UNIVERSIDAD LAICA “ELOY ALFARO” DE MANABÍ
EXTENSIÓN EN EL CARMEN

CARRERA DE INGENIERÍA EN SISTEMAS

PREVIO A LA OBTENCIÓN DE TÍTULO DE INGENIERA EN SISTEMAS

TRABAJO DE INVESTIGACIÓN

Implementación de guía de ataques informáticos y medidas de seguridad como solución preventiva a WhatsApp en la entidad “Asesorarte” El Carmen – Manabí

AUTOR(A)

Torres Pinargote María Monserrate

DOCENTE TUTOR

AS. María Soraida Zambrano Quiroz, Mg.

El Carmen, Marzo 2023

CERTIFICACIÓN DE LA TUTORA

Uleam	NOMBRE DEL DOCUMENTO: CERTIFICADO DE TUTOR(A)	CÓDIGO: PAT-01-F-010
	PROCEDIMIENTO: TITULACIÓN DE ESTUDIANTES DE GRADO	REVISIÓN: 2
		Página 1 de 1

En calidad de docente tutor(a) de la Extensión en El Carmen de la Universidad Laica "Eloy Alfaro" de Manabí, CERTIFICO:

Haber dirigido y revisado el trabajo de investigación, bajo la autoría de la estudiante **Torres Pinargote Maria Monserrate**, legalmente matriculado/a en la carrera de Ingeniería en Sistemas, período académico 2022-2023, cumpliendo el total de 400 horas, bajo la opción de titulación de Proyecto de Investigación, cuyo tema del proyecto es **"Implementación de guía de ataques informáticos y medidas de seguridad como solución preventiva a whatsapp en la entidad Asesorarte – El Carmen - Manabí"**.

La presente investigación ha sido desarrollada en apego al cumplimiento de los requisitos académicos exigidos por el Reglamento de Régimen Académico y en concordancia con los lineamientos internos de la opción de titulación en mención, reuniendo y cumpliendo con los méritos académicos, científicos y formales, suficientes para ser sometida a la evaluación del tribunal de titulación que designe la autoridad competente.

Particular que certifico para los fines consiguientes, salvo disposición de Ley en contrario.

El Carmen, 23 de enero del 2023.

Lo certifico,

A.S. María Soraida Zambrano Quiroz, Mg.
Docente Tutor(a)
Área: Sistemas

UNIVERSIDAD LAICA "ELOY ALFARO" DE MANABÍ
EXTENSIÓN EN EL CARMEN

DECLARACIÓN DE AUTORÍA

Yo, **Torres Pinargote María Monserrate con** C.I **131088446-3**, estudiante de la Facultad de Sistemas de la Universidad Laica "Eloy Alfaro" de Manabí; con relación al informe final presentado para la obtención del título de Ingeniera en Sistemas, declaro que la presente tesis es de mi autoría la argumentación, el sustento de la investigación y los criterios vertidos, son originalidad del autor siendo de su responsabilidad.

_____

Torres Pinargote María Monserrate

131088446-3

DEDICATORIA

En primer lugar, quiero dedicar esta tesis a Dios, quién ha sido mi fortaleza, luz y guía, a mi madre, mi tía, mi esposo y mi hijo por ser un pilar fundamental y nunca dejarme sola. A mi tutora de tesis la A.S Soraida Zambrano y todos los docentes, que me impartieron sus conocimientos y quienes hicieron de esta experiencia una de las más especiales en mi vida.

María Torres

AGRADECIMIENTO

Primero quiero, agradecer a Dios por haberme permitido tener salud en estos momentos de pandemia y poder así culminar mi trabajo de titulación. Además de ello agradecerle a mi madre por ser madre y padre y por siempre ayudarme a seguir adelante en mi vida, a mi tía por apoyarme en esta etapa además de mi esposo y mi hijo los cuales son mi motivo para seguir adelante y poder superarme.

También quiero agradecerle a cada uno de los ingenieros que aportaron con sus conocimientos en este trayecto, en especial a mi tutora de tesis la A.S Soraida Zambrano que con su esfuerzo y dedicación fue un pilar importante en la elaboración y diseño de esta tesis académica.

María Torres

INDICE

Índice de Tablas

RESUMEN

El proyecto de titulación se enfoca, en la implementación de una guía de ataques informáticos y medidas de seguridad como solución preventiva a WhatsApp en la entidad “ASESORARTE”. Resulta que ha sido atacado por los ciber delincuentes, y el ataque se ha llevado a cabo con diversos virus, que han existido a lo largo del avance de la tecnología.

Lastimosamente gracias a que WhatsApp es la red social más utilizada a nivel mundial está expuesta a ser atacada, ahí es donde está verdaderamente el problema. Ya que con varios tipos de virus hoy en son muy fáciles de utilizar y manejar para los ciberdelincuentes.

Durante la investigación se utilizó la metodología inductiva y deductiva conocer la información específica, partió desde lo general hasta llegar a una sola conclusión a fin de que se pudo hacer la orientación en el proceso investigativo en un correcto desarrollo de la investigación y así obtener un criterio acertado. Se analizó la información que proporcionó la empresa, en una o varias partes de forma individual, con el fin de haber observado las causas y efectos que se produjeron y así poder elegir las mejores alternativas para resolver dicho problema.

La población que se considera para esta investigación es lo 450 clientes, haciendo un cálculo de muestreo de población finita de10 usuarios que fueron encuestados.

Para encontrar una solución a dicho problema se realizó en la empresa “ASESORARTE” una entrevista a el gerente y dueño del local, en la cual el gerente dio a conocer acerca de dicho problema, y se realizó una encuesta a los

clientes de la empresa donde supieran manifestar sus conocimientos acerca de los ataques a WhatsApp.

Por todos los problemas que han causado los ataques informáticos se ha creado esta guía. Para protegerse de los ataques deben saber la definición de qué son los ataques informáticos, qué son los virus, cómo se pueden prevenir, cómo se puede solucionar qué tipos de virus existen en qué se basan qué es lo que quieren hacer cómo pueden afectar, cómo se puede solucionar, cómo se puede contrarrestar.

.

Abstract

The titling project focuses on the implementation of a guide to computer attacks and security measures as a preventive solution to WhatsApp in the "ASESORARTE" entity. It turns out that it has been attacked by cyber criminals, and the attack has been carried out with various viruses, which have existed throughout the advancement of technology.

Unfortunately, thanks to the fact that WhatsApp is the most used social network worldwide, it is exposed to being attacked, that is where the problem really lies. Already with various types of viruses today very easy to use and handle for cybercriminals.

To find a solution to this problem, an interview with the manager and owner of the premises was carried out in the company "ASESORARTE", in which the manager informed us about his information about said problem, and a survey was carried out with the clients. of the company where they knew how to express their knowledge about the attacks on WhatsApp.

For all the problems that computer attacks have caused, this guide has been created. To protect them from attacks, we must know the definition of what computer attacks are, what viruses are, how we can prevent them, how we can solve it, what types of viruses exist, what they are based on, what they want to do, how they can affect us, how we can fix it how can we counteract it,

We drew on the research to come up with the guide, and we located all the necessary topics based on the results of both the survey and the interview. That is to say, taking information that both the manager and the clients have no knowledge of the attacks that they may be victims of.

INTRODUCCIÓN

A nivel mundial la red social WhatsApp es la red más conocida y utilizada para comunicarse, enviar fotos, videos, emojis y de más elementos, WhatsApp cuenta con más de treinta millones de usuarios. Debido a que se ha convertido en un medio de comunicación esencial tanto a nivel laboral como personal.

Por lo que conlleva que este medio de comunicación se haya visto vulnerable por los ciberdelincuentes, es decir se han reportados ataques hacia esta red. Ataques que han sido muy graves entre estos ataques se encuentran, hurto de claves bancarias, robo de contraseñas de correos personales y sustracción de información personal. Para chantajear y manipular a usuarios que ha sido victimas de estos ataques.

El objetivo de dicho proyecto es realizar una guía metodológica que le de conocimiento acerca de los ataques y lo que puede hacer para prevenirlos.

Se ha utilizado la metodología de investigación la cual abarca varias metodologías como la inductiva la deductiva y la analítica, estas fueron las metodologías utilizadas lo largo del desarrollo de este proyecto de titulación, en la cual se procesa y analiza la información con el fin de obtener los datos los cuales validaran la información obtenida.

Gracias a la investigación realizada se concluyó en los resultados obtenidos, que no hay mucho conocimiento de los ataques que se pueden realizar y de esta manera afectar a la víctima.

La empresa “ASESORARTE” fue el lugar donde se realizó dicha investigación empresa dirigida por el ingeniero Roody Ramírez, es una empresa de asesoría tributaria lo que quiere decir que esta empresa se dedica a el asesoramiento de negocios, el asesoramiento con propiedades el préstamo en efectivo entre otros.

Una vez realizada la encuesta y entrevista se le aplico a los clientes y al gerente dichos procesos al momento de recibir los resultados se detectó el problema el cual se basa en el poco conocimiento que tienen sobre los ataques informáticos.

Por todos estos motivos se ha propuesto crear una guía metodológica que tendrá la suficiente información, para tener conocimiento de cómo podemos protegernos de estos ataques.

Para saber más de los peligros que corre la red social de WhatsApp es necesario definir qué son los ataques y qué tipos de virus existen, cómo podemos protegernos de dichos virus, hay un virus en especial el cual se llama Keylogger este virus es uno de los más utilizados, ya que registra las pulsaciones que realizamos en nuestro celular, ya puede registrar puede saber de qué estamos hablando, qué estamos buscando y en que estamos navegando al igual que existen virus existen antivirus los cuales nos pueden ayudar a controlarlos y ponerles un alto.

Hay muchos temas que van a tocar este proyecto en el capítulo uno se encuentra.

En el primer capítulo se describe el marco teórico con los ataques informáticos, su definición, la definición de medidas de prevención y seguridad informática, la solución preventiva y definición de la aplicación de WhatsApp.

En el capítulo dos se encuentra el estudio de campo su metodología de investigación, los tipos de investigación, la bibliográfica, los métodos de investigación, el método Inductivo deductivo y analítico,

En el capítulo tres la propuesta, antecedentes, reseña histórica, misión, visión y su estructura empresarial.

1. MARCO TEÓRICO

1.1 Ataques informáticos

1.1.1 Definición

Un ataque informático se basa en aprovechar las vulnerabilidades que se pueden presentar en el software, hardware e incluso en los individuos que integran parte de un ambiente en el campo de la informática, con la finalidad de obtener un beneficio, que por lo general este beneficio suele ser económico, generando un efecto negativo en la seguridad del sistema. Uno de los pasos más importantes en seguridad, es la educación. Comprender cuáles son las debilidades más comunes que pueden ser aprovechadas y cuáles son sus riesgos asociados, permitirá conocer de qué manera se ataca un sistema informático, ayudando a identificar las debilidades y riesgos para luego desplegar de manera inteligente estrategias de seguridad efectivas. (Weber, 2020)

Por otra parte, de acuerdo con el registro publicado por el Boletín N° 46 (2018), considera que un ataque informático son las acciones deliberadas por uno o más individuos que caen bajo la denominación de ciberdelincuentes organizados que en esencia no se dediquen al cibercrimen, pero poseen la intención de generar algún daño informático en los sistemas, redes y dispositivos electrónicos.

Es por esta razón que considero fundamental, aplicar herramientas de seguridad informática, que nos permitan proteger de forma segura tanto el software como el hardware de nuestros dispositivos, ya que no solo nos beneficiara de prevenir ataques generados por los hackers o ciberdelincuentes, sino que además nos ayudar a estar menos expuestos a virus informáticos, y mejorara el sistema óptimo de desarrollo de nuestros aparatos tecnológicos

1.1.2 Definición de los tipos de ataques informáticos

De acuerdo con Ciberseguridad (2021), los ataques informáticos constituyen una de las mayores amenazas para las empresas, y para el mundo debido a que afecta a ambos por igual, sean estas de carácter público o privado e incluso sociedades mixtas y personas naturales, debido a esto, es necesario dar prioridad a las medidas de prevención informáticas, en especial para aquellas organizaciones que depende en su totalidad del internet para la realización de sus operaciones, entre los ataques más comunes podemos destacar los siguientes:

1.1.1.2 Malware

Un ciberataque es denominado un conjunto de acciones ofensivas, las cuales consiste en irrumpir o atacar los sistemas de información, los cuales suelen estar representados por bases de datos, redes informáticas, etc. Es por esta razón que el principal objetivo de un ataque informático se basa en dañar, alterar, manipular o destruir los datos informáticos almacenados a fin de obtener un beneficio económico, o a su vez destruir a las organizaciones o persona, además de que mediante el ataque informático ejecutado pueden anular los servicios que prestan las organizaciones, y así robar los datos con el propósito de poder emplearlos para espiar o extorsionar a la víctima. (Bello, 2021)

De acuerdo con el criterio de Infocyte (2021), determina que un ataque informático es aquel que se encuentra integrado por varios tipos de ataques entre los cuales se incluyen spyware, virus y gusanos, esta modalidad emplea una vulnerabilidad para romper una red, cuando el usuario haga clic en un enlace de correo electrónico peligroso, que se utiliza para instalar software malintencionado en el sistema generando como consecuencia la denegación de acceso a los componentes críticos de la red, interrupción del sistema o avería. Cabe mencionar que a pesar de su variedad ente los tipos más comunes podemos observar los siguientes:

- **Virus:** infectan aplicaciones que se adjuntan a la secuencia de inicialización, se replica a sí mismo, infectando otro código en el sistema informático.

- **Troyanos:** un programa que se esconde dentro de un programa útil con fines maliciosos se utiliza comúnmente para establecer una puerta trasera para ser explotada por los atacantes.

- **Gusanos:** son programas autónomos que se propagan a través de redes y equipos a menudo, se instalan a través de archivos adjuntos de correo electrónico, enviando una copia de sí mismos a cada contacto de la lista de correo electrónico del equipo infectado.

- **Ransomware:** un tipo de malware que niega el acceso a los datos de las víctimas, amenazando con publicarlos o eliminarlos al menos que se pague un rescate. El software de rescate avanzado utiliza la extorsión criptoviral, cifrando los datos de la víctima para que sea imposible descifrarlos sin la clave de descifrado.

- **Spyware:** un tipo de programa instalado para recopilar información sobre los usuarios, sus sistemas o hábitos de navegación, enviando los datos a un usuario remoto. El atacante puede utilizar la información con fines de chantaje o descargar e instalar otros programas maliciosos desde la Web.

1.1.1.3 Phishing

Se trata de diversas técnicas de ingeniería social con la finalidad de obtener datos privados de la víctima, datos que van desde la suplantación de identidad y obtención de contraseñas de cuentas bancarias. Entre los medios más empleados se encuentran los correos electrónicos, mensajerías o llamadas telefónicas mediante el cual el victimario se hace pasar por alguna entidad conocida, solicitando datos confidenciales para posteriormente emplear dicha información a beneficio propio (Ciberseguridad, 2021)

1.1.1.4 Denegación de Servicio (DOS)

Funcionan inundando sistemas, servidores y/o redes con tráfico para sobrecargar recursos y ancho de banda. Este resultado hace que el sistema sea incapaz de procesar y satisfacer las solicitudes legítimas, los ataques saturan los recursos del sistema con el objetivo de impedir la respuesta a las solicitudes de servicio. (Infocyte, 2021)

1.1.1.5 Inyecciones SQL

Esto ocurre cuando un atacante inserta código malicioso en un servidor utilizando el lenguaje de consulta del servidor (SQL), forzando al servidor a entregar información protegida. Este tipo de ataque suele consistir en enviar código malicioso a un comentario o cuadro de búsqueda del sitio web no protegido. Las prácticas de codificación segura, como el uso de sentencias preparadas con consultas parametrizadas, son una forma eficaz de evitar las inyecciones de SQL. (Shaumik , 2020)

1.1.1.6 Rootkits

Se instalan dentro de un software legítimo, donde pueden obtener control remoto y acceso a nivel de administración a través de un sistema, el atacante lo utiliza para robar contraseñas, claves, credenciales y recuperar datos críticos. Dado que los rootkits se esconden en software legítimo, una vez que permite que el programa realice cambios en su sistema operativo, se instala en el sistema y permanece inactivo hasta que el atacante lo activa o se activa a través de un mecanismo de persistencia. Los rootkits se propagan normalmente a través de archivos adjuntos de correo electrónico y descargas de sitios web inseguros. (Infocyte, 2021)

Respecto al criterio de Bello E, (2021) considera los ataques informáticos suelen ser de naturaleza diversa pero su objetivo radica en dañar, alterar y destruir tanto a las personas como a las organizaciones debido a que además de anular los servicios informáticos pueden robar los datos o a su vez usarlos para espiar, esto se debe a que vivimos en una era digital por lo que los atacantes cibernéticos

han optado emplear estos mecanismos o herramientas tecnológicas para delinquir por lo que su clasificación es variada las más comunes pueden ser categorizadas en tres categorías la primera de ella es denominada Phishing attacks, la segunda es denominada Malware attacks y la tercera y última categoría Web attacks cada una de estas categorías se integran por subcategorías que se presentan en el recuadro:

TIPOS DE ATAQUES INFORMÁTICOS		
Phishing attacks	**Phishing**	Ingeniería social empleada, para robar datos del usuario
	SPEARS PHISHING	Ataques informáticos que tienen como objetivo una persona o empleado específico de una compañía en concreto
	WHALING	Se centran en un perfil de alto directivo, el objetivo es robar información vital y confidencial de una empresa
Malware attacks	**RANSOMWARE O SECUESTRO DE DATOS**	Software malicioso que, al penetrar en nuestro, le otorga al hacker la capacidad de bloquear un dispositivo desde una ubicación remota
Web attacks	**DESCARGAS AUTOMÁTICAS**	Propagan Malware, los ciberdelincuentes buscan páginas web inseguras y plantan un script malicioso, en el código HTTP o PHP este script puede instalar Malware directamente en el dispositivo del usuario, que visite el sitio.

