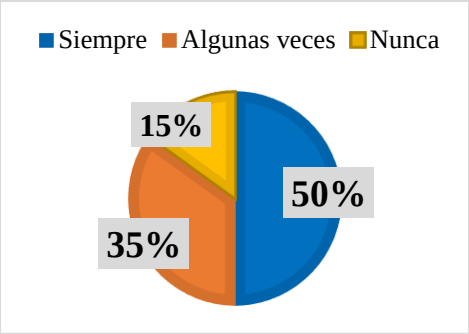


Tabla 2: Porcentaje de la pregunta N° 1.

Elaborado por: Keyla Alarcon T.

De las personas encuestadas un 50% si usa con frecuencias los mensajes de textos SMS, mientras que un 35% algunas veces lo usan y por lo consiguiente un 15% no lo utilizan.

Tabla 3: Respuestas de las personas encuestadas.

SIEMPRE	ALGUNAS VECES	NUNCA
50%	35%	15%

Elaborado por: Keyla Alarcon T.

2. **¿Ha sido víctima o conoce a alguien que haya sido víctima de algún tipo de ataque cibernético a través de mensajes de texto (SMS)?**

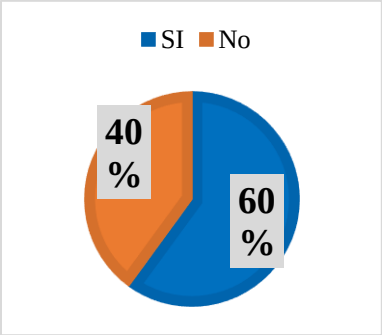


Tabla 4: Porcentaje de la pregunta N° 2.

Elaborado por: Keyla Alarcon T.

El 60% Si han sido víctimas en ataques cibernéticos a través de los SMS, mientras que un 40% No son víctima del mismo.

Tabla 5: Respuestas de las personas encuestadas.

SI	NO
60%	40%

Elaborado por: Keyla Alarcon T.

3. **¿Ha recibido alguna vez un mensaje de texto (SMS) sospechoso que solicitaba información personal o financiera?**

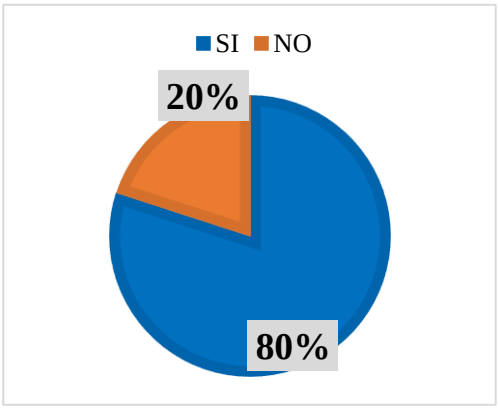


Tabla 6: Porcentaje de la pregunta N° 3.

Elaborado por: Keyla Alarcon T.

El 80% Si han recibido mensajes sospechosos pidiéndoles información, mientras que un 20% No han recibido mensajes desconocidos.

Tabla 7: Respuestas de las personas encuestadas.

SI	NO
80%	20%

Elaborado por: Keyla Alarcon T.

4. **¿Considera que el aprendizaje a los usuarios es fundamental para prevenir ataques cibernéticos a través de mensajes de texto (SMS)?**

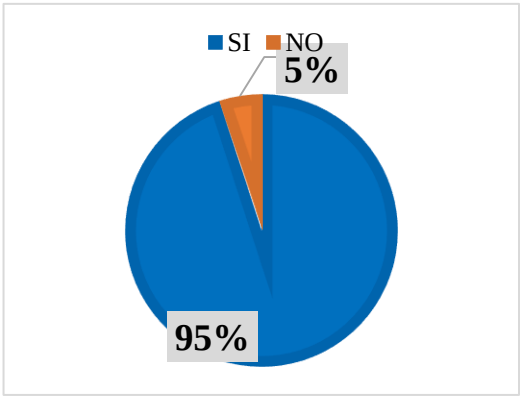


Tabla 8: Porcentaje de la pregunta N° 4.

Elaborado por: Keyla Alarcon T.

El 90% Si está de acuerdo en el aprendizaje a los usuarios para prevenir los ataques cibernéticos a través de los SMS, mientras que un 5% No está de acuerdo.

Tabla 9: Respuestas de las personas encuestadas.