Tabla 1Ataques informáticos

1.1.1.7 Clasificación de los ataques informáticos

Su clasificación suele ser muy variada, pero estos se suelen agrupar en tres categorías la primera de ella es el phishing la cual se enmarca en una persona especifica con la finalidad de robar sus datos personales, la segunda modalidad es la del malware que consiste en un programa o código que se instala en el sistema informático, asumiendo el control sin que la empresa sea consciente de ello y por ultimo están los ataques en la web que se basan en códigos que se infiltran en páginas o navegadores para dañarlos. Cabe destacar que dentro de cada uno de estos ataques existen varias modalidades entre la cuales se pueden examinar las siguientes (SAP España, 2020):

- Spears Phishing (ciberataque a empleados)
- Whaling (robo de información a altos directivos)
- Ransomware (pérdida de control sobre sus dispositivos)
- Spyware (Robo de datos personales e íntimos)
- Troyano (medio de transmisión de virus para espiar, robar y controlar)
- Inyección SQL (Ataques a servidores de las empresas)
- Denegación de Servicios (Satura el servidor hasta inutilizarlo)

1.1.1.8 Fases de los ataques informáticos

De acuerdo con el criterio del conjunto de analistas Lockheed Martin Corporación las fases de los ataques informáticos empieza con el reconocimiento es decir la recolección de la información para hallar sus puntos débiles posterior a ello se empieza con el proceso de preparación en el cual se puede añadir un malware que va dirigido al objetivo, seguido de la distribución en el cual los cibercriminales lanzan el malware u otro tipo de ataque al objetivo con la finalidad de obtener datos, además del proceso de la explotación se puede apreciar la instalación

finalizando con el comando y control en donde el atacante puede sustraer información confidencial u alterar y eliminar datos a su favor. Cabe destacar que este proceso no queda allí debido a que el atacante piensa cuál será su siguiente meta. (Nubelia Cloud, 2021)

1.1.1.9 Principales ataques Suscitados en la red social WhatsApp

De acuerdo con la estadística proporcionada por la entidad financiera Banco Pichincha en el año 2020 se logró estimar que en el Ecuador más de 2.000 millones de usuarios en el mundo emplean la denominada red Social WhatsApp ya sea para uso personal o laboral de acuerdo con el criterio de cada usuario Debido a que su nivel de popularidad sea incrementado considerablemente, los delincuentes informáticos han encontrado una vía de acceso fácil y gratuita que les permitan manipular el nivel de información compartida por esta red, a través de la suplantación de identidad, envió de mensajes y links dañados, acceso a información privada entre otros con la finalidad de poder sacarle algún tipo de beneficio económico al victimario. (Banco Pichincha, 2021)

Aunque puedan existir millones de riesgos y vulnerabilidades como lo manifiesta la página del banco de Pichincha se puede determinar que existen riesgos que dependen directamente de la aplicación como a su vez también existen otros que están debidamente relacionados con el usuario es por esta razón que para evitar ser víctima de algún ciberdelito es esencial que el usuario sea consciente de sus actos y verifique si la información que se recibe proviene de fuentes confiables antes de proceder a abrir dicha información o compartir datos personalmente privados que puedan afectar su integridad física y económica.

1.1.1.10 Smishing

De acuerdo con el criterio emitido por la plataforma Incibe (2020), es considerado como otro ataque de ingeniería social del cual el usuario puede convertirse en victima a través de la red social de WhatsApp, este se produce mediante el envío de un mensaje de texto, consiste en suplantar a una empresa de confianza y solicitar datos sensibles o confidenciales a fin de solucionar el inconveniente

suscitado, entregar un premio o a su vez ofrecer un descuento por su compra, aunque también existe la posibilidad de adjuntar un link a un sitio web falso manejado por los ciberdelincuentes a fin de extraer información y acceder a las cuentas bancarias del victimario.

1.1.1.11 Extorción y suplantación de identidad

De acuerdo con el Banco Pichincha (2021) .Este ataque es generado debido a las brechas de seguridad que se producen en el ambiente digital, en esta situación WhatsApp, permite el acceso no autorizado, robo y secuestro de la información de la víctima, generando como consecuencias negativas la extorsión y suplantación de la identidad en donde el atacante mediante engaños e intimidación obliga al usuario a entregar credenciales o dinero, es por esta razón que entre las forma más comunes que emplean los ciberdelincuentes se pueden determinar las siguientes:

- Se hacen pasar por un conocido que pide apoyo para recuperar mercancías en la aduana.
- Suplantan la identidad de un familiar o amigo para solicitar ayuda para recuperar maletas durante un viaje y obtener dinero.
- Se hacen pasar por un familiar que erróneamente ha solicitado el envío de una clave al número celular de la víctima. Si esta le envía el código, el atacante obtiene el historial de conversaciones y archivos de WhatsApp, entre los que puede haber credenciales y cuentas bancarias.
- Contactan a la víctima y piden una recompensa en dinero a cambio de fotografías y videos privados que han sido secuestrados.
- Suplantan la identidad de una empresa de confianza con la que la víctima tiene relación, para cobrarle una deuda ficticia y presionarla a desembolsar dinero.

- Suplantan la identidad de un asesor financiero solicitando la actualización de datos y así apoderarse de las cuentas bancarias de la víctima.

1.1.1.12 Ataques desde redes publicas

El problema de navegar en internet a través de una conexión de redes públicas desde el dispositivo móvil o computador se debe a que este tipo de redes no pueden cifrar la información que se trasmite con cada clic o mensaje que envíes, así que en consecuencia cualquier persona con habilidades de hacker podría tener acceso total a los datos personales. Cabe destacar que este problema no es propio de WhatsApp, el usuario si puede ser vulnerado al usar redes públicas debido a que el ataque del intermediario o man in the middle el delincuente puede interceptar toda la información que se genera en internet para usarla a su favor por lo que es aconsejable no emplear el acceso a una red pública y en el caso extremo que te conectes a una lo esencial es no abrir WhatsApp.

1.1.1.13 Robos de mensajes y respaldos

Esta modalidad se genera en el instante en que por alguna situación el usuario realiza compras vía WhatsApp entregando datos confidenciales de su tarjeta de débito o crédito o a su vez le haya proporcionado esta información a algún familiar de su confianza para que este realice alguna transferencia cuando el propietario no pueda realizarla ,como consecuencia cualquiera con los conocimientos esenciales puede acceder a la información que supuestamente ya no existía, por otra parte los respaldos de WhatsApp más que una ayuda también significan un peligro debido a que por medio del acceso del correo electrónico el delincuente puede recuperarlos y emplearlos a su conveniencia. (Banco Pichincha, 2021)

1.1.1.14 QRL Jacking (Quick Response Code Login Jacking)

De acuerdo con Dodda, (2021) este tipo de ataque de ingeniería social se basa en la vulneración de los códigos QR generados por las aplicaciones moviles, para ofrecer funcionalidades a los usuarios, en el caso de la aplicación de WhatsApp esta emplea el código QRL para el inicio de sesión en el portal de

WhatsApp Web, este código es denominado una suerte de imagen que almacena de forma privada varios códigos encriptados que no son visibles para los usuarios. Además, este funciona como un código de barras, de esos que vemos en los empaques de productos y que también almacenan información.

Es por este motivo que los ciberdelincuentes toman la imagen del código QR que entrega la aplicación para acceder a WhatsApp Web y colocan un nuevo código encriptado creado por ellos**.** De esta manera, cuando el usuario inicia sesión**,** el atacante ya ha almacenado sus datos de acceso. A partir de ahí, podrá usar la cuenta de la víctima**.** Todas sus conversaciones, fotografías, imágenes y videos que hayan sido enviados por este canal estarán en sus manos.

1.1.1.15 Pagos sin cifrado de extremo a extremo

En algunos países, WhatsApp tiene habilitada la opción de pagos directos desde la aplicación y, aunque de momento esa funcionalidad no está activa en Ecuador, te adelantamos información sobre este tipo de riesgo de ciberseguridad. Partiendo del cifrado de extremo a extremo que WhatsApp aplicó en todas las conversaciones, este es un sistema de comunicación que encripta los mensajes, permitiendo que solo el emisor y el receptor puedan verlos. Este método de seguridad básicamente garantiza que no seas víctima de un *ataque* man-in-the-middle. (Banco Pichincha, 2021)

Según el apartado de seguridad del sitio web oficial de WhatsApp*,* la función de pagos permite a los usuarios hacer transferencias entre cuentas de bancos y otras instituciones financieras. A pesar de que los datos sensibles**,** como números de tarjetas y cuentas se cifran y almacenan en una red de seguridad, estos no pueden ser cifrados de extremo a extremo porque las entidades bancarias necesitan acceder a esta información para procesar las transacciones, generando vulnerabilidad al usuario debido a que por esta brecha el ciberdelincuente podrá introducirse y sustraer información empleándola a su favor.

1.1.1.16 Riesgos de seguridad en red social WhatsApp para los negocios

La red social WhatsApp se ha convertido en una herramienta indispensable tan to de forma personal como para la mayoría de las organizaciones, por esta razón para la mayoría de estas organizaciones el uso de esta red es fundamental para lograr el éxito en relación a la atención del servicio de sus clientes y la aplicación del marketing empresarial, y no aprovechar el correcto uso de esta aplicación podría poner en riesgo la participación de las partes interesadas y la oportunidad de ingresar a nuevos mercados o adaptarse al cambio sin quedarse rezagados con el fin de evitar su quiebra (Russell, 2020)

Es por esta sencilla razón que, al emplear esta red social en el ámbito empresarial, se debe ser consciente que, aunque esta aplicación posee beneficios, también puede generar consecuencias adversas si no se la emplea de forma correcta, lo que generaría poner en riesgo su reputación y el riesgo de la información de la organización y de sus clientes. Cabe destacar que entre los factores de riesgos que pueden presentarse en la aplicación se pueden determinar los siguientes:

1.1.1.16.1 Error humano

El desconocimiento humano al emplear una aplicación o ignorar las consecuencias, que puede generar el indebido uso de la aplicación puede ocasionar que la organización o el mismo sea una potencial víctima de los ciberdelincuentes debido a que a través de la brecha abierta generada por el desconocimiento pueden enviarle links o correos dañidos a los que el usuario accede sin antes verificar la fuente de la información y su confiabilidad, además de aquello el usuario podría enviar información privada y confidencial al receptor sin sospechar que a través de los enlaces o vínculos que el por desconocimiento abrió género que terceros tuvieran acceso a dicha información que podrá ser empleada por el hacker con fines maliciosos (Russell, 2020)

1.1.1.16.2 No prestar la adecuada atención a las redes sociales

Este factor se encuentra estrechamente relacionado con el error humano, debido a que al no prestar la atención adecuada a la cuenta puede ocasionar graves consecuencia, entre la que destaca la infección de los equipos a través de un virus malicioso que podría esparcirse a los demás sistemas, tanto de la organización como la de los usuarios, generando como consecuencia negativa que la organización no sea un ente confiable perdiendo su cartera de clientes o usuarios. (María Sicilia, 2021)

1.1.1.16.3 Aplicaciones y ataques maliciosos

Cabe destacar que el internet suele estar plagado de software maliciosos los cuales suelen abarcar programas maliciosos y de publicidad, además de la variedad de Ransomware, los cuales son considerados como ataques informáticos sofisticados debido a que a través de archivos adjuntos de correo electrónico incrustaban códigos maliciosos en los archivos de imágenes, que cuando el usuario se dispondría a abrir, esta le pondría una restricción total de todos los archivos de su ordenador, para posteriormente generar una ventana mínima en la cual se manifestaba que el usuario tendría que pagar de forma obligatoria la cantidad demandada por el ciberdelincuente, el cual una vez realizado el pago enviaría una clave para que pueda desbloquear los archivos y uso del ordenador. (TALLEDO SAN MIGUEL)

1.1.1.16.4 Fraude de suplantación de identidad

En un mundo globalizado digitalmente no solo los ciberdelincuentes emplearan aplicaciones maliciosas para cometer fraudes, sino que también suelen recurrir a la suplantación de identidad ya se dé una organización o de una persona en específico, este técnica de ingeniería social es empleada a fin de engañar a las personas para que estas brinden información confidencial y privada al solicitante, haciéndoles creer que la información que se les está pidiendo es para poder agilizar el trámite o para tener un mayor control de seguridad en los servicios que la empresa le esté proporcionando, o a su vez también por este mecanismo el

atacante suele enviar enlaces o vínculos a los usuarios diciéndoles que por favor ingresen y llenen una encuesta, de la organización.

Generando que al ingresar el victimario este de manera indirecta este permitiendo el acceso de su ordenador al abrir dicho vinculo o enlace se descarga de manera automática una extensión maliciosa del navegador, que tiene como fin extraer los datos personales de la víctima para emplear dicha información sustraída con fines maliciosos o lucrativos. (Immaculada Barral Viñals).

1.2 Seguridad, solución y prevención

1.2.1 Definición de medidas de prevención y seguridad informática

El robo de información en las empresas han aumentado considerablemente en un 46% y en la mayoría de los casos este problema de fugas suele ser interno causando la preocupación en los dueños, inversionistas, directores y colaboradores por lo que es esencial emplear medidas de seguridad informática para salvaguardar los datos de la entidad, entre las medidas de prevención más factibles que deben considerar es la sensibilización y capacitación de los empleados, creación de copias de seguridad de toda la información relevante, servidor propio, instalación de antivirus y spam, cifrar información, establecer contraseñas y la creación de un plan de contingencias con la finalidad de proteger la información (Castro, 2019).

De acuerdo con el criterio emitido por el Centro Europeo de Postgrado (2021) considera que las medidas de seguridad son acciones dirigidas a proteger la integridad, confidencialidad, disponibilidad y seguridad de los datos almacenados de forma digital, aunque no se tenga conciencia de la cantidad de información o datos que se manejan por medio de herramientas tecnológicas se debe optar por emplear una serie de medidas con el fin de proteger la información que será almacenada en los dispositivos tecnológicos, estos datos suelen estar representados en forma de historial, información bancaria y un sin

números de datos confidenciales que pueden ser alterados, borrados o modificados por los hackers sin que se pueda percatar de lo sucedido.

1.2.2 Definición de la aplicación de WhatsApp

Es una aplicación de mensajería que puede utilizarse en un dispositivo móvil o computador, y tiene por finalidad contactar a las personas por medio del envío de mensajes de texto, llamadas y contenido visual, su funcionamiento es instantáneo permitiendo que los mensajes se reciban y se envíen de manera rápida y directa. (Cao, 2018).

Dioses J, (2020) considera que WhatsApp es una famosa aplicación de mensajería instantánea que se utiliza para enviar y recibir mensajes a través de una conexión a internet. En enero de 2015, esta herramienta decidió ampliar su universo de utilización hasta los dispositivos de escritorio, por lo que le dio la bienvenida a WhatsApp Web. Esta novedosa función puede ser ejecutada si se cuenta con una versión igual o posterior a la 2.11.498 instalada en el teléfono y con el navegador Google Chrome, Firefox u Opera funcionando en la PC. A través del simple escaneo de un código QR, la aplicación puede ser abierta desde el smartphone y configurada para que se sincronice con el ordenador.

1.2.3 Importancia de los mecanismos de protección informática

La seguridad de la información es vital es por este motivo que los mecanismos empleados son esenciales debido a que ayudara a suprimir riesgo y amenazas que no se logran a identificar a simple vista, es por ello que su importancia radica en salvaguardar los documentos o datos con la finalidad de evitar el robo de la información y evitarle al usuario pérdidas económicas al protegerlo de cualquier ataque generando seguridad y confianza en el usuario evitando que este sea vulnerable ante los cyber-delincuentes (Muñoz , 2020)

La importancia de la seguridad informática de las empresas radica esencialmente en que la utilización maliciosa de sus sistemas de información privados, y de los recursos internos puede acarrear desastrosas consecuencias

en todas las áreas de la organización, generando problemas tanto productivos como financieros. Por ende, la seguridad informática de las empresas debe estar dirigida a prevenir las amenazas y los riesgos a los sistemas de información internos.es por esta razón que se concluyó, que para la existencia de una correcta seguridad de información en las empresas se debe contar con el personal experto en tecnologías informáticas capaces de predecir dichas amenazas y riesgos.

1.2.4 Importancia de la aplicación de WhatsApp en la empresa

La importancia que tiene el uso de la aplicación de WhatsApp en las empresas es vital debido a que por medio de esta, ayuda a las empresas a interactuar con sus clientes de manera directa y sencilla de forma gratuita, el poder que tiene WhatsApp es descomunal debido a que por medio de ella no solo se podrá contactar con los clientes, colaboradores y demás usuarios que la empresa considere necesarios, sino que también les permite poder crear marketing digital las 24/7 recayendo su importancia en la factibilidad, accesibilidad y rentabilidad para la empresa, es por ello que es crucial que en las empresas se maneje con cuidado los datos compartidos que pueden ser sustraídos, por los atacantes informáticos para beneficios propios por lo que es importante tomar medidas de seguridad. (Agencia Digital Costa Rica, 2018).

1.2.5 Clasificación de los tipos de seguridad informática

Aunque su clasificación suele ser variada coma por lo general se integra de tres componentes del hardware como software y redes. El hardware está destinado a garantizar la protección del equipo, el software está destinado a ejecutar medidas que prevengan cualquier ruptura en el sistema y finalmente la protección de redes coma que consiste en establecer filtros que protejan a los equipos y la información que almacenan y transmiten antes de que pudieran acceder al sistema. (AVANSIS, 2021)

1.2.6 Clasificación de los mecanismos de seguridad informática

Existen varios mecanismos de seguridad entre los cuales se puede determinar los preventivos el cual consiste en prevenir la ocurrencia de un ataque informático, por su parte los mecanismos correctivos son los encargados de reparar los errores cometidos o causados por algún tipo de ataque modificando el sistema restaurándolo a su estado original, los mecanismos disuasivos se encargan de desanimar a los atacantes a que cometan dicho ataque y finalmente los detectores que se encargan de determinar todo aquello que pueda ser una amenaza para los bienes. (Castro R. , 2020)

1.2.7 Configuración de privacidad

El factor de configuración de la privacidad debe ser esencial en las organizaciones que emplean la red Social WhatsApp, debido a que si la organización emplea este mecanismo de protección estarán menos expuesta de convertirse en una víctima más por parte de los ciberdelincuentes que buscan de alguna forma ingresar a los sistemas de las entidades, irrumpir el sistema y dañar de manera íntegra la reputación de las empresas.

Aunque este mecanismo debe ser prioritario la mayoría de las entidades siguen poniendo en juego su reputación empresarial, debido que al no poseer una política de restricción de privacidad generan como resultado que los hackers accedan fácilmente a los canales sociales de la empresa, enviando publicaciones fraudulentas a sus clientes o usuarios además de realizar modificaciones de la apariencia de la marca empresarial, cabe destacar que la mayoría de las marcas empresarial se han convertido en víctima de los hacker como fue el caso de la reconocida marca de Burger King, cuya cuenta de Twitter fue secuestrada e hicieron parecer que promocionaba a McDonald’s., esto debido a que no administro de forma correcta el uso de privacidad de la aplicación. (Perez J. , El debate sobre la privacidad y seguridad en la red: regulación y mercados, 2021)

1.2.8 instalación de firewall o cortafuegos

Un firewall, también llamado cortafuegos, es un sistema cuya función es prevenir y proteger a nuestra red privada, de intrusiones o ataques de otras redes, bloqueándole el acceso, permite el tráfico entrante y saliente que hay entre redes u ordenadores de una misma red. Si este tráfico cumple con las reglas previamente especificadas podrá acceder y salir de la red, si no las cumple este tráfico es bloqueado. De esta manera se impide que usuarios no autorizados accedan a redes privadas conectadas a internet además este se puede implementar en forma de hardware, de software o en una combinación de ambos. (GIPGRUP, 2020).

1.2.9 Bloqueo con huella dactilar

Esta opción de seguridad introducida en el 2019 permite al usuario bloquear el acceso al chat a través de la huella del propietario del dispositivo móvil de forma general, para poder activar este mecanismo de seguridad se debe seguir pasos simples como acceder a la aplicación de allí se selecciona los tres puntitos de la parte superior y se da click en ajustes, de allí en cuenta y después a privacidad para así finalizar activando la opción de bloqueo por huella dactilar y se debe verifica la huella. Una vez finalizado el proceso de activación la aplicación da la opción de escoger entre el bloqueo inmediato, justo después de salir de la aplicación, después de 1 o 30 minutos de salir de la app, este mecanismo de seguridad tiene como finalidad salvaguardar la integridad de la información en caso de ataques informáticos o pérdida o robo del dispositivo (Collado, 2021).

1.2.10 Verificación en dos pasos

Este mecanismo de seguridad consiste en la activación y generación de un código PIN integrado por seis dígitos los cuales el usuario ha creado, para poder activar este mecanismo se debe abrir WhatsApp entrando a ajustes para allí proceder a buscar la opción de cuenta la cual nos mostrara la opción de verificación en dos pasos y seleccionamos la alternativa activar, adicionalmente

y de forma opcional se podrá ingresar una dirección de correo electrónico valida en caso de querer restaurar el pin de acceso. Cabe destacar que en caso de recibir un correo electrónico sin que el usuario no haya pedido desactivar la verificación en dos pasos lo más recomendable es eliminar el enlace debido a que por este medio los cyber atacantes está intentado verificar tu número móvil para acceder a tus datos e información móvil (Otero, 2018).

1.2.11 Cifrado de extremo a extremo

Se usa cuando envías un mensaje a una persona a través de WhatsApp Messenger, este cifrado garantiza que solo el emisor y el receptor con quien se esté comunicando sean capaces de leer, escuchar o ver el contenido enviado sin que nadie más pueda acceder a ello, asegurando los mensajes con un candado en donde solo el emisor y destinatario poseen la llave para desbloquearlos y leerlos, escucharlos y observarlos. Todo esto es automático, sin que haya necesidad de activar ninguna opción en los ajustes ni de crear chats secretos especiales para asegurar los mensajes. (Alvarez, 2020).

1.2.12 Privacidad de estados perfil y conexión

Este mecanismo de seguridad se enmarca en la seguridad de la información personal, entre las cuales se puede ubicar la privacidad de la foto de perfil de WhatsApp, estados y la hora de ultima conexión. Para cada una de estas opciones se puede seleccionar tres apartados para determinar quién puede acceder a la información personal entre los apartados se puede determinar solo mis contactos, mis contactos excepto y finalmente la opción de nadie. Este proceso se realiza para ver con quien se comparte la información y con quien no, pero a su vez nos podría volver vulnerables. ello por lo que es esencial para la Entidad “ASESORARTE” saber el correcto uso y manejo de la aplicación de WhatsApp y los diferentes ataques a los que se pueden exponer además de las medidas preventivas para salvaguardar los datos y evitar el robo de estos mismos. (Perez J. , 2020).

1. 2.13 Beneficios de proteger la red social WhatsApp

Según el criterio de (Romero, 2021), determina que una vez que se haya asegurado la red social WhatsApp con los mecanismos de protección y privacidad como es el bloqueo con huella dactilar, verificación en dos pasos, cifrado de extremo a extremo entre otros es esencial tener el debido cuidado con los vídeos que se comparten por la red social pese a que WhatsApp posee un sistema de cifrado que evita la intercepción o descifrar conversaciones, los piratas informáticos pueden infiltrarse de otro modo que desconoce. Esto, a través de la infección y pirateo de vídeos reales que, al reproducirlos, toman control del móvil. Es por ello por lo que uno de los mayores beneficios que se obtiene al proteger esta red es que el riesgo de ser hackeado es mínimo o casi nulo además también permitirá con ayuda de los debidos mecanismos de seguridad un desarrollo óptimo de la aplicación y del dispositivo inteligente.

CAPÍTULO II

2 ESTUDIO DE CAMPO

2.1 Metodología de investigación

De acuerdo con el criterio emitido por Vera (2017), se considera que la metodología de la investigación es la que emplea el conjunto de procedimientos y técnicas de manera sistemática, con el fin de poder procesar la información es por este motivo que el investigador debió buscar, analizar y preparar los datos obtenidos que le permitieron validar la información con el fin de haber brindado soluciones a los fines investigativos.

La metodología de investigación se usó con sus técnicas para desarrollar esta investigación. También ayuda con la organización de la investigación y obtener la información necesaria para asi darle fundamentos a dicha investigación.

2.2 Tipos de investigación

2.2.1 Bibliográfica

Cabe destacar que este tipo de investigación se aplicó en la revisión del material bibliográfico referente al tema propuesto de estudio, con el fin de obtener información confiable y veraz de libros, artículos, revistas, documentos de sitio web, periódicos etc. Que, por ende, favorece el enfoque de estudio a los contenidos que se utilizaron en el proyecto de investigación. (Callejas, 2020).

Por lo que se aplicó esta técnica a través de la recolección de fuentes bibliográficas logro determinar los distintos virus informáticos, y las diferentes vías o mecanismos que emplearon los hacker o ciberdelincuentes para sustraer, dañar, alterar y modificar los datos informativos del usuario o víctima, además también se logró determinar los mecanismos de protección informáticas y las medidas preventivas, que se deben tener en cuenta a fin de no ser víctimas de los hacker protegiendo la red social WhatsApp de ataques externos o internos.

2.3 Métodos de investigación

2.3.1 Método Inductivo

El método inductivo se basó en las características genéricas o comunes para obtener conocimiento, es imprescindible observar la naturaleza de lo que se desea explorar, el cual planteo un razonamiento ascendente que fluye de lo particular o individual hasta lo general. Es decir, este método es una reflexión enfocada en el fin, reuniendo datos particulares y luego hacer generalizaciones. Este método inductivo no suele ser muy factible o recomendado para la práctica puesto que este se basó en la observación, sin embargo, si este método es utilizado deberá confiarse en la inducción imperfecta que se basó en observaciones incompletas. (Rodriguez & Perez, 2017).

Por tal motivo este método fue aplicado en la entidad al momento que se decidió recopilar información por la que se obtendría mediante la observación, al momento que se realizó la visita respectiva a la empresa “ASESORARTE”, se pudo determinar si los colaboradores y clientes estaban tomando las respectivas medidas de seguridad, al instante que se realizó el uso de la aplicación de WhatsApp y los riesgos a los que estaban expuestos.

2.3.2 Método deductivo

Por otra parte, en el método deductivo trata de aquella orientación el cual procederá de lo general a lo particular o especifico, este método se dividió en dos particulares el deductivo directo el juicio se obtiene de una sola premisa, es decir, se llegó a una conclusión directa o inmediata sin intermediarios, a diferencia del deductivo indirecto el cual se necesitó de conclusiones lógicas, su argumento consto de tres proposiciones, es decir primero se compararon dos extremos las premisas o términos con un tercero para haber descubierto la relación entre ellos. La premisa mayor contiene la proposición universal, la premisa menor contiene la proposición particular, de su comparación lo que conlleva a la conclusión. (Behar, 2017).

Por esta razón se consideró que el método deductivo que se aplicó a la empresa “ASESORARTE”, permitió descomponer un elemento o información específica, partió desde lo general hasta llegar a lo especifico, a fin de que se pudo hacer la orientación en el proceso investigativo en un correcto desarrollo de la investigación y asi obtener un juicio o criterio acertado.

2.3.3 Método Analítico

El método analítico fue un proceso que requiere de observación constante en cada etapa independientemente de la etapa en la que se encontraron, a su vez, la experimentación es crucial para tener asi la determinación de los comportamientos de la muestra analizada tanto en un proceso como en las diferentes partes que lo componen, este se basa al objeto de una rigurosa investigación documental. (Echeverria, 2019).

Este método fue esencial en el proceso investigativo en la entidad “ASESORARTE”, debido ya que por medio de este el elemento investigativo se analizó la información que proporciono la empresa, en una o varias partes de forma individual, con el fin de haber observado las causas y efectos que se produjeron, para posteriormente poder determinar los mecanismos idóneos que permitieron presentar alternativas viables, las cuales resolvieron problemáticas que fueron suscitadas beneficiando a la organización.

2.4 Técnicas - instrumentos de investigación

2.4.1 Entrevista

Fue una herramienta utilizada para obtener información sobre un tema que se desea conocer o es de interés para un grupo determinado de personas, las cuales se la realizo de manera oral, pueden ser personalizada, o de manera colectiva o grupal, según como amerite el caso, entre las partes que intervienen, está el entrevistado, que se refiere al persona o grupo de personas de las cuales se le preguntara una serie de preguntas subjetivas, con el fin de obtener información de esta fuente y del entrevistador, que es la otra parte que interviene

la encargada de emitir las preguntas a ser respondidas, es una técnica que es muy utilizada para la investigación. (Folgueira, 2019).

La entrevista fue aplicada directamente al gerente de la entidad “Asesorarte”, este mecanismo de investigación fue aplicado con el fin de determinar si tanto el gerente como sus miembros colaboradores, cumplen a cabalidad las políticas empresariales, y si la organización estuvo apta para enfrentarse ante las amenazas presentes en un mundo digitalizado, en donde deberían tomar la medidas correctivas ya que si lo ignoran estarían expuestos a riesgos, que pueden atentar con su integridad física y jurídica.

2.4.2 Encuesta

Es una técnica utilizada para obtener información cuantitativa o en datos numéricos, puesto que la información es transformada en números o en cantidades para ser analizadas sobre un determinado caso, generalmente este tipo de procedimiento de obtención de información es implementado, a través de un cuestionario de preguntas objetivas que buscaron darle un análisis y conclusiones del caso, lo cual toma una población específica y su respectiva muestra. (Diaz, 2019).

Es por esta razón que se procedió a ejecutar la encuesta a la entidad contable de asesoría tributaria “ASESORARTE” se determinó a través de los clientes de la organización a quienes les realizamos dicha encuesta, si la entidad en las que les brindaron el servicio de asesoría tributaria les brindaron las herramientas y mecanismos de seguridad física, integra y digital, con el fin de que el cliente se sintió seguro, y depósito su confianza con la seguridad de saber que su información se respaldó bajo mecanismos de protección informática, con el fin de no ser víctimas de los hacker o ciberdelincuentes que pueden sustraer dicha información con fines maliciosos.

2.5 Población y muestra

2.5.1 Población

La población en investigación es un conjunto completo de elementos que poseen un parámetro común entre sí. Es de suma importancia dar a conocer que todos son conscientes de que quiere decir población pues significa vida diaria. Es utilizada para describir cierto número de personas que viven en un área geográfica ya sea de un país o estado. (M.Gomez, 2019).

La población que se utilizará para esta investigación son los 450 clientes de la empresa los cuales van a apoyar con la investigación al momento de la realización de una encuesta.

2.5.2 Muestra

La muestra es una pequeña parte de todas las personas, es decir, un pequeño subconjunto de todos. Cuando se aplica una encuesta la muestra son las personas de la población.

Dicho de manera sencilla, una muestra es un subgrupo o subconjunto dentro de la población, que puede ser estudiado para investigar las características o el comportamiento de los datos de población. (M.Gomez, 2019).

La muestra que se uso fue la de población finita la cual gracias a los datos obtenidos de la empresa se aplicó y se concluyó que solo a 10 clientes se debía aplicar la encuesta.

Por su parte en relación con la encuesta del total de la población de sus clientes, que es un aproximado de 450 usuarios con un nivel del 80% de confianza y un 20% de error, y con el 50% de la probabilidad de éxito y de el mismo valor la probabilidad de que falle el evento estudiado, se procedió a aplicar los respectivos cuestionarios a un total de 10 personas con el fin de recolectar la información, es por ello por lo que solo 10 clientes fueron objetos de estudio en el desarrollo de la auditoria.

2.5.3 Fórmula aplicada de población finita

$$n=\frac{Z^2 * N * P * Q}{e^2 * N - 1 + Z^2 * P * Q}$$

$$n=\frac{(1.28)^2(450)(0.50)(0.50)}{(0.20)^2(450-1)+(0.28)^2(0.50)(0.50)}$$

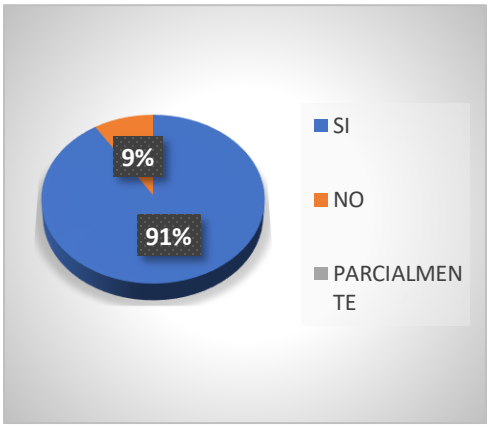
$$n=\frac{(1.64)(450)(0.50)(0.50)}{(0,04)(449)+(1.64)(0.50)(0.50)}=\frac{184.5}{(17.96)+(0.41)}=\frac{184.5}{18.37}=10$$

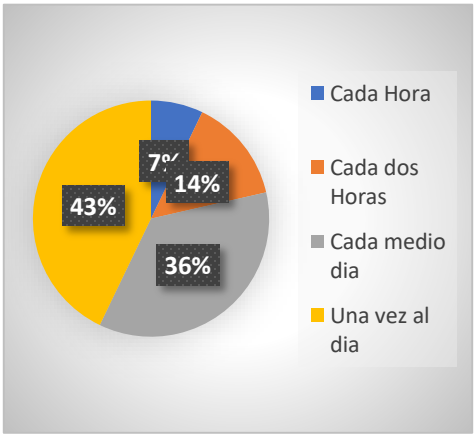
2.5.4 Resultados de la investigación de campo.

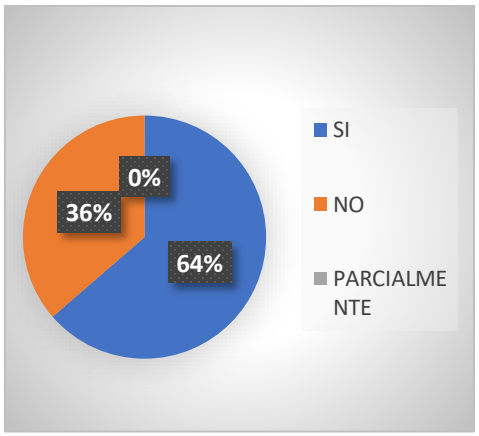
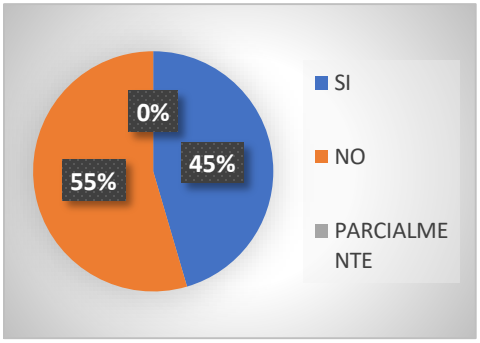
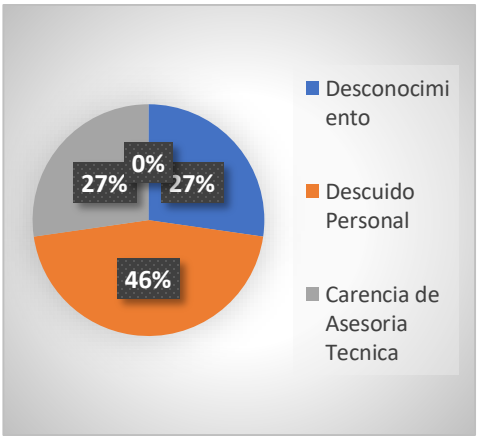
Esta encuesta fue realizada a los clientes de la entidad “ASESORARTE”, quiénes son los que adquieren al servicio de le empresa.