SI	NO
95%	5%

Elaborado por: Keyla Alarcon T.

5. **¿Ha tomado alguna medida para protegerse hacia los posibles ataques cibernéticos a través de mensajes de texto (SMS)?**

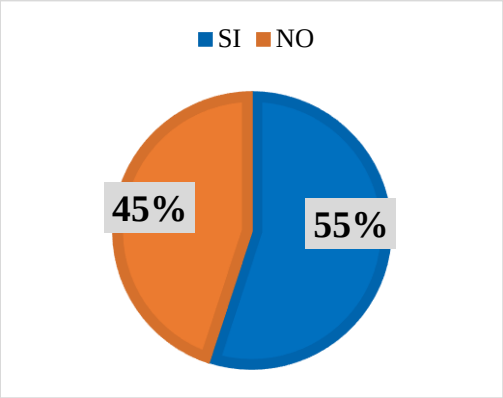


Tabla 10: Porcentaje de la pregunta N° 5.

Elaborado por: Keyla Alarcon T.

El 55% Si ha tomado medidas de seguridad para proteger sus dispositivos móviles, mientras que un 45% No han tomado medidas.

Tabla 11: Respuestas de las personas encuestadas.

SI	NO
55%	45%

Elaborado por: Keyla Alarcon T.

DISCUSIÓN DE RESULTADOS

Los resultados obtenidos a través de la investigación y análisis de los ataques cibernéticos a través de SMS revelan una amenaza significativa para la seguridad de los usuarios y organizaciones en el entorno digital. La identificación de estos ataques y la comprensión de sus consecuencias son esenciales para desarrollar estrategias de protección efectivas.

Como se menciona en la tesis Según (Freire Cobos & Pazmino Velez, 2019) La importancia de la seguridad de la información en el contexto de una empresa de servicios de SMS masivos. Ambos resaltan la necesidad de tomar medidas para proteger los datos críticos y salvaguardar la privacidad y la confidencialidad.

Los ataques a través de SMS pueden llevar a la divulgación de datos personales y financieros, lo que tiene consecuencias significativas tanto a nivel personal como empresarial. Además, la exposición a la manipulación de datos representa una amenaza adicional para la integridad de la información. Estos resultados subrayan la importancia crítica de proteger los datos y preservar la privacidad en el entorno digital.

Los resultados de este estudio enfatizan la necesidad de abordar de manera proactiva los riesgos asociados con los ataques cibernéticos a través de SMS. La concienciación, la educación y la implementación de medidas de seguridad adecuadas son fundamentales para proteger la información sensible y salvaguardar la privacidad y la seguridad en el mundo digital. El conocimiento y la preparación son las mejores defensas contra estas amenazas en constante evolución.

Sin embargo, los avances tecnológicos y las tácticas de ataque en constante evolución requieren que las instituciones y personas se mantengan al día con las últimas tendencias en ciberseguridad y continúen fortaleciendo sus defensas. La discusión también subraya la importancia de la concienciación y la educación en materia de seguridad informática, la falta de conocimiento puede ser una brecha significativa en la protección de datos.

Como también lo menciona la tesis; (Albán, Urvina, & Andrade, 2022) Es evidente que la seguridad de la información no se limita únicamente a salvaguardar los equipos físicos, sino que también implica la creación de un ambiente organizado y consciente en el que el personal técnico y administrativo esté debidamente capacitado para prevenir y responder a posibles amenazas. La necesidad de preparación y respuesta se destaca aún más al considerar que no solo los hackers externos representan una amenaza, sino que también pueden surgir riesgos internos, lo que subraya la necesidad de una vigilancia constante y de políticas sólidas de seguridad de la información.

Es necesario tomar en cuenta las recomendaciones para evitar los ataques, mucho más tener una buena capacitación, software que proteja los dispositivos móviles y no mostrar las informaciones personales a las personas, lugar o páginas que desconozcamos para asi evitar caer y se filtren a nuestros datos personales.

CONCLUSIONES

Se concluyó el presente estudio de cado dando a conocer el cumplimiento de los objetivos.

Se fundamentó teórica de los tipos de ataques cibernéticos más comunes a través de SMS nos ha permitido alcanzar sus características, las graves consecuencias que pueden llevar y las medidas de seguridad favorables para protegernos. Este conocimiento es esencial para abordar eficazmente las amenazas cibernéticas relacionadas con los mensajes de texto y tomar acciones preventivas informadas para salvaguardar nuestros datos y nuestra seguridad en el mundo digital.