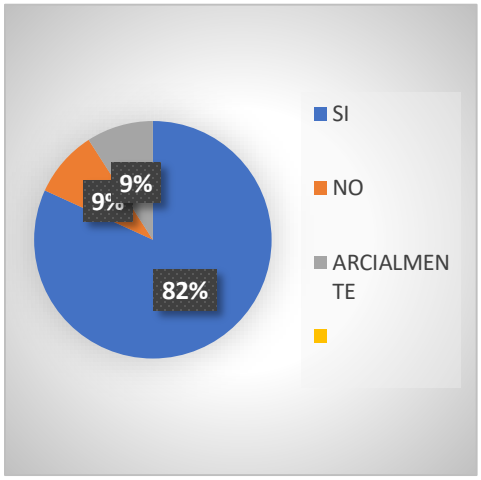
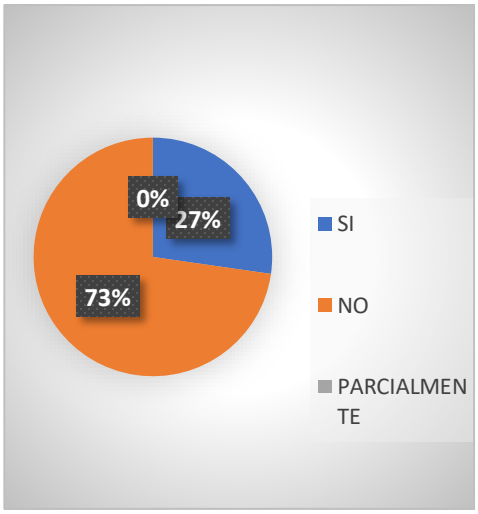
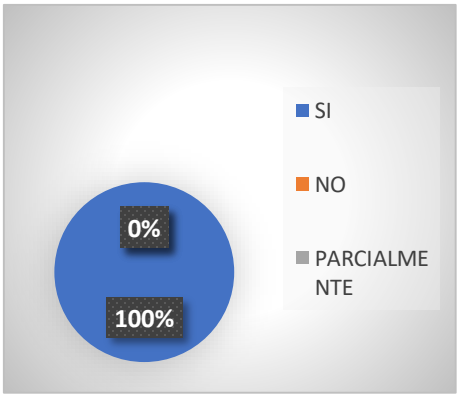
2.6 Tabulación de la encuesta

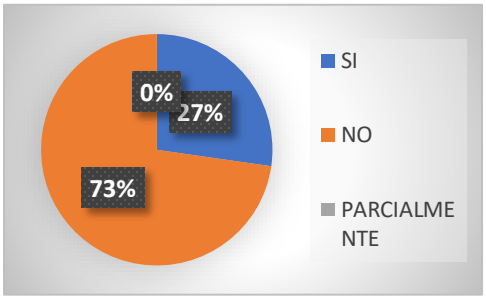
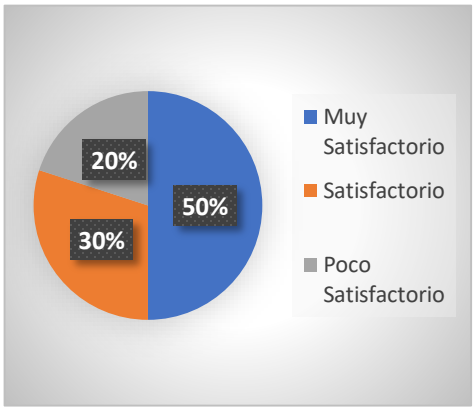
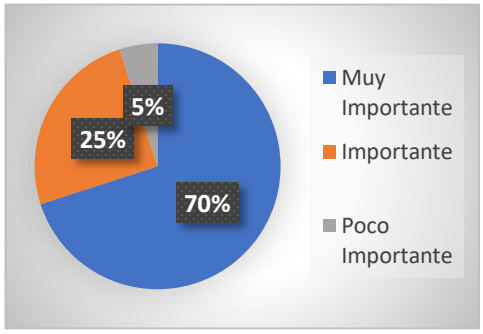
La tabulación de la encuesta fue hecha en la entidad asesorarte aplicada a los clientes que requieren de los servicios de dicha identidad.

Preguntas	Respuestas	Análisis
1. ¿Considera usted que cada miembro o colaborador de la empresa "Asesorarte" emplea la red social de WhatsApp para asuntos laborales y personales?		La mayoría de los clientes afirman que los colaboradores usan la red social de WhatsApp con frecuencia para asuntos laborales, lo cual es un problema, los hackers pueden

		asechar y tener información valiosa.
2. ¿Con qué frecuencia los miembros de la organización emplean la red social de WhatsApp para transmitirle un mensaje en relación con el trámite que este realizando usted como cliente?		De todos los clientes encuestados se concluyó que el cuarenta y tres por ciento opina que para comunicarse con ellos por medio de WhatsApp lo hacen una vez al día. Lo cual sigue siendo preocupante porque cualquier información les sirve a los hackers para atacar a los clientes.
3. ¿Usted tiene el conocimiento		La mayoría de los clientes

acerca de los distintos virus informáticos que pueden existir y que pueden ser manipulados por medios de diversos mecanismos incluyendo la red social de WhatsApp?		concordaron que no tienen ningún conocimiento sobre los virus que existen.
4. ¿Cree usted que los dispositivos electrónicos deben contar con mecanismos de seguridad informática?		La mayoría de los clientes opinan que no necesitan un mecanismo de seguridad para evitar ser víctimas de los ataques.
5. ¿Cuáles cree usted que deben ser los factores para hacernos vulnerables a los ataques informáticos originados por los cyber-delincuentes?		La mayoría de los clientes concluyen que es por descuido personal son vulnerables a los ataques informáticos originados por los ciberdelincuentes.

6. ¿Estaría de acuerdo con la elaboración de una guía metodológica acerca de los ataques informáticos y las medidas preventivas de seguridad de WhatsApp?		La mayoría opina que si debiera existir una guía que les diga cómo protegerse.
7. ¿Piensa qué la elaboración de la guía servirá para conformar directrices integrales de seguridad en el correcto uso y manejo de la aplicación de WhatsApp?		La mayoría considera que si sirviera una guía.
8. ¿Considera esencial una capacitación acerca de los ataques informáticos y mecanismos de protección y prevención de		Todos consideran esencial el proceso de capacitación.

seguridad informática de la red social WhatsApp?		
9. ¿Sus dispositivos inteligentes cuentan con algún tipo de antivirus que le permita contrarrestar los virus informáticos?		La mayoría cuenta que no tienen ningún antivirus que los proteja.
10. ¿Como define usted a la entidad al momento en que le solicita documentos confidenciales por medio de la red social WhatsApp?		La mayoría los define como muy satisfactorio.
11. ¿Qué tan importante cree usted qué es seguridad en los archivos y enlaces enviados por la entidad?		La mayoría opina que es muy importante.

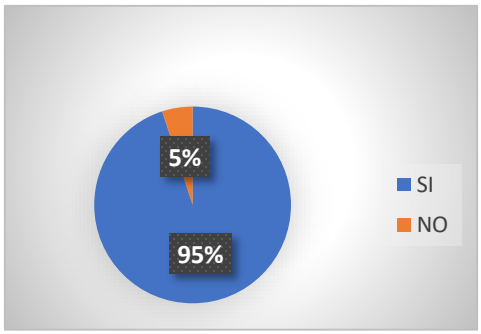
12. ¿Ha sido víctima de algún tipo de ataque informático?		La mayoría han revelado que si han sido víctimas de ataques.

Tabla 2 Tabulación de la encuesta

2.7 Resultados de la entrevista aplicada a el gerente de la empresa "ASESORARTE"

Esta entrevista se le realizó a el Ing. Roddy Ramírez Coordinador general de la empresa de Asesoría contable y tributaria "ASESORARTE" El Carmen Manabí, con el propósito de obtener información y profundizar los resultados obtenidos para la investigación, y como diagnóstico de conocimiento en el área informática.

Preguntas	Respuestas	Análisis
1. ¿Cómo miembro de la organización "ASESORARTE" con qué frecuencia emplea el uso de la red social WhatsApp para comunicarse con sus usuarios?	El gerente manifestó que tanto el cómo sus colaboradores emplean la red social de manera diaria, debido a que por este medio se mantienen de forma permanente comunicados con los clientes, en caso de emplear información o notificarles algún mensaje.	Diariamente usan WhatsApp en la entidad.
2. ¿Suelen compartir información laboral entre los colaboradores de la organización a través de la aplicación de WhatsApp u otros medios?	El propietario también expreso que no solo se comunica con sus colaboradores de manera directa, sino que además emplea esta red social y también existe un grupo de WhatsApp entre los miembros colaboradores de la organización, por el cual se comparte la información o se	Usan WhatsApp para comunicarse entre colaboradores y el gerente de la empresa.

	resuelven inquietudes que se susciten.	
3. ¿A criterio personal conoce a que se le denomina virus informático y cuantos tipos de virus pueden existir?	De acuerdo con lo mencionado por el gerente, el desconoce que es un virus informático y no sabe cuántos virus pueden existir y la manera en que estos pueden llegar a distribuirse.	No tienen conocimiento de que son los virus informáticos.
4. ¿Tiene conocimiento acerca de la privacidad que debe tener al momento de compartir una información por medio de la red social de WhatsApp a fin de que no sea manipulada por ningún ciber-delincuentes o terceros con fines maliciosos?	A pesar de no poseer conocimientos informáticos ni de que es un virus el gerente nos manifestó, que hace todo lo posible por no ser una víctima más de los ciberataques o delitos informáticos.	Tratan de no ser víctimas de estos delincuentes.
5. ¿Cuenta con algún sistema que le ayude a prevenir y proteger sus dispositivos y la	No cuentan con algún sistema de seguridad informática, por lo que se encuentran vulnerables ante la posibilidad de algún ataque informático.	No cuentan con ningún sistema de seguridad informática.

información que puede ser sustraída por parte de los atacantes?		
6. ¿Toma las precauciones necesarias al momento de recibir un mensaje o correo de algún tipo de fuente de origen desconocido?	Si se les notifica un mensaje o correo electrónico de fuentes que desconocen tanto a el gerente como sus colaboradores tienen como política no abrir el mensaje o en lace hasta verificar su fuente.	Toma sus precauciones necesarias.
7. ¿A criterio personal contrataría los servicios de un asesor informático que le brinde información de cómo proteger sus datos?	El gerente considero fundamental contratar los servicios de algún asesor informático, a fin de que este lo oriente y le ayude a proteger la información de los ciberdelincuentes y los capacite en este ámbito tanto a los colaboradores como a sus usuarios.	Piensan que es necesario los servicios de un asesor informatico.
8. ¿Compartiría la información de la guía creada con sus clientes a fin de proteger la integridad de sus usuarios?	Considero que una vez culminada la guía lo esencial seria compartir dichos documentos, con el fin de que tanto los colaboradores como los clientes empleen de manera correcta la aplicación y conozcan las amenazas a las que pueden estar expuestos, si no toman las medidas preventivas idóneas.	Si compartiera la guía.

9. ¿Brindarían el apoyo y recursos necesario para la estructuración y elaboración de la guía de ataques informáticos y las medidas preventivas de seguridad a la red social WhatsApp?	El gerente y sus colaboradores están dispuestos a brindar toda la ayuda y mecanismos necesarios para la elaboración y diseño de la guía metodológica, acerca de los ataques informáticos y las medidas preventivas de seguridad en la red social WhatsApp.	Si apoyaran a la elaboración de la guía.
10. ¿Conoce los pasos que se deben realizar en caso de sufrir un ataque informático?	Supo manifestar que desconoce que acciones seguir en caso de sufrir un ataque informático	No conoce los pasos a seguir en caso de ser atacado.
11. ¿El personal de la empresa y usted han recibido capacitación acerca de los mecanismos de seguridad y distintos ataques que pueden ser ejecutados a través de la red social WhatsApp?	Hasta el momento no han recibido ningún tipo de capacitación en relación con los ataques informáticos y las medidas preventivas y de seguridad informática. Pero que estaría dispuesto a recibir una capacitación para protegerse de los ataques y por ende incluir mecanismo de seguridad en WhatsApp para no sufrir ningún ataque	No han tenido capacitación acerca de los ataques informáticos que puede afectar a la red de WhatsApp
12. ¿La empresa ha sido afectada por	A lo largo de la historia de vida de la organización no han sido víctimas de los ciberdelincuentes,	hasta el momento la empresa no ha llegado a ser

un ataque informático? .	por lo que se considera que no han sufrido ningún tipo de ciberataque.	afectada por ciberdelincuentes.

Tabla 3 Resultados de la entrevista aplicada a el gerente de la empresa "ASESORARTE"

2.7 Triangulación de resultados análisis

2.7.1 Análisis de resultados

En la encuesta la pregunta 1 la mayoría de los clientes afirman que los colaboradores usan la red social de WhatsApp con frecuencia para asuntos laborales, Por lo que el gerente manifestó que en la pregunta 2 de la entrevista que no solo se comunica con sus colaboradores de manera directa, sino que además emplea esta red social y también existe un grupo de WhatsApp entre los miembros colaboradores de la organización, por el cual se comparten información por lo que si usan WhatsApp para asuntos laborales.

En la pregunta 8 todos consideran esencial el proceso de capacitación por lo que el gerente manifestó en la pregunta 7 que fundamental contratar los servicios de algún asesor informático, a fin de que este lo oriente y le ayude a proteger la información de los ciberdelincuentes y los capacite en este ámbito tanto a los colaboradores como a sus usuarios, por lo que todos están de acuerdo con una capacitación

En la pregunta 6 de la encuesta la mayoría opina que si debiera existir una guía que les diga cómo protegerse y en la pregunto 8 de la entrevista el gerente Considero que una vez culminada la guía lo esencial seria compartir dichos documentos, con el fin de que tanto los colaboradores como los clientes empleen de manera correcta la aplicación y conozcan las amenazas a las que pueden estar expuestos, si no toman las medidas preventivas necesarias por lo que creen necesaria la guía.

CAPÍTULO III

3. La propuesta

3.1 Desarrollo de la propuesta

El desarrollo de la propuesta se basó en el riesgo y vulnerabilidad de compartir datos tanto personales como laborales, por medio de la red social WhatsApp, donde existen riesgos que involucran tanto a los colaboradores como a los clientes, de la entidad “Asesorarte”. Debido a él desconocimiento de los colaboradores clientes y el gerente de la empresa acerca de los virus informáticos que pueden introducir los ciberdelincuentes para poder llevar a cabo su plan de hurto de tanto datos personales como laborales.

Por esta razón se propone diseñar una guía digital acerca de los ataques informáticos que pueden suceder en la empresa por medio de populares y diversos virus y pues así también la guía contara con las prevenciones necesaria para evitar caer en las manos de los ciberdelincuentes.

3.2 Alcance

Unos de los elementos importantes en dicha investigación es la aplicación de la red social WhatsApp, y conocer los virus más utilizados los cuales pueden afectar a WhatsApp. Pues es la red social más utilizada hoy en día. Al conocer e informarse del virus se puede también conocer las prevenciones.

Para cuidar y resguardar información personal y los dispositivos electrónicos. Con esta información es decir al conocer las vulnerabilidades de WhatsApp, así como los virus y las prevenciones podemos iniciar a crear una guía digital para darle a conocer a los usuarios riesgos y vulnerabilidades de las cuales pueden ser víctimas.

3.3 Objetivos

3.3.1 Objetivo General

Crear una guía digital mediante análisis, y conocimiento de virus y los ataques informáticos que pueden suceder, en la red social de WhatsApp en la entidad. “Asesorarte”.

3.3.2 Objetivos específicos

- Establecer reglas de seguridad para evitar ser víctimas de estos ataques.
- Analizar las fallas que pueden tener la red social de WhatsApp al momento de usarla.
- Implementar los mecanismos de seguridad para WhatsApp.

3.4 Antecedentes

3.4.1 Reseña histórica

La empresa surge a partir de una necesidad suscitada al ingeniero Roddy Rubén Ramírez Loor, quien se encontraba incorporado como ingeniero y no encontraba alguna fuente de ingresos o trabajo, por lo que decide ponerse en contacto con la ingeniera Erika Isabel Estrada Vélez, manifestándole que si ella estuviese dispuesta en conjunto ubicar una empresa de asesoría tributaria y laboral.

Dando como resultado que el día 01 de enero del año 2014 se creara la empresa de Asesoría Contable y tributaria “ASESORARTE”, creada con el fin de brindar un servicio asesor a la comunidad carmense en relación con temas tributarios y de aspecto jurídico a fin de que las personas eviten ser sancionadas, multadas

y el cese o cierre de sus negocios por no pagar sus tributos a tiempo. Poco a poco la organización fue ganando fama y prestigio además de ir incorporando a más colaboradores hasta no solo ser una empresa de asesoría en materia tributaria, sino que también puedan ayudar a sus clientes a realizar cualquier tipo de trámites que se requieran.

3.4.2 Misión

Todo lo que queremos podemos, lo hacemos y lo gestionamos.

3.4.3 Visión

Ser una empresa eficaz y líder en materia de asesoría tributaria, brindando todas las herramientas, mecanismos e información vital a nuestros usuarios y colaboradores, logrando expandirnos hacia nuevas provincias, siendo íntegros y responsables con nuestro trabajo.

3.4.4 Datos informativos del personal de la empresa

Nombres: Roddy Rubén

Apellidos: Loor Ramírez

Cel:0992460369

Domicilio: Operativa. San Luis cajones

Cargo: presidente

Correo: **roddy_ramirezloor@hotmail.com**

Nombres: Erika Isabel

Apellidos: Estrada Vélez

Cel:0991485463

Domicilio: 18 de octubre y Carlos Alberto Aray

Cargo: Gerente

Correo: **eres_1983@hotmail.com**

Nombres: Vanessa Roxana

Apellidos: Párraga Marcillo

Cel:0991819910

Domicilio: Unión popular

Cargo: secretaria

Correo: **rox_par13@hotmail.com**

Nombres: Gisella Carolina

Apellidos: Muñoz Vera

Cel:0994697726

Domicilio: Km34 vía a sumita pita

Cargo: Asesor inmobiliario

Correo: **jicamuve_1994@hotmail.com**

Nombres: María Fernanda

Apellidos: Zambrano Bazurto

Cel:0990025329

Domicilio: Av. La Esperanza

Cargo: Asesor laboral

Correo: **jicamuve_1994@hotmail.com**

Nombres: Adolfo Polivio

Apellidos: Loor Castillo

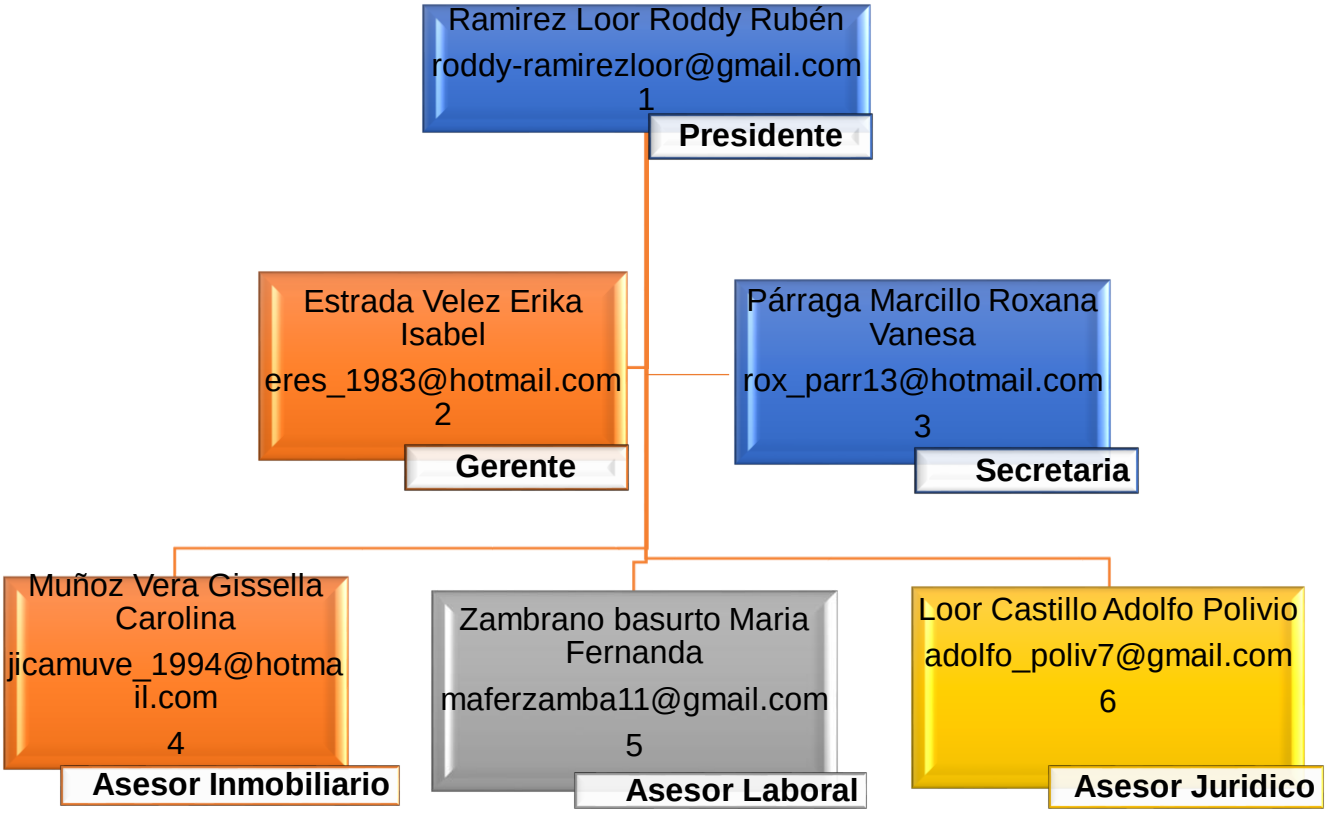
Cel:0997208789

Domicilio: 18 de octubre y Víctor Astudillo

Cargo: Asesor jurídico

Correo: **adolfo_poliv7@gmail.com**

3.4.5 Estructura empresarial



3.4.6 Objetivos de la empresa “ASESORARTE”

- Cumplir con los propósitos del cliente.
- Dar confianza y seguridad de los servicios profesionales brindados en la asesoría.
- Hacer crecer finalmente bajo asesoramiento al cliente.

3.4.7 Historia de la empresa “ASESORARTE”

El primero de enero del 2014 fue creada la oficina contable tributaria y laboral asesorable bajo la perspectiva de dar servicios y asesoramiento a la ciudadanía El Carmen bajo el profesionalismo del Mg. Roddy Ramírez Loor y la Ing. Erika Vélez Hasta la actualidad. Aumentarle a la historia

Es así como a medida transcurría del tiempo, “ASESORARTE” ha logrado obtener experiencias en cuanto a la administración de entidades, clientes locales etc. Basando sus métodos en el entendimiento del negocio u oficio del cliente y el análisis de peligros, para así imaginar y realizar las inspecciones que más se ajusten a su necesidad y que le ayuden aminorar, buscando siempre un ambiente de cercanía y confianza con nuestros clientes con una asesoría de calidad y trasparencia.

3.4.8 Tipos de ataques informáticos y sus soluciones

Existen varios tipos de ataques informáticos entre los más comunes y populares están:

- **Phishing**

  Lo primordial en phishing es hurtar cierta información como datos de la víctima y lo logran utilizando la “confianza”, a través de, el engaño es decir se hace pasar por una persona de confianza.

El atacante envía una comunicación dirigida con el fin de persuadir a la víctima para que haga clic en un enlace, descargue un archivo adjunto o envíe una información solicitada, o incluso para que complete un pago. (Ramos, 2022)

Solución

Para protegerte ante ellos, Microsoft dispone de varias soluciones o herramientas como:

MFA – Multi Factor Authentication.

Microsoft Defender for Office 365.

Microsoft Defender for Endpoint. (Ramos, 2022)

Prevención

No dé a conocer datos personales usando la comunicación del correo electrónico. En el correo electrónico, si no se utilizan técnicas de cifrado y/o firma digital.

No descargar ni abrir archivos de fuentes sospechosas (Ramos, 2022)

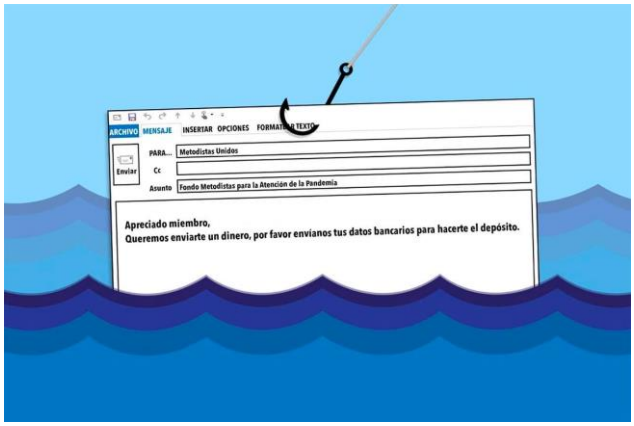


Figura 1. Virus de phishing

- **Ransomware**

Es un tipo de ataque que impide a las víctimas ingresar a sus sistemas, dispositivos o documentos personales pidiendo un rescate para volver a ingresar a ellos. (Bottini, 2021)

Solución

Ante este tipo de ataque, podemos contar con estas dos soluciones de Microsoft:

Microsoft Defender for Office 365

Microsoft Defender for Endpoint (Bottini, 2021)

Prevención

Jamás acceda en enlaces poco confiables: evite hacer clic en enlaces de mensajes de spam o en sitios web que desconoce.

Evite dar a conocer información personal: si recibe una llamada, un mensaje de texto o un correo electrónico de una fuente que no sea de confianza en donde se le solicita información personal, no responda. (Bottini, 2021)

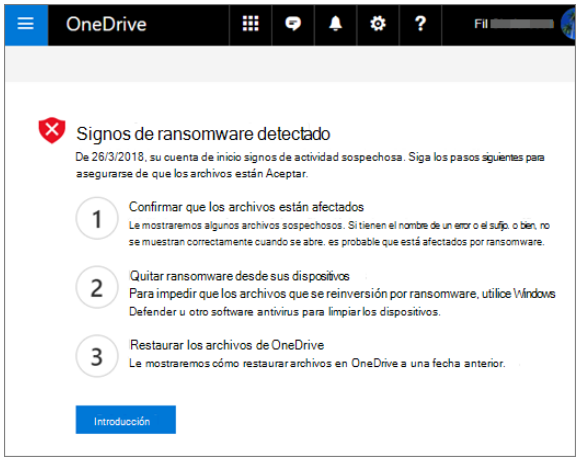


Figura 2. Virus de ransomware

- **Exploits**

Exploits es un hacker el que encuentra un agujero de seguridad y logra acceder a nuestro sistema, podrá cargar un malware tanto para hurtar información como para suplantar nuestra identidad, pudiendo llevar a cabo ataques de phishing. (A., 2020)

Solución

Una de las acciones importantes que se puede llevar a cabo para protegerse de ellos es tener siempre bien actualizado su sistema y aplicaciones, y tener un buen antivirus, el cual no solo lo proteja, sino que lo permita crear una central de alertas personalizadas para rastrear posibles amenazas:

Microsoft Defender for Endpoint. (A., 2020)

Prevención

El verdadero problema con el virus exploits es que constituyen parte de un ataque mucho más complicado. Eternamente vienen con otras sorpresas desagradables e infectan el dispositivo con códigos peligrosos. (A., 2020)

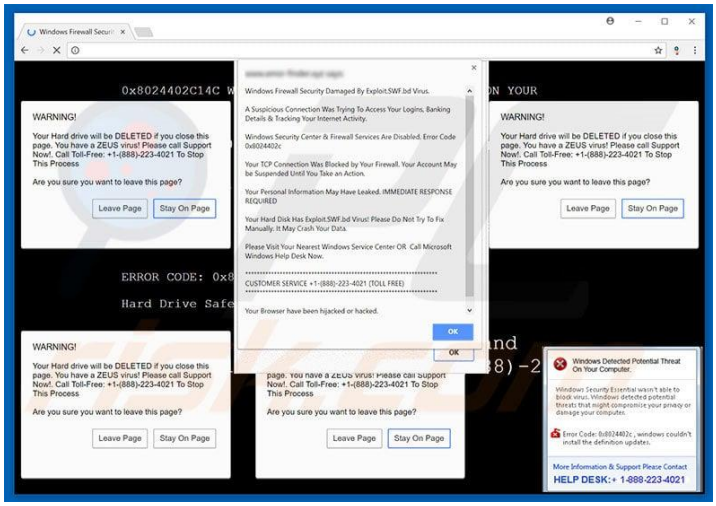


Figura 3. Virus de exploit

- **Keylogger**

Es una herramienta la cual logra registrar las pulsaciones que ocurren en el teclado del usuario, logrando sustraer contraseñas y demás datos sensibles. (Pérez, 2018)

Solución

La forma más fácil y segura de detener los keyloggers es utilizar un detector para eliminarlos automáticamente.

Avast analiza en profundidad su sistema para asegurarse de que cualquier tipo de infección por Keylogger se elimina inmediatamente. (Pérez, 2018)

Prevención

Conservar el computador renovado es decir actualizado con los últimos parches de seguridad.

Contar con un antivirus y debe estar actualizado.

Utilizar un gestor de contraseñas para iniciar sesión sin necesidad de escribir las credenciales. (Pérez, 2018)

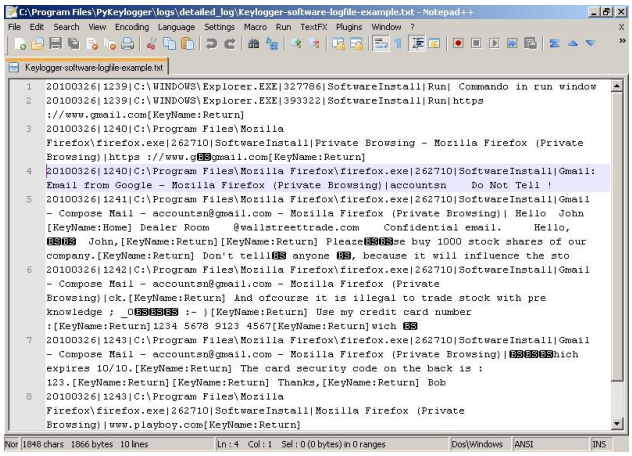


Figura 4. Virus de Keylogger

- **Gusano**

Un gusano informático, al igual que un virus, se replica automáticamente, sin embargo, se diferencia de este porque no requiere de un software para alojarse en la computadora de la víctima, y ataca principalmente a la red y al ancho de banda. (Huerta, 2019)

Solución

Una cuestión importante, es que los gusanos se van a aprovechar del software obsoleto para acceder a el ordenador. Por lo tanto, para evitarlo necesita tener actualizado lo siguiente:

- El sistema operativo.
- Un antivirus, y si es posible, software antimalware.
- Los programas y aplicaciones. (Huerta, 2019)

Prevención

Un tema importante, es que los gusanos se van a aprovechan del software antiguo para lograr acceder a su computador. Por lo tanto, para evitarlo necesita tener actualizado lo siguiente:

- El sistema operativo.
- Un antivirus.
- Los programas y todas sus aplicaciones.
- Otra cosa significativa es jamás abrir archivos adjuntos del e-mail de desconocidos.

(Huerta, 2019)

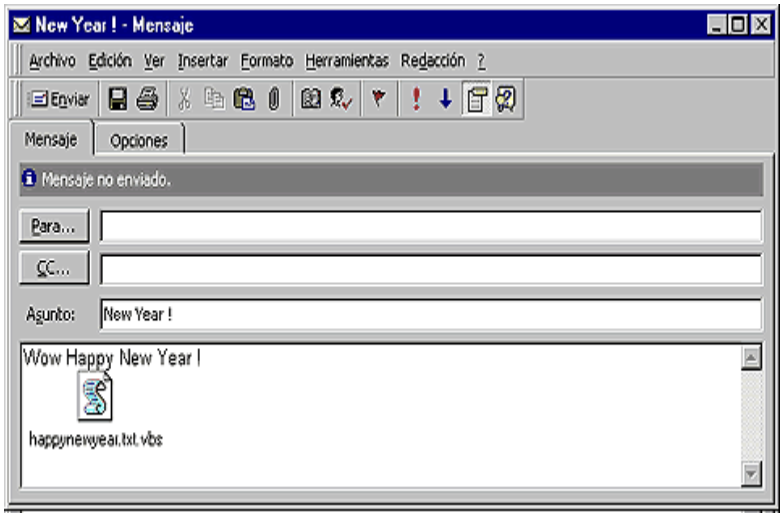


Figura 5. Virus de gusano

- **Troyano**

El malware conocido como troyano o caballo de troya, se presenta inicialmente como un software legítimo, pero al ser instalado, concede acceso remoto al atacante sobre el equipo informático de la víctima, pudiendo manejarlo casi a su antojo. (Larrocha, 2017)

Solución

No se debe abrir los archivos adjuntos que vengan con el correo electrónico, salvo que se esté totalmente seguro de que no están infectados. Incluso los correos de personas conocidas pueden contener virus. (Larrocha, 2017)

Prevención

Los troyanos se bautizaron así porque necesitan su autorización para ejecutarse en el computador, y lo consiguen si ejecutas el programa su mismo o si abre un documento o imagen que ejecuta el programa. Con esto en mente, la primera y mejor defensa frente a los troyanos es no abrir nunca un archivo adjunto de correo electrónico ni ejecutar un programa si no está totalmente seguro de la fuente, lo que incluye todos los archivos descargados de sitios web o programas punto a punto (P2P, del inglés Peer-to-Peer). Pero esto rara vez es posible en el mundo interconectado de hoy en día, por lo que se requiere tomar algunas medidas de seguridad específicas. (Larrocha, 2017)

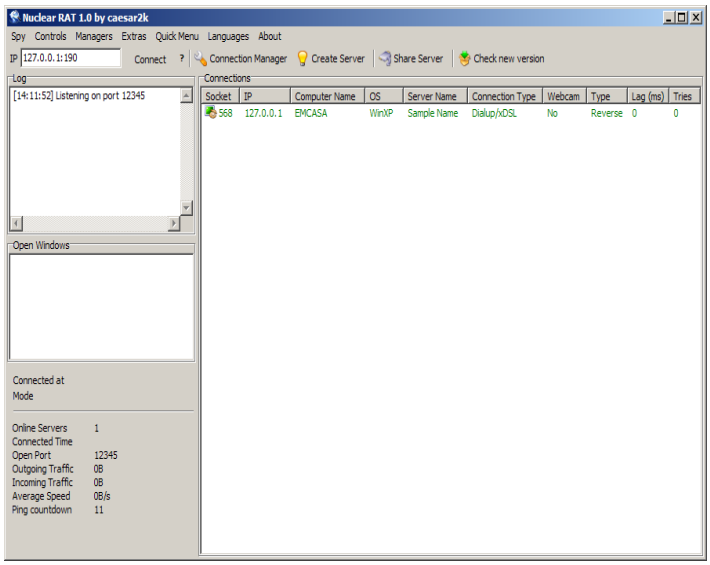


Figura 6. Virus de troyano

3.5 Hallazgos

El marco de investigación fue elaborado en la empresa “ASESORARTE”

El primer procedimiento de evaluación fue el análisis de los celulares de cada uno de los colaboradores de la empresa, en la aplicacion WhatsApp se encontró ciertos mensajes con el fin de estafar a los usuarios promocionando premios falsos.

En la visita realizada a la empresa “ASESORARTE”, se descubrió que varios teléfonos de los colaboradores han recibido mensajes de promociones y premios falsos.

También se pudo comprobar que ninguno de sus celulares tiene un antivirus, con el fin de proteger la información que contengan en sus dispositivos.

El segundo procedimiento fue la implementación de la guía la realización de una guía sobre los ataques informáticos, en la cual van a informarse sobre qué medidas de seguridad puede tomar para proteger sus dispositivos. De cualquier ciberataque que se quiera realizar

La empresa asesorarte no cuentan con seguridad en las máquinas que están disponibles es decir en los computadores que tienen en la empresa, ni en los celulares de los colaboradores, por lo cual son más vulnerables a cualquier ciberataque que se quiera realizar por vía WhatsApp.

Debido a esto se ha implementado la guía para que ellos así puedan informarse, y saber que hacer en caso de dichos riesgos y poder solucionar cualquier ciberataque que esté listo para dañar sus dispositivos.

3.5.1 Aplicación de la guía de ataques informáticos

La aplicación de WhatsApp fue sometida a un análisis utilizando la guía metodológica, con toda la información recolectada en cuanto a los virus sus soluciones y prevenciones. La cual nos permite dar una solución para los virus que atacan a la red social de WhatsApp.

3.5.6 WhatsApp web

3.5.6.1 Keylogger

Los keyloggers hacen un rastreo e inspeccionan las teclas que se usan en una computadora, sin la autorización y mucho menos el conocimiento de la persona que está usando el equipo. Un Keylogger puede estar basado en hardware o software, y su uso puede ser como herramienta legal de control de TI

(tecnologías de la información), tanto en su vida laboral como particular. Pero a pesar de esto, los keyloggers son utilizados con fines maliciosos por los ciberdelincuentes. Los keyloggers son utilizados para capturar información personal, como contraseñas o información financiera que posteriormente se envía a terceros para su explotación con fines delictivos.

Todos están expuestos a un virus Keylogger, básicamente muestra una pestaña que el lado derecho de la pantalla se puede visualizar sus aplicaciones, entre estas están las pulsaciones que se realizan en el computador.