Se identificó los daños causados por los ataques cibernéticos a través de SMS revela la amenaza real que estos ataques simbolizan en términos de pérdida de información sensible. Además, pueden resultar en la divulgación de datos personales y financieros, así como en la exposición a la manipulación de datos. Es fundamental tomar medidas de seguridad y educar a los usuarios sobre estas inseguridades para mitigar la pérdida de información y preservar la privacidad y la seguridad en el entorno digital.

Se determinó las herramientas y técnicas utilizadas en los ataques cibernéticos a través de SMS nos proporciona una visión más clara de la complejidad y la astucia detrás de estos ataques. Estas herramientas incluyen la creación de sitios web de phishing, el desarrollo de malware móvil y la suplantación de identidad, entre otros. Comprender cómo operan estas herramientas es crucial para desarrollar estrategias efectivas de defensa cibernética y protegerse contra estas amenazas en el entorno digital.

RECOMENDACIONES

En el presente estudio de caso se da a conocer las recomendaciones para evitar los ataques cibernéticos a través de los SMS.

- Implementar programas de educación y concienciación para los usuarios de dispositivos móviles. Enséñales a identificar posibles ataques a través de SMS y cómo evitar caer en trampas de phishing o malware. El conocimiento y la concienciación son la primera línea de defensa contra los ataques cibernéticos a través de SMS.
- Anticipar la protección de datos personales y financieros al interactuar con mensajes de texto. Insta a las personas a ser especialmente cautelosas al compartir información sensible a través de SMS y a verificar la autenticidad de los mensajes y remitentes antes de divulgar datos. Además, fomenta el uso de soluciones de seguridad cibernética en dispositivos móviles para proteger la información sensible de posibles ataques a través de SMS.
- Considera la adopción de soluciones de seguridad móvil en dispositivos que permitan proteger datos personales y financieros. Estas soluciones pueden incluir aplicaciones de seguridad que detecten y bloqueen mensajes de texto maliciosos y proporcionen una capa adicional de protección contra posibles ataques cibernéticos a través de SMS. Al invertir en tecnología de seguridad móvil, puedes ayudar a mitigar la pérdida de información y garantizar la privacidad y la seguridad en el entorno digital.

BIBLIOGRAFÍA

Albán, F., Urvina, M., & Andrade, R. (2022). *Análisis y Diseño de un Modelo Predictivo para Detección de Phishing Basado en Url y Corpus del Correo Electrónico.* Quito: Vol. 50, No. 3.

ALVARADO CHANG, J. E. (2020). *Análisis de ataques cibernéticos hacia el Ecuador.* Daule: ISSN: 2600-5662.

Alzas Hernandez, J. (2023). *Estudio de fraudes basados en la técnica de Ingeniería Social.* Catalunya: Universitat Oberta de Catalunya (UOC).

Balderas Méndez, M. G., & Alvarez Monjaraz, M. Y. (2023). *Sociedad de la información y nuevas formas de victimización.* Querétaro: Derecho.

Chambi Machaca, L. I. (2020). *Estrategias para evitar ataques de Phishing en Empresas.* La Paz: IEEE.

Condori, I., Menacho Alvirio, L. A., Pérez-Lu, J. E., & Cavagnaro, C. C. (2019). *Envío de mensajes de texto para mejorar la adherencia de pacientes en targa: ensayo aleatorizado controlado.* LIMA: Rev Peru Med Exp Salud Publica.

Cuéllar Fernández, R. (2023). *La capacitación delos cuadros y reservas del sector empresarialcubano, en gestión y cultura de seguridad.* Cuba: 1684-5765.

EKOS. (18 de Nobiembre de 2022). Obtenido de EKOS: https://ekosnegocios.com/articulo/kaspersky-registra-mas-de-2-300-ataques-de-malware-por-minuto-en-la-region

Fernández, M. J. (2019). *Inyección de malware en aplicación Android legítima.* Sevilla: Attribution-NonCommercial-NoDerivatives 4.0 Internacional.

Fernando, G. R. (2020). *Internet de las Cosas: una revisión de vulnerabilidades, amenazas y contramedidas.* Ocaña: ISSN 2011-642X.

Freire Cobos, L. D., & Pazmino Velez, G. E. (2019). *Implementación de un esquema de seguridad en base a las normas de calidad iso 27001 para una empresa de servicio de mensajes simples (sms).* Guayaquil: Espol.

Garcia Garcia, M. (2020). *Seguridad en dispositivos móviles: Análisis de riesgos, de vulnerabilidades y auditorías de dispositivos.* Barcelona: Universitat Oberta de Catalunya (UOC).

Garcia, M. G. (Enero de 2020). *Seguridad en dispositivos moviles.* Obtenido de Seguridad en dispositivos moviles: https://openaccess.uoc.edu/bitstream/10609/107326/6/mgarciagarcia45TFM0120memoria.pdf

GIRALDO PORTILLO, L. A. (17 de Febrero de 2022). *ANÁLISIS DE LOS TIPOS DE ATAQUES CIBERNÉTICOS OCURRIDOS EN COLOMBIA DURANTE LA PANDEMIA COVID-19 ENTRE LOS AÑOS 2020 Y 20211.* Obtenido de ANÁLISIS DE LOS TIPOS DE ATAQUES CIBERNÉTICOS OCURRIDOS EN COLOMBIA DURANTE LA PANDEMIA COVID-19 ENTRE LOS AÑOS 2020 Y 20211: https://repository.unimilitar.edu.co/bitstream/handle/10654/43621/GiraldoPortilloLuzAdriana2022.pdf?sequence=1&isAllowed=y

Gómez Zúñiga, J. G., & Suquilanda Rodríguez, Á. A. (2022). *Aplicación de una metodología de seguridad para el desarrollo seguro de aplicaciones móviles de pagos en línea usando herramientas OPEN SOURCE.* Guayaquil: Universidad de Guayaquil. Facultad de Ciencias Matemáticas y Físicas. Carrera de Ingeniería en Networking y Telecomunicaciones.

Huerta Riveros, P. C., Gaete Feres, H. G., & Pedraja Rejas, L. M. (2020). *Dirección estratégica, sistema de información y calidad. El caso de una universidad estatal chilena.* Chile: vol.31 no.2 La Serena.

Llanos Mora, E. L. (2020). *Diseño de un sistema inalámbrico de monitoreo para pacientes epilépticos de la clínica Anglo Americana.* Obtenido de Diseño de un sistema inalámbrico de monitoreo para pacientes epilépticos de la clínica Anglo Americana: https://repositorio.utp.edu.pe/bitstream/handle/20.500.12867/3125/Erika%20Llanos_Trabajo%20de%20Suficiencia%20Profesional_Titulo%20Profesional_2020.pdf?sequence=1&isAllowed=y

López Sempere, A. (2022). *Identificación y detección de vulnerabilidades.* Valencia: Universitat Politècnica de València.

Magne Quispe, J. W. (2020). *Modelo de Ciberseguridad Corporativa en el Sistema Bancario.* La Paz - Bolivia: Universidad Mayor de San Andrés.

MEDINA, H. C. (2022). *ANÁLISIS DE VULNERABILIDADES EN DISPOSITIVOS MÓVILES CON SISTEMA OPERATIVO ANDROID* . BOGOTÁ: Creative Commons Atribución-NoComercial-SinDerivadas 4.0.

Mishra, S., & Devpriya, S. (2019). *Enfoques de phishing y mitigación de SMS.* Noida, India: IEEE.

Molina Castaño, S. (2021). *Ciberseguridad de las empresas financieras.* Colombia: Tecnológico de Antioquia, Institución Universitaria.

Palacios, A. P. (2020). *Seguridad Informática.* España: COPYRIGHT © 2020 Ediciones Paraninfo, SA 1st edition.

Parra Medina, J. E. (2020). *Diseño de un sistema de información para el control de inventario de medicamentos en farmacias colombianas.* Bogotá: CC BY-NC 2.5.

Postigo Palacios, A. (2020). *Seguridad informática.* Madrid: Ediciones Paraninfo, SA 1. edición, 2020.

Prieto, M. D. (2019). *Seguridad en dispositivos móviles.* Obtenido de Seguridad en dispositivos móviles: http://recsi2012.mondragon.edu/es/programa/recsi2012_submission_05.pdf

Reyes Corredor, E., & Bernal Medina, H. C. (2022). *Análisis de vulnerabilidad en dispositivos móviles con sistema operativo Android.* Santa Fe: Editorial Universitaria San Mateo.