Lo que es importante para el ciberdelincuente, es poder hackear sus redes sociales entre estas WhatsApp, que actualmente es la más utilizada en la que se comparte información muy importante como cuentas bancarias. En la empresa “ASESORATE” WhatsApp es la red social más utilizada para comunicarse con los colaboradores y clientes de dicha empresa, sobre todo WhatsApp web que al poseer este virus Keylogger puede enterarse de la información que comparte con los clientes y colaboradores de “ASESORARTE” lo cual es perjudicial para el personal y los clientes pues por este medio de vía WhatsApp hablaban de los tramites o prestamos que se podían realizar.

Como se puede observar en este este grafico todavía no hay datos ni ningún tipo de información.

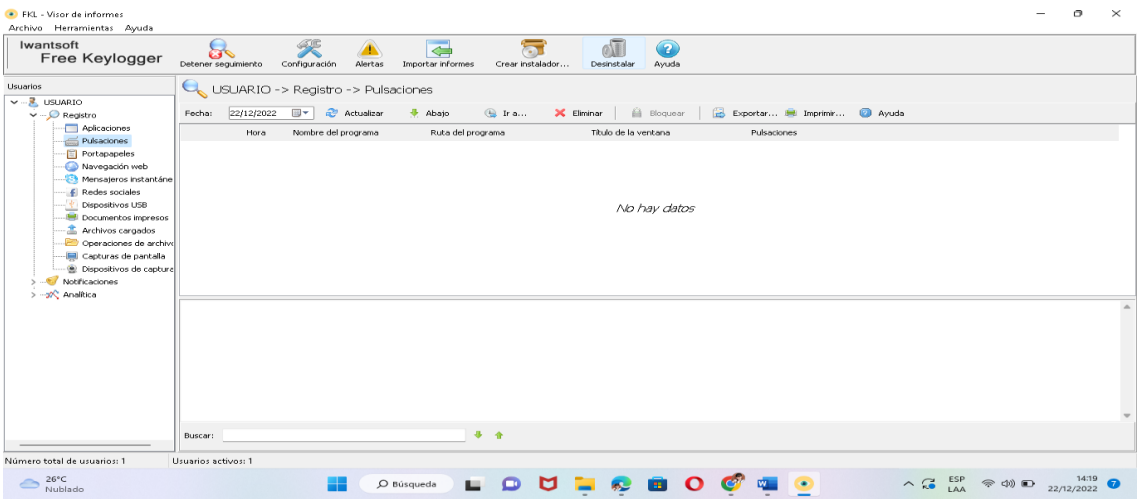


Figura 7. Página de entrada de Keylogger

En este grafico se puede observar que hay dos registros de Word donde se registró las pulsaciones que se realizaron en el computador. Al dar clic en pulsaciones automáticamente se muestran los registros que se han realizado en dicho computador. Muestra la hora, el nombre del programa, la ruta del programa, el título de la ventana y por último las pulsaciones. Las cuales son las más importantes pues hay puede contener la información de conversaciones de WhatsApp que son las más esenciales, pues esta es la red social más utilizada para hackeo y robo de información.

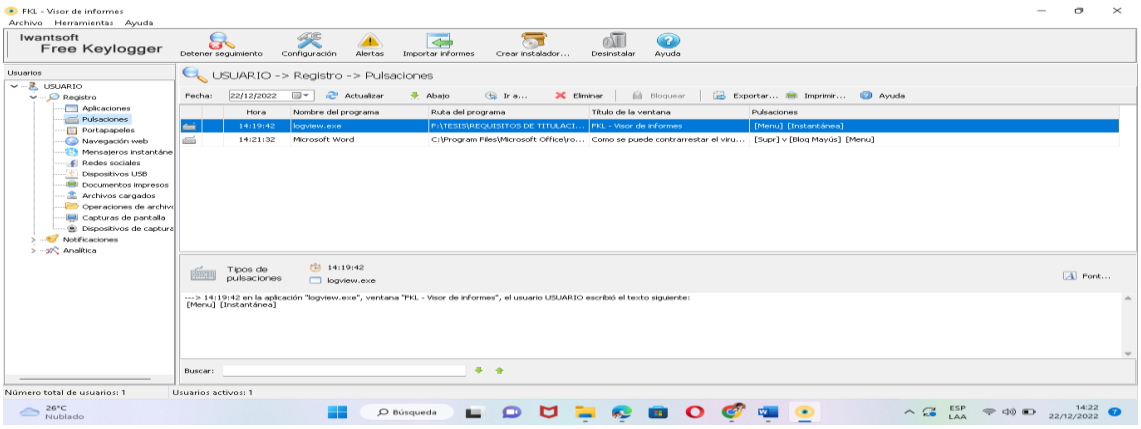


Figura 8. Pulsaciones registradas

Al momento de pulsar la opción de actualizar se puede ver todas las actividades que se han realizado y aquí es donde entra a afectar a WhatsApp web es la red social que más se usa para comunicarse en “ASESORARTE”.

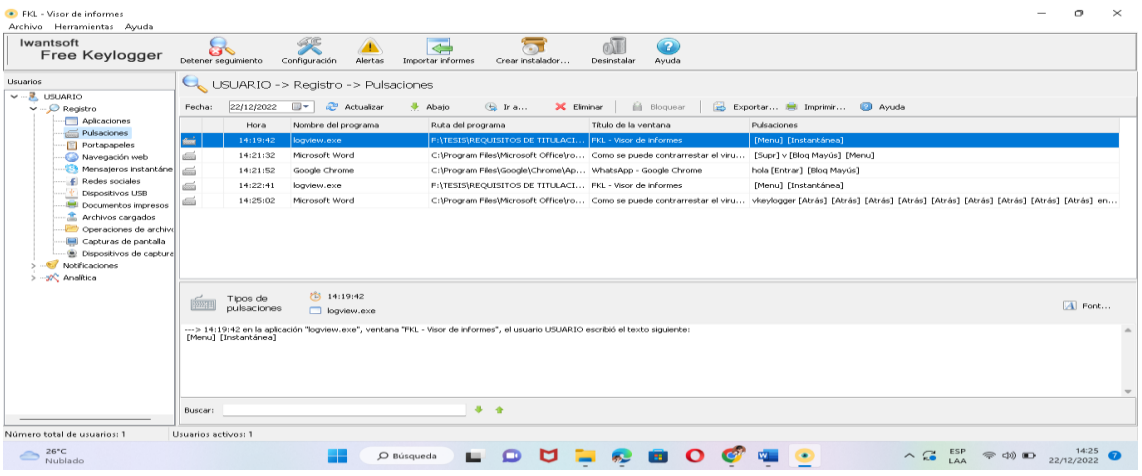


Figura 9. Registro de pulsaciones de navegación

En este gráfico se muestra información relevante (conversación por la red social WhatsApp) de la cual los ciberdelincuentes pueden sacar provecho, para sus fines maliciosos.

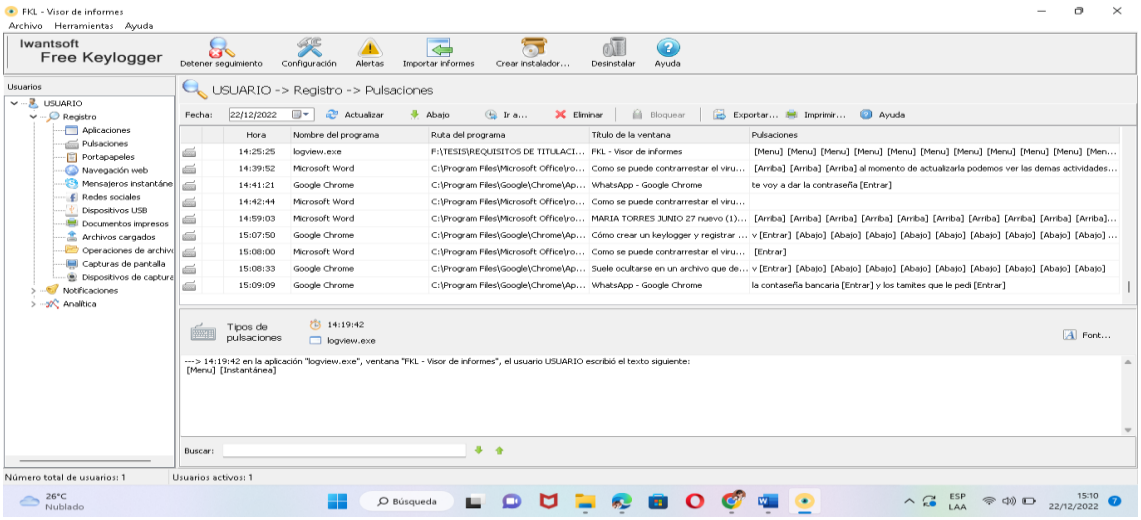


Figura 10. registro de pulsaciones de todo lo que se ha realizado en el ordenador

3.5.7 Solución

3.5.7.1 Keylogger detector

Keylogger Detector es una herramienta con la que se puede mantener privacidad, protegiendo información y por completo el computador de entradas no autorizadas. Con este software, se tiene la total garantía de que en una PC no se ha instalado ningún programa Keylogger, que puede registrar todas las pulsaciones que se realicen en el ordenador.

En gráfico muestra la primera ventana de keylogger detector, y se puede vizualizar en el panel que se encuenta en lado derecho, nos indicar dar click allí.

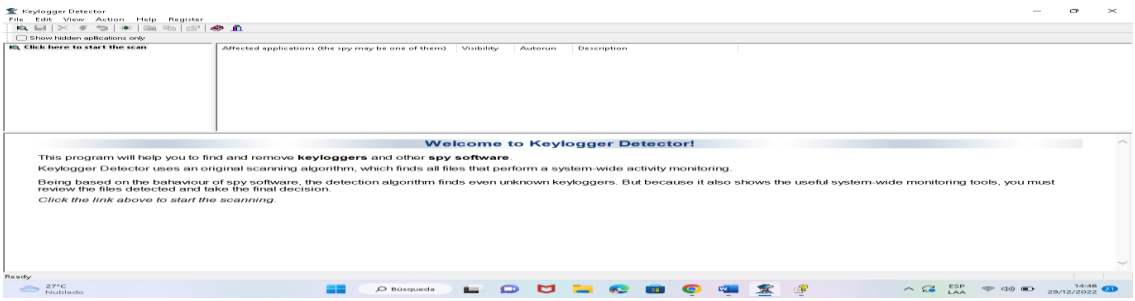


Figura 11. Primera ventana de keylogger

Como muestra en el grafico está analizando el computador con la finalidad de ver si hay un Keylogger que este ejecutándose en segundo plano.

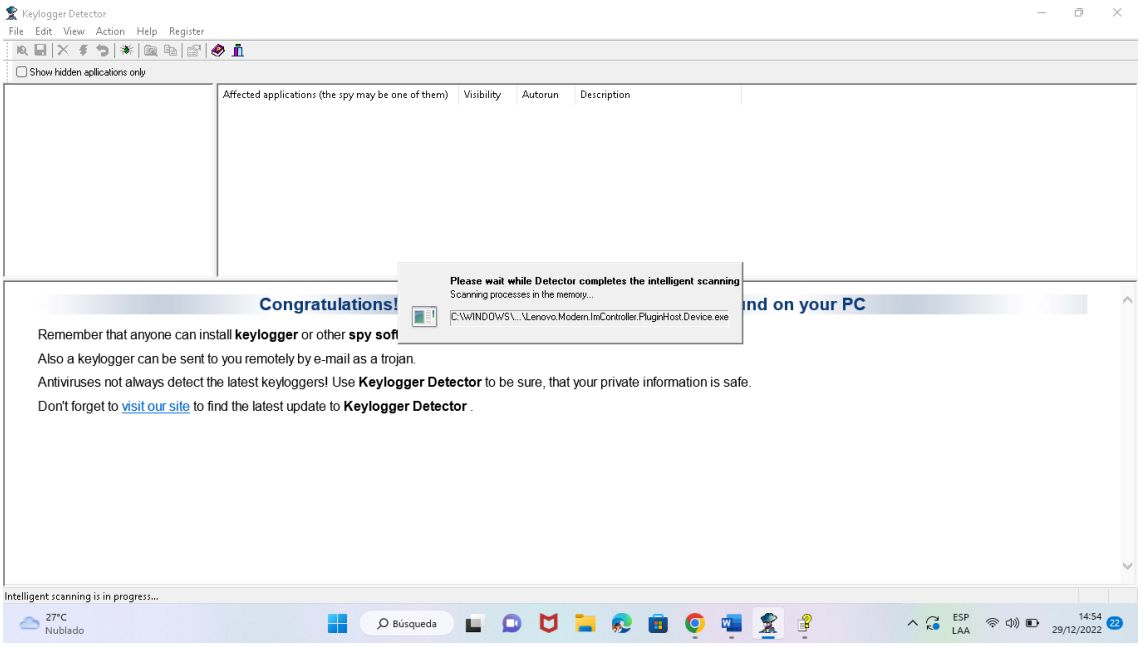


Figura12. Analizando el computador para ver si se encuentra un Keylogger

Al finalizar, muestra una frase que da conocer que no existe un keylogger que se este ejecutando, la palabra que muestra es : felicitaciones no se encontraron archivos de monitoreo de todo el sistema en su PC.

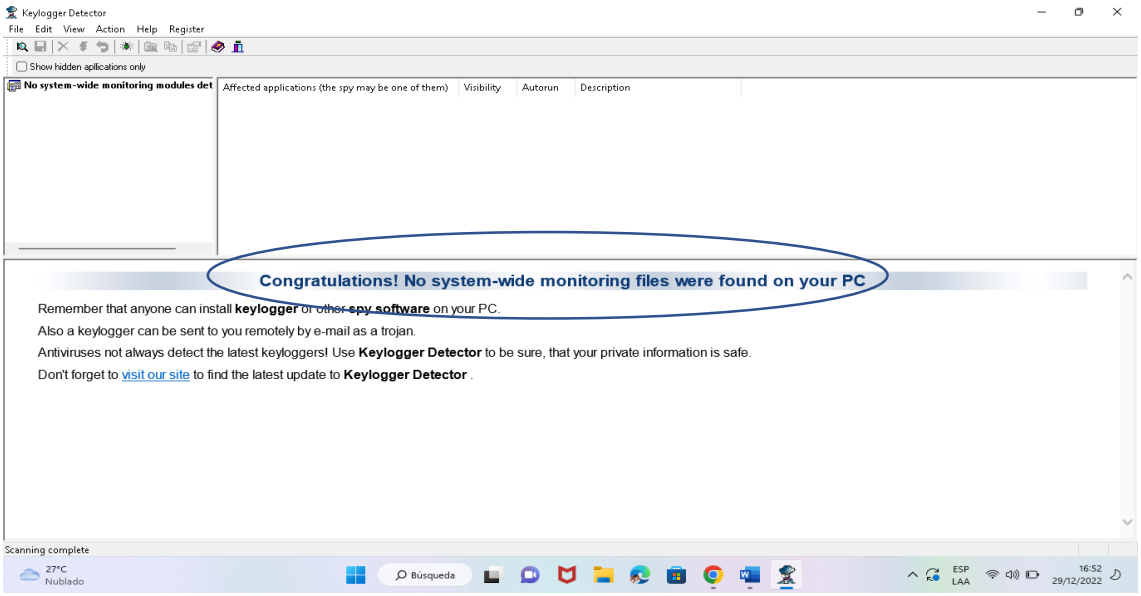


Figura 13. ningún virus

Lo que muestra e el siguiente grafico da a conocer como lle ga al computador del hacker sus pulsaciones .

Figura 14. muestra las pulsaciones

3.5.7.2 ¿Cómo Keylogger puede llegar a el ordenador de la víctima?

Keylogger suele ocultarse en un archivo que se puede descargar por internet, por ejemplo, una aplicación que se ha instalado.

Se realiza en un segundo plano en dicho sistema sin que el propietario del ordenador tenga conocimiento de lo que está sucediendo mientras registra todas las pulsaciones que se realizan en el teclado del ordenador.

Esto, a continuación, se envía a un servidor controlado por ciberdelincuentes.

3.5.7.3 WhatsApp en smartphone

3.5.7.4 Keylogger

Es una aplicación sencilla y muy fácil de usar la cual cumple la función de registrar los textos que se escriban en el celular. Es decir, registra las pulsaciones y las conversaciones que se realicen en dicho dispositivo, las más

importantes son las conversaciones de la red social de WhatsApp las cuales pueden ser sustraídas de la empresa “ASESORARTE” para fines maliciosos.

En el grafico se puede visualizar el logo de Keylogger. La aplicación que registra las pulsaciones y conversaciones. Que se realicen en el celular.

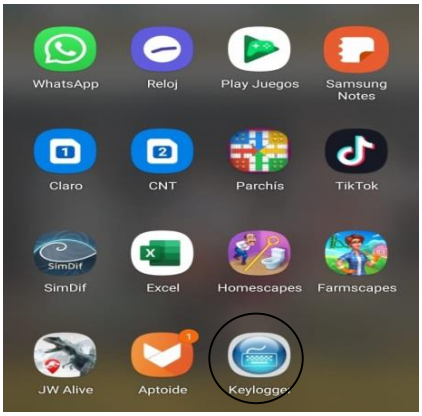


Figura 15. Keylogger descargado en el celular

En este gráfico demuestra cómo se pueden ajustar ciertos aspectos de Keylogger como el idioma la contraseña entre otros.

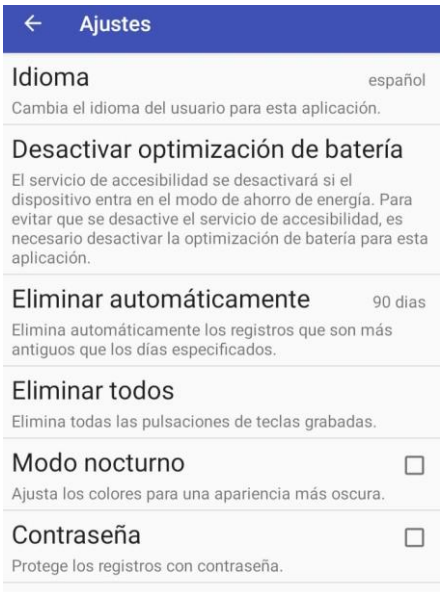


Figura 16. Ajustes de Keylogger

En este grafico se visualiza donde se deben mostrar todas las pulsaciones y las conversaciones de cualquier red ya pueden se mensajes de Facebook Instagram. Pero las conversación más comunes e importantes actualmente se

realizan por la red social WhatsApp. Y en esta red social se concentran los ciber delincuentes porque aquí es donde encuentran información muy útil para sus planes maliciosos.

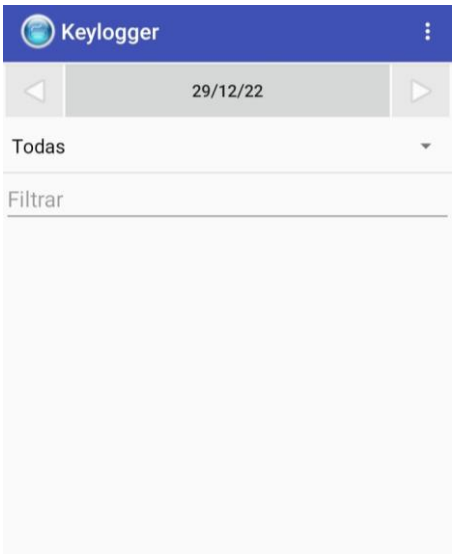


Figura 17. ventana donde se muestran las pulsaciones.

Finalmente, aquí se muestran las pulsaciones y conversaciones de todas las redes sociales especialmente las de WhatsApp.

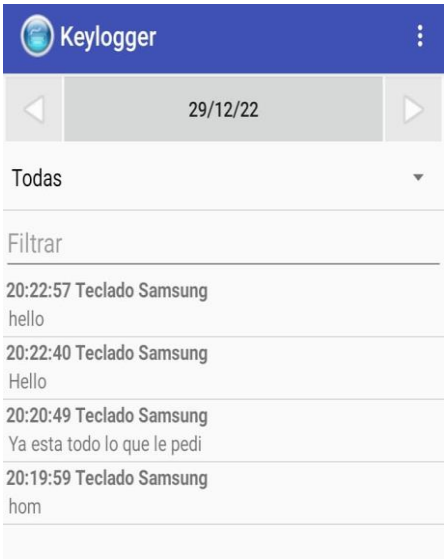


Figura 18. Muestra pulsaciones

3.5.8 Solución

En este gráfico muestra el malwarebytes. Es decir, un software que funciona como un antivirus. El cual puede proteger tu celular.

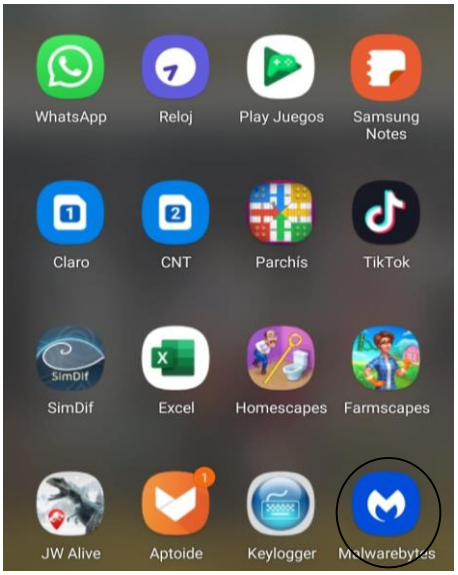


Figura 19. antivirus instalado

En este gráfico muestra la información de la aplicación que se instaló para proteger el dispositivo de cualquier virus malicioso.

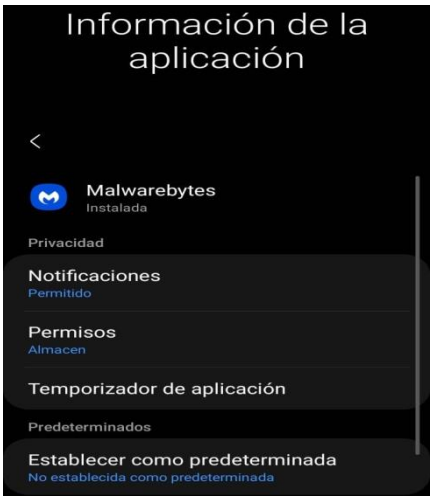


Figura 20. Información del antivirus

En este gráfico se muestra el funcionamiento de la aplicación la aplicación funciona analizando archivos y aplicaciones. Al momento de analizarlo pretende

encontrar algún virus mientas la aplicación analiza los archivos muestra las aplicaciones que va analizando, los archivos y el tiempo.

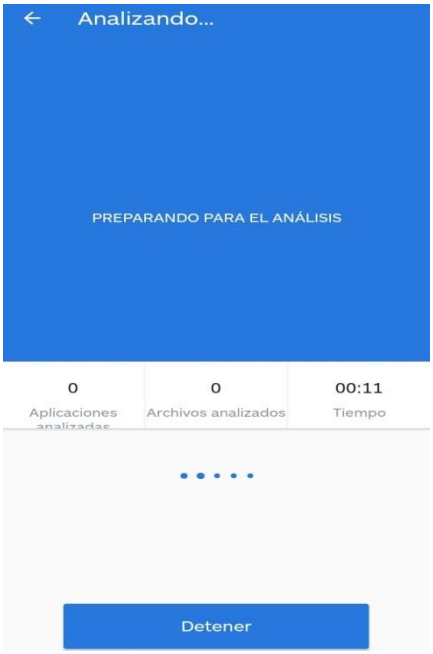


Figura 21. analizando el celular

Se puede visualizar en este gráfico que la aplicación empezó a analizar las aplicaciones instaladas en el celular. Y notifica de un virus encontrado.

Figura 22. Analizando el celular

Como se puede ver encontró un malware y da la opción de eliminar las amenazas encontradas.

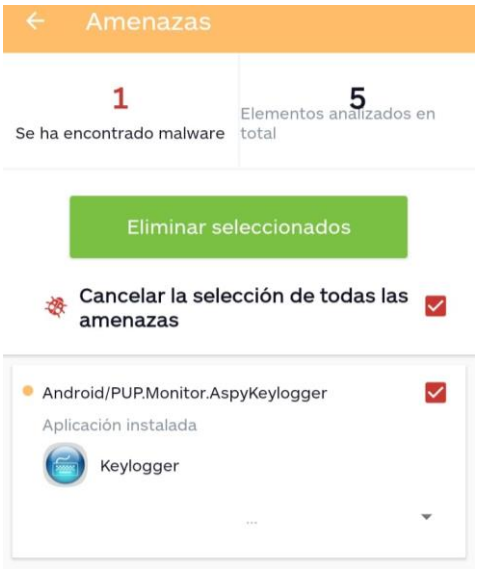


Figura 23. Virus encontrado

3.5.8.1 ¿Cómo Keylogger puede llegar a el celular de la víctima?

Keylogger por lo general se oculta en un archivo que se puede descargar por internet. Se realiza en un segundo plano en dicho sistema sin que el propietario del ordenador tenga conocimiento de lo que está sucediendo mientras registra todas las pulsaciones que se realizan en el teclado del ordenador.

Esto, a continuación, se envía a un servidor controlado por ciberdelincuentes.

3.5.8.2 ¿Qué medidas preventivas se deben tomar para no ser víctimas de Keylogger?

- Rechazar a cualquier programa de computador gratuito dudoso.
- Cambiar las contraseñas cada 3 semanas, claves de redes sociales, banca móvil entre otros.
- Si se deben hacer deberes diarios, pueden usar un perfil de “privilegios limitados”.
- Cree copias de sus datos y respáldelos, para futuras perdidas en caso de que su computador sea hackeado.

3.5.9 Medidas de seguridad

Los keyloggers no son fáciles de revelar, porque fueron creados para y registrar la que nadie lo note, y asi robar información y no provocar problemas perceptibles en el ordenador.

Es por esto por lo que varios antivirus no logran diferenciarlo de un programa fiable.

Sin embargo, sí se puede salvaguardar un equipo informatico de un Keylogger. Y las medidas de seguridad son:

- Conservar el equipo actualizado.
- Tener un antivirus y actualizarlo.
- No pinchar en noticias y enlaces no fiables.
- No instalar programas de origen desconocido.

Conclusiones

- Se pudo encontrar contenido de la bibliografía de los ataques informáticos en libros en revistas científicas las cuales fueron un poco difíciles de encontrar ya que no está tan actualizada la información en dichos libros
- La visita a la empresa dio a conocer hallazgos los cuales se evidenciaron mediante herramientas de investigación que sustentan la factibilidad en esta investigación ya que existen falencias en la seguridad de la información y los dispositivos electrónicos que poseen los colaboradores de la empresa.
- Se concluyó con la implementación de una guía de la prevención de los ataques informáticos que contiene las medidas necesarias que se pueden tomar con base a los resultados de los análisis previos.

Recomendaciones

- Actualizar conocimientos sobre los ataques informáticos explorando la guía.
- Compartir información de la guía para evitar que más personas sean víctimas de los hackers informáticos.
- Utilizar la guía para contrarrestar los virus y cualquier ataque que quieren intentar los hackers.

Referencias bibliográficas

A., S. P. (2020). *CoNaSSoL (Congreso de Hacking y Software Libre).*

Abreu, J. (24 de Diciembre de 2017). *El Método de la Investigación.* Obtenido de El Método de la Investigación: http://www.spentamexico.org/v9-n3/A17.9(3)195-204.pdf

Agencia Digital Costa Rica. (18 de Febrero de 2018). *Importancia Del WhatsApp en las empresas.* Obtenido de Importancia Del WhatsApp en las empresas: https://agenciadigitalcostarica.com/importancia-whatsapp-para-empresas/

Alvarez, G. (13 de Marzo de 2020). *thinkbig.* Obtenido de thinkbig: https://blogthinkbig.com/cifrado-vida-privada-esta-en-whatsapp-quien-mas-la-conoce

AVANSIS. (07 de Enero de 2021). *TIPOS DE SEGURIDAD INFORMÁTICA Y CIBERSEGURIDAD.* Obtenido de TIPOS DE SEGURIDAD INFORMÁTICA Y CIBERSEGURIDAD: https://www.avansis.es/ciberseguridad/tipos-de-seguridad-informatica/

Banco Pichincha. (15 de Marzo de 2021). *Pichincha.com.* Obtenido de Pichincha.com: https://www.pichincha.com/portal/blog/post/riesgos-seguridad-whatsapp

Bello, E. (21 de Noviembre de 2021). *Ciberseguridad: Tipos de ataques y en qué consisten.* Obtenido de Ciberseguridad: Tipos de ataques y en qué consisten: https://www.iebschool.com/blog/ciberseguridad-ataques-tecnologia/

Bello, E. (29 de Noviembre de 2021). *IEBS.* Obtenido de IEBS: https://www.iebschool.com/blog/ciberseguridad-ataques-tecnologia/

BOLETÍN N°46. (30 de Octubre de 2018). *CIBER ATAQUES.* Obtenido de CIBER ATAQUES: https://bacsirt.buenosaires.gob.ar/files/boletines/B46_AtaquesCiberneticos.pdf

Bottini, C. (2021). *RANSOMWARE: Cronología de un ataque y cómo enfrentarlo.*

Callejas, J. E. (2020). *Metodolia de la investigación.* Mexico.

Cao, C. (04 de Septiembre de 2018). *WhatsApp.* Obtenido de WhatsApp: https://ladefinicion.com/whatsapp/

Castro, R. (11 de Noviembre de 2019). *medidas de Seguridad Informática.* Obtenido de medidas de Seguridad Informática: https://www.teamnet.com.mx/blog/las-mejores-medidas-de-seguridad-informatica

CENTRO EUROPEO DE POSTGRADO. (12 de Enero de 2021). *medidas de seguridad informática.* Obtenido de medidas de seguridad informática: https://ceupe.com.ar/blog/que-son-las-medidas-de-seguridad-informatica/

Chambers, J. (29 de Noviembre de 2021). *IEBS.* Obtenido de IEBS: https://www.iebschool.com/blog/ciberseguridad-ataques-tecnologia/

Ciberseguridad. (26 de Enero de 2021). *Tipos de ataques informáticos y previsiones para el 2021.* Obtenido de Tipos de ataques informáticos y previsiones para el 2021: https://www.optical.pe/blog/tipos-de-ataques-informaticos-y-previsiones-para-el-2021/

Collado, C. (11 de Mayo de 2021). *Cómo bloquear WhatsApp con tu huella dactilar: evita que espíen tus chats.* Obtenido de Cómo bloquear WhatsApp con tu huella dactilar: evita que espíen tus chats: https://andro4all.com/2019/04/bloquear-chats-whatsapp-huella

- De TALLEDO SAN MIGUEL, J. V. (s.f.). *Instalación y configuración de aplicaciones informáticas.*

Diaz, L. (07 de Septiembre de 2019). *Redalyc.* Obtenido de Redalyc: https://www.redalyc.org/pdf/3497/349733228009.pdf

Dioses, J. (06 de Abril de 2020). *Significados.* Obtenido de Significados: https://designificados.com/whatsapp/

Dodda, S. (O8 de Junio de 2021). *QRL Jacking.* Obtenido de QRL Jacking: https://sumododda.medium.com/qrl-jacking-217103bd6ee7

Echeverria, J. (01 de Junio de 2019). *EL MÉTODO ANALÍTICO COMO MÉTODO NATURAL.* Obtenido de EL MÉTODO ANALÍTICO COMO MÉTODO NATURAL: https://www.redalyc.org/pdf/181/18112179017.pdf

Folgueira, P. (01 de Enero de 2019). *LA ENTREVISTA.* Obtenido de LA ENTREVISTA: http://diposit.ub.edu/dspace/bitstream/2445/99003/1/entrevista%20pf.pdf

GIPGRUP. (09 de Agosto de 2020). *Firewall .* Obtenido de Firewall : https://idgrup.com/firewall-que-es-y-como-funciona/

Huerta, A. V. (2019). *Seguridad en Unix y redes. Versión 2.1'.*

Immaculada Barral Viñals, A. Q. (s.f.). *La resolución de conflictos con consumidores: De la mediación a las ODR.*

Incibe. (08 de Julio de 2020). *Instituto Nacional De Ciberseguridad.* Obtenido de Instituto Nacional De Ciberseguridad: https://www.incibe.es/aprendeciberseguridad/smishing

Infocyte. (23 de Agosto de 2021). *tipos más comunes de ataques de ciberseguridad.* Obtenido de tipos más comunes de ataques de

ciberseguridad: https://www.infocyte.com/es/blog/2019/05/01/cybersecurity-101-intro-to-the-top-10-common-types-of-cyber-security-attacks/

Larrocha, E. R. (2017). *Nuevas tendencias en los sistemas de información.*

María Sicilia, M. P. (2021). *MARKETING EN REDES SOCIALES.* febrero 2021.

Muñoz , I. (10 de Julio de 2020). *La importancia de la Seguridad de la Información.* Obtenido de La importancia de la Seguridad de la Información: https://blog.posgrados.ibero.mx/seguridad-de-la-informacion/

Nubelia Cloud. (05 de Mayo de 2021). *fases de un ataque informático.* Obtenido de fases de un ataque informático: https://nubeliacloud.com/2021/05/06/conocer-las-fases-de-un-ataque-informatico-es-la-clave-para-proteger-a-tu-empresa/

Ortiz , M. (30 de abril de 2019). *Guia de entrevista y observacion.* Obtenido de Guia de entrevista y observacion: https://prezi.com/ooatecj5_fgt/guia-de-entrevista-y-de-observacion/

Otero, C. (06 de Junio de 2018). *Qué es la verificación en 2 pasos de WhatsApp y por qué debes usarla.* Obtenido de Qué es la verificación en 2 pasos de WhatsApp y por qué debes usarla: https://as.com/meristation/2018/06/06/betech/1528275087_218210.html

Perez , J. (24 de Febrero de 2020). *WhatsApp permite ocultar la foto, el estado y la última conexión.* Obtenido de WhatsApp permite ocultar la foto, el estado y la última conexión: https://www.hijosdigitales.es/es/2014/02/ahora-whatsapp-permite-ocultar-la-foto-el-estado-y-la-ultima-conexion/

Pérez, J. C. (2018). *Operaciones Auxiliares de Mantenimiento de Sistemas Microinformáticos (MF1208_1).*

Perez, J. (s.f.). *El debate sobre la privacidad y seguridad en la red: regulación y mercados.*

Ramos, J. (2022). *Cómo protegerte del phishing: Evita que te roben tu información y tu dinero.*

Rodriguez , A., & Perez, O. (01 de Junio de 2017). *Métodos científicos de indagación y de construcción del conocimiento.* Obtenido de Métodos científicos de indagación y de construcción del conocimiento: http://www.scielo.org.co/pdf/ean/n82/0120-8160-ean-82-00179.pdf

Romero, J. (04 de Febrero de 2021). *Redes Sociales y Tecnologias.* Obtenido de Redes Sociales y Tecnologias: https://www.trecebits.com/2020/02/04/seis-consejos-para-evitar-que-tu-cuenta-de-whatsapp-sea-hackeada/

Russell, J. (22 de Julio de 2020). *Hootsuite.* Obtenido de Hootsuite: https://blog.hootsuite.com/es/riesgos-de-seguridad-en-redes-sociales/

SAP España. (11 de Diciembre de 2020). *España News Center .* Obtenido de España News Center : https://news.sap.com/spain/2020/12/los-7-tipos-de-ataques-informaticos-mas-frecuentes/

Shaumik , D. (06 de Febrero de 2020). *Kinsta.* Obtenido de Kinsta: https://kinsta.com/es/blog/inyeccion-sql/

TALLEDO SAN MIGUEL, J. V. (s.f.). *Instalación y configuración de aplicaciones informáticas.*

Vera , A. (2017). *Metodologia de la investigacion.* España: Athenaica Ediciones Universitarias.