Rodriguez Canfranc, P., Villar Garcia, J., Farin Quiros, C., & Blachez Sora, J. (2022). *Sociedad digital en España 2022.* Casarrubuelos(MADRID): 978-84-306-259-8.

Roldán Álvarez, M. Á., & Vargas Montoya, H. F. (2020). *Ciberseguridad en las redes móviles de telecomunicaciones y su gestión de riesgos.* Colombia: 2145-9371 (on line).

Romero, D. (2019). *EL ARTE DE LA INGENIERÍA SOCIAL.* Obtenido de EL ARTE DE LA INGENIERÍA SOCIAL: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/6354/El%20arte%20de%20la%20ingenier%c3%ada%20social.pdf?sequence=1&isAllowed=y

Romero, J. E. (Enero de 2019). *Estudio de metodologías de Ingeniería Social.* Obtenido de Estudio de metodologías de Ingeniería Social: https://openaccess.uoc.edu/bitstream/10609/89045/6/joanenricgarciaromeroTFM0119memoria.pdf

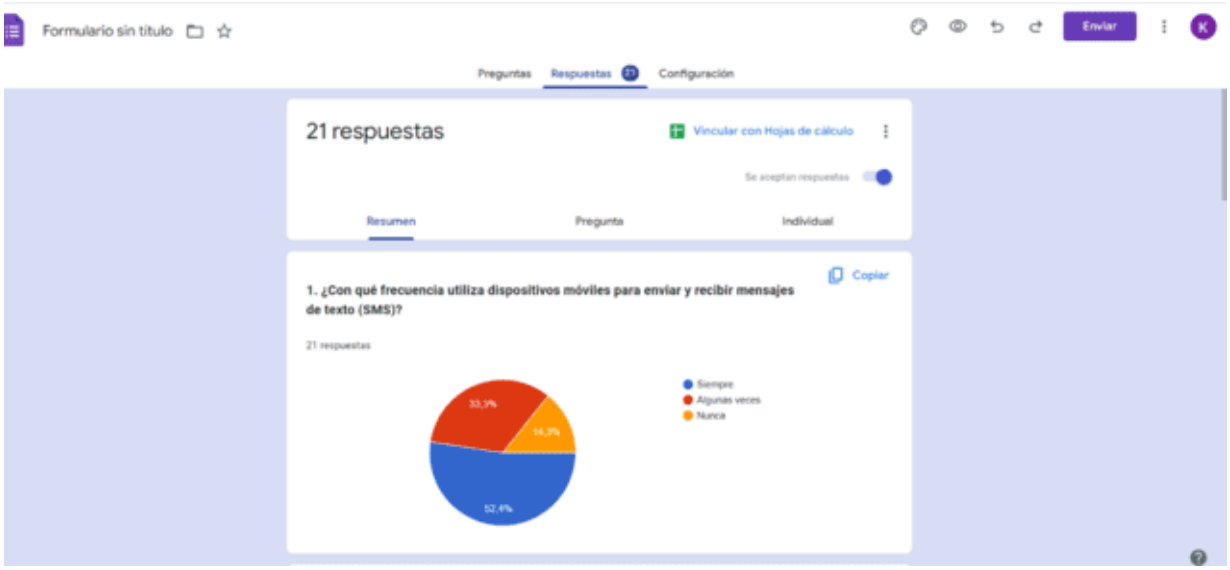
Roy, P. K. (2020). *Aprendizaje profundo para filtrar SMS Spam.* India: 2019 Elsevier B.V. All rights reserved.

Scolari, C. A. (2022). *Evolution of the media: map of a discipline under construction. A review.* Barcelona: Vol. 31 Núm. 2 (2022): Edición, libro y lectura.

Sonowa, G. (2020). *Detecting Phishing SMS Based on Multiple Correlation Algorithms.* India: Editors-in-Chief.

ANEXOS

Anexo 1: Imagen de total de encuestados.