Weber, J. (09 de Enero de 2020). *Ataques informáticos.* Cordoba: Jorge Sarmiento Editor - Universitas. Obtenido de Ataques informáticos: https://www.evilfingers.com/publications/white_AR/01_Ataques_informaticos.pdf

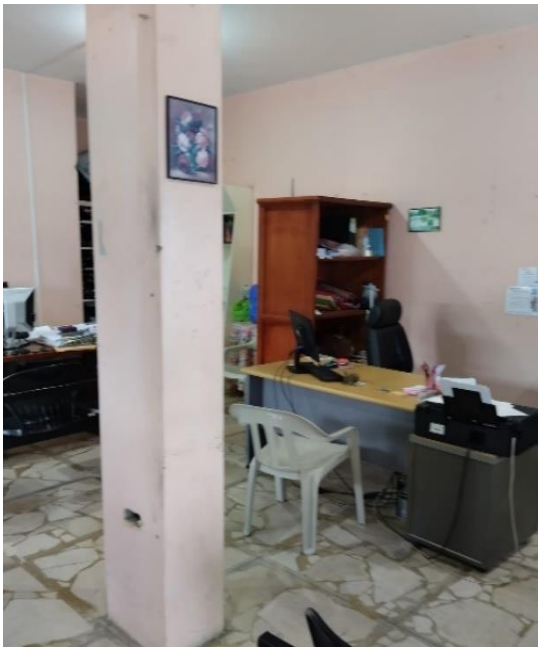
3.5.2 Anexos

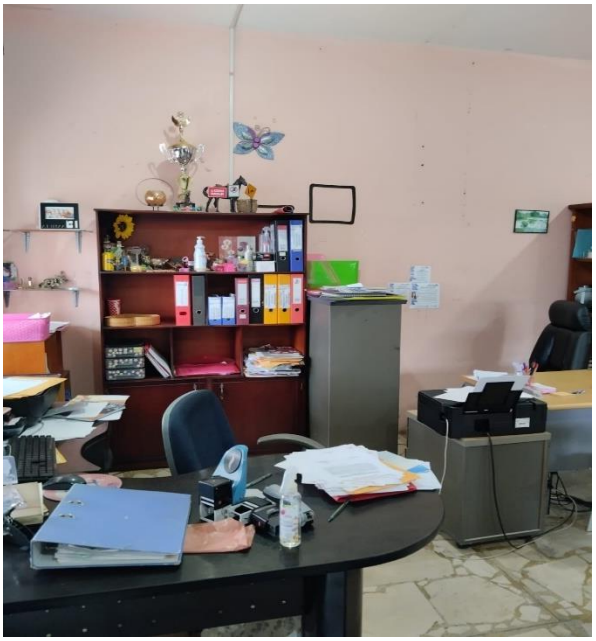
Anexo 1 entidad "ASESORARTE"

Anexo 2 entrada de la empresa

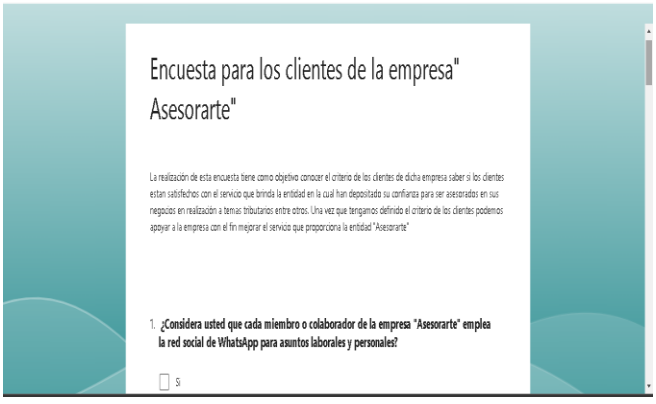
Anexo 3 entrevista el gerente

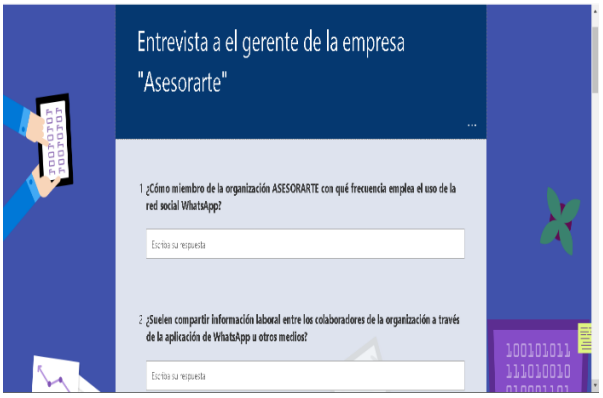
Anexo 4 encuesta a los clientes de la empresa





Anexo 5 oficinas de la empresa





Anexo 6 encuesta y entrevista

Encuesta

Encuesta realizada a los clientes de la Entidad de Asesoría Contable y Tributaria “Asesorarte” Del Cantón El Carmen.

Datos personales

Nombre:

Fecha:

1. ¿Considera usted que cada miembro o colaborador de la empresa "Asesorarte" emplea la red social de WhatsApp para asuntos laborales y personales?

Si

No

2. ¿Con qué frecuencia los miembros de la organización emplean la red social de WhatsApp para transmitirle un mensaje con relación al trámite que este realizando usted como cliente?

Opción única.

Siempre

A veces

Nunca

3. ¿Usted tiene el conocimiento acerca de los distintos virus informáticos que pueden existir y que pueden ser manipulados por medios de diversos mecanismos incluyendo la red social de WhatsApp?

Si

No

4. ¿Cree usted que los dispositivos electrónicos deben contar con mecanismos de seguridad informática?

Si

No

5. ¿Cuáles cree usted que deben ser los factores para hacernos vulnerables a los ataques informáticos originados por los cyber-delincuentes?

Desconocimiento

Descuido personal

Otros

6. ¿Estaría de acuerdo con la elaboración de una guía metodológica acerca de los ataques informáticos y las medidas preventivas de seguridad de WhatsApp?

Si

No

7. ¿Piensa qué la elaboración de la guía servirá para conformar directrices integrales de seguridad en el correcto uso y manejo de la aplicación de WhatsApp?

Si

No

8. ¿Considera esencial una capacitación acerca de los ataques informáticos y mecanismos de protección y prevención de seguridad informática de la red social WhatsApp?

Si

No

9. ¿Sus dispositivos inteligentes cuentan con algún tipo de antivirus que le permita contrarrestar los virus informáticos?

Si

No

10. ¿Como define usted a la entidad al momento en que le solicita documentos confidenciales por medio de la red social WhatsApp?

Muy satisfactorio

Satisfactorio

Poco satisfactorio

11. ¿Qué tan importante cree usted qué es seguridad en los archivos y enlaces enviados por la entidad?

Muy importante

Importante

Poco importante

12. ¿Ha sido víctima de algún tipo de ataque informático?

Si

No

Anexo 7 formato de la encuesta

Entrevista realizada al Sr. Roddy Ramírez y Asociados

1. ¿Cómo miembro de la organización “ASESORARTE” con qué frecuencia emplea el uso de la red social WhatsApp para comunicarse con sus usuarios?

2. ¿Suelen compartir información laboral entre los colaboradores de la organización a través de la aplicación de WhatsApp u otros medios?

3. ¿A criterio personal conoce a que se le denomina virus informático y cuantos tipos de virus pueden existir?

4. ¿Tiene conocimiento acerca de la privacidad que debe tener al momento de compartir una información por medio de la red social de WhatsApp a fin de que no sea manipulada por ningún ciber-delincuentes o terceros con fines maliciosos?

5. ¿Cuenta con algún sistema que le ayude a prevenir y proteger sus dispositivos y la información que puede ser sustraída por parte de los atacantes?

6. ¿Toma las precauciones necesarias al momento de recibir un mensaje o correo de algún tipo de fuente de origen desconocido?

7. ¿A criterio personal contrataría los servicios de un asesor informático que le brinde información de cómo proteger sus datos?

8. ¿Compartiría la información de la guía creada con sus clientes a fin de proteger la integridad de sus usuarios?

9. ¿Brindarían el apoyo y recursos necesario para la estructuración y elaboración de la guía de ataques informáticos y las medidas preventivas de seguridad a la red social WhatsApp?

10. ¿Conoce los pasos que se deben realizar en caso de sufrir un ataque informático?

11. ¿El personal de la empresa y usted han recibido capacitación acerca de los mecanismos de seguridad y distintos ataques que pueden ser ejecutados a través de la red social WhatsApp?

12. ¿La empresa ha sido afectada por un ataque informático?

Anexo 8 formato de la entrevista

130770661001

Anexo 9 Ruc de la entidad

GUÍA DE ATAQUES INFORMÁTICOS Y MEDIDAS DE SEGURIDAD COMO SOLUCIÓN PREVENTIVA A WHATSAPP EN LA ENTIDAD "ASESORARTE".

Objetivos de los ataques y consecuencias para la víctima

Los ciberdelincuentes y ataques siempre están al investigando sobre nuevas maneras con las cuales puede atacar a las víctimas. Gracias al inexperiencia o vulnerabilidad.

Sus objetivos son varios y hay una variedad de consecuencias para la víctima.

Figura 1. Seguridad de ataques

Regularmente los ciberdelincuentes informáticos usan plataformas muy reconocidos para realizar sus ataques.

El objetivo es que se pueda estar atento y detectar cuando podrían tratar de estafarnos y evitar caer en este tipo de trampas.

A continuación, se presentarán ataques que se realizan por WhatsApp los más comunes.

Tipos de ciberataques en WhatsApp

Hay un sin número de ataques que puede sufrir WhatsApp, pero los más populares son 3 los cuales presentare a continuación:

Enlace falso

Atravez de WhatsApp se puede recibir enlaces falsos, no solo pueden ser contactos que no conocemos estos enlaces pueden venir desde alguien de confianza, esta persona puede ser un amigo o familiar.

Es decir, la victima abre el enlace y hay automáticamente se envía a todos sus contactos y ahí es cuando estas personas también pueden llegar a ser víctimas de estos enlaces.

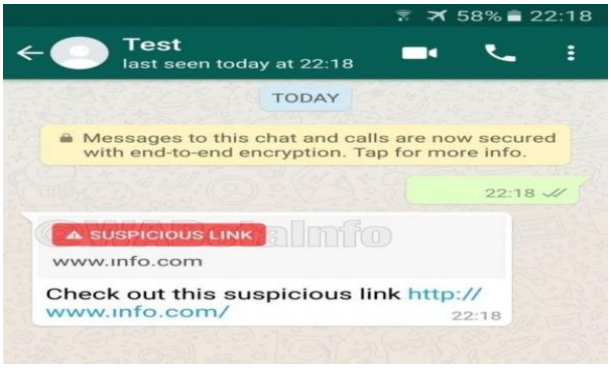


Figura 2. Enlace falso

¿Cómo funcionan?

Normalmente se reciben links los cuales nos trasladan a una supuesta página para iniciar sesión las redes sociales.

Un ejemplo puede ser una oferta que haga que la victima de clic en el enlace y posteriormente ubique sus datos para poder ver el contenido de dicha página.

Hacer comprar las ciertas plataformas como las que pueden ser, Amazon y muchas más por lo general este tipo de enlaces llama mucho la atención.

Una vez en el sitio empiezan actuar las ciberdelincuentes robando cuentas

bancarias, contraseñas etc.

Figura 3. Elance de estafa

¿Cómo me protejo?

1. Comprobar quien envía el mensaje

El paso número uno es recibir un mensaje por WhatsApp o por otra plataforma y asi ver el remitente es decir ver quién es el que envía el mensaje.

Si la fuente no es conocida, deberá activar las alarmas.

Pero por lo contrario si es conocida y le nota algo sospechoso lo mejor que puede hacer es contactar con esa persona o empresa de confianza por otro medio de comunicación.

2. Observar el contexto del mensaje.

Se muestran particularidades que pueden despertar sospechas, por ejemplo, que le digan a la persona que recibe el mensaje como ‘cliente o también como ‘usuario’.

En vez de por su nombre o que el mensaje o el mensaje tenga faltas ortográficas.

Sin embargo, los ataques y el ciberdelincuente están cada vez más preparado y sus técnicas son muy actuales y difíciles de detectar.

3. Revisar letras del enlace

Si el enlace empieza por 'https://' es muy buena señal. Al momento de que se abre el enlace, y esta de color verde y con un candado significa que la pagina si es verídica es decir es de quien dice ser.

Si no empieza con 'https://' o no tiene el candado cerrado, se puede acceder a la información y ver si la conexión no nos va a afectar

Tipos de ciberataques en WhatsApp

Ingeniería social por mensajes

Una herramienta que ayuda a los ciberdelincuentes atravez de WhatsApp es la ingeniería social para estafar con mensajes falsos.

Unos de sus mayores trucos es enviar un mensaje diciendo que se han enviado por error un mensaje con 6 dígitos a dicho celular, y si puede dar a conocerlos.

Se trata de un código de autenticación en dos pasos.

El cual tiene como función que el ciberdelincuente pueda entrar a una red social, o en cualquier servicio haciéndose pasar por la victima al momento de dale el código el atacante podrá hackear nuestros mensajes de WhatsApp

Figura 4. La ingeniería social

¿Cómo funciona?

- Hacerse pasar por un familiar un conocido un compañero de trabajo.
- Ofrece a la víctima premios y promociones únicas ilimitadas que son falsas a cambio de sus datos.

- Se hace pasar por la persona responsable del sistema para obtener los datos de esta persona es decir de la víctima.
- Invitar a completar formularios los cuáles son falsos para ganar un premio o un producto.
- Ofrecer actualizaciones de navegadores o de distintas aplicaciones a través de páginas las cuales son falsas.

Figura 5. Estafas

¿Cómo me protejo?

- No entregar datos personales a personas completamente desconocidas por ningún medio de comunicación menos por WhatsApp.
- Configurar la privacidad de redes sociales que se tengas en uso sobre todo WhatsApp que es la más utilizada para que no queden expuestos nuestros datos.
- Usar contraseñas seguras es decir no escoger nombre ni fechas especiales.
- No dar menor importancia a cualquier persona que pida información tanto personal como laboral.

Una falsa actualización

Uno de los casos más temidos y peligrosos en la aplicación de mensajería ha sido la falsa actualización. Un virus de WhatsApp camuflado, en una actualización de las aplicaciones de mensajería. Pues de esta forma las víctimas fueron infectadas con el malware breta capaz de espiar todo lo que dicen sus víctimas, puesto que se encarga de realizar un espejo de la pantalla de su dispositivo, y de esta manera puede tener información confidencial de ellos acceso a sus cuentas a sus mensajes etc.

Figura 6. Falsa actualización

¿Cómo funciona?

Si este programa maligno te infecta será capaz de espiar todo lo que se realice en su celular, a través de la pantalla de este con lo que podrían conocer sus claves bancarias su correo electrónico sus redes sociales.

saber las conversaciones de sus vidas privadas y laborales que tienen en su celular.

Lo malo es que malware está oculto al usuario es decir no lo puede ver.

Pero en concreto breta coloca una superposición en la pantalla de la víctima para ocultar la actividad que realizan los delincuentes, los cuales están controlando remotamente el dispositivo o equipo que esté utilizando.

Figura 7. No son actualizaciones reales

¿Cómo me protejo?

La manera en la que se puede proteger es comprobando que sean sitios legítimos y no malicioso, de los cuales se pueden de descargar aplicaciones pues si la descarga de otra aplicación que no es segura puede traer problemas.

Ataques a WhatsApp con su objetivo, definición, como afecta a WhatsApp, y prevención.

Ingeniería social

Objetivos

- Obtener información privada de la victima
- Engañar a la victima

Definición

- **Ingeniería social:**
  Sirve para manipular mediante chantaje a las personas más incautas, con el objetivo de acceder sistemas críticos con información totalmente confidencial y privada de mucho valor para la organización.

Afectación a WhatsApp

- **¿Cómo afecta a WhatsApp?**
  Una vez que se aplica este malware se puede ver lo que hace el usuario en la pantalla de su celular, se puede ver las acciones que realiza y eso lo pueden usar los ciber atacantes pues pueden ver sus conversaciones privadas por medio de la red social WhatsApp, el medio más utilizado en la actualidad para la comunicación donde compartimos información confidencial información que ellos pueden ver y con la que pueden chantajearnos los atacantes.

Prevención

- Poner en uso un software de total de seguridad y confianza.
- Si le llega mensajes de que gano un premio o que fue seleccionado para ganar algo, muy probablemente sea falso.
- Investigar de quien o de donde viene el mensaje

Fallas en los sistemas informáticos

Objetivos

- Aprovechar las fallas
- Poder hurtar todos los datos almacenados

Definición

- **Fallas en los sistemas informáticos**
  Se puede descifrar como deficiencias al momento de que los desarrolladores diseñan los sistemas que van a hacer utilizados y es allí cuando los atacantes aprovechan.

Afectación a WhatsApp

- **¿Cómo afecta a WhatsApp?**
  Afectan revelando que los fallos en los sistemas informáticos explican que WhatsApp puede revelar la información que contenga el dispositivo, y los hackers tiene total acceso a los archivos almacenados en el celular de la víctima.

Prevención

Normalmente se deberían usar para que no venga con fallos los sistemas con los que viene nuestros Smartphone

- Un equipo con una confiabilidad mayor (MTBF)
- Incluir los equipos de protección adecuados.

Enlace falso

Objetivos

- Robar información.
- Estafar a las víctimas.

Definición

- **Enlace falso**

Si un enlace falso se marca como sospechoso, al darle clic se abrirá una ventana de emergencia que destacará el carácter inusual dentro de él.

Afectación a WhatsApp

¿Cómo afecta a WhatsApp?

Atravez de WhatsApp se puede recibir enlaces falsos, no solo pueden ser contactos que no conocemos estos enlaces pueden venir desde alguien de confianza, esta persona puede ser un amigo o familiar.

Prevención

- Comprobar quien envía el mensaje.
- Observar el contexto del mensaje.
- Revisar letras de enlace.

Virus

Hay varias interrogantes que los usuarios nos hacemos cuando hablamos de ataques a red social de WhatsApp entre estas interrogantes se encuentran:

¿Qué son los virus en WhatsApp?

Los virus que pueden atacar a la red social WhatsApp son programas peligrosos los cuales fueren creados por Piratas informáticos, también conocidos como ingenieros informáticos a los que se les denomina con hackers.

¿Qué buscan los hackers?

Los hackers o piratas informáticos buscan estafar y robas a los usuarios toda la información que contengan para esto existen distintos virus.

¿Cuáles son los virus que pueden atacar a WhatsApp?

Existe una diversidad de virus, pero mostrare los 10 tipos de virus más usados para atacar WhatsApp.

- **WhatsApp Gold**

  Los ciber atacantes pueden difundir esta estafa a través de un contacto desconocido o hacerse pasar por una persona conocida.
  Se suele presentar como una nueva versión