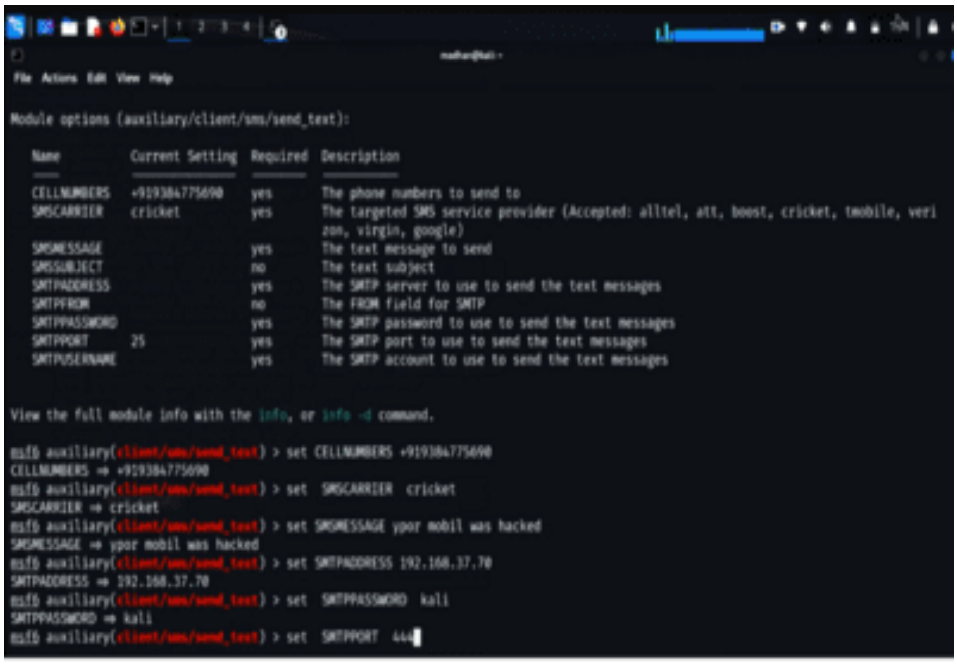


Elaborado por: Keyla Alarcon T.

Anexo 2: Practica en el sistema operativo Kali Linux

Elaborado por: Keyla Alarcon T.

Anexo 3: Practica en la herramienta SPOOFING SMS



Elaborado por: Keyla Alarcon T.

CERTIFICADO ANTIPLAGIUM

Anexo 1: Certificado de porcentaje de similitud con otras fuentes.

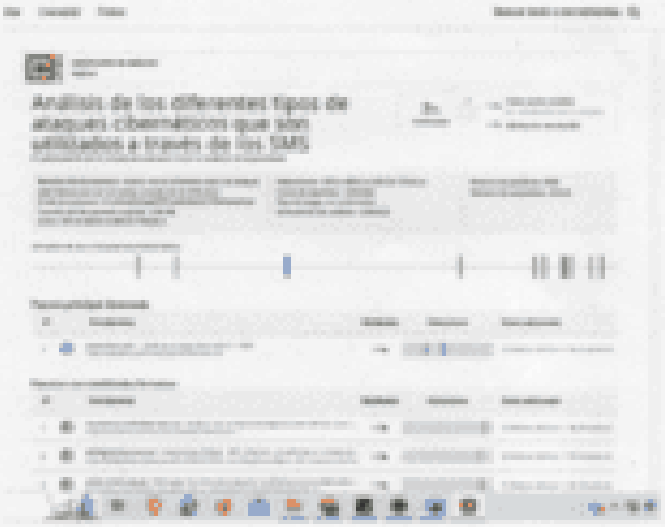
UNIVERSIDAD TÉCNICA DE BABAHOYO
FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA
CARRERA DE SISTEMA DE INFORMACIÓN

Babahoyo, 14 de septiembre del 2023

CERTIFICACIÓN DE PORCENTAJE DE SIMILITUD CON OTRAS FUENTES EN EL SISTEMA DE ANTIPLAGIO

En mi calidad de Tutora del Trabajo de la Investigación de la Srta:ALARCÓN TOMALA KEYLA ARISA, cuyo tema es: ANÁLISIS DE LOS TIPOS DE ATAQUES CIBERNÉTICOS UTILIZADOS A TRAVÉS DE LOS SMS, Certifico que este trabajo investigativo fue analizado por el Sistema Antiplagio Compilatio obteniendo como porcentaje de similitud de: **[3%]**, resultados que evidenciaron las fuentes principales y secundarias que se deben considerar para ser citadas y referenciadas de acuerdo a las normas de redacción adoptadas por la institución y Facultad.

Considerando que, en el Informe Final el porcentaje máximo permitido es el 10% de similitud, queda aprobado para su publicación.



Por lo que se adjunta una captura de pantalla donde se muestra el resultado del porcentaje indicado.

Ing. Sist. Narcisa María Crespo Torres, MSc.
DOCENTE DE LA FAFI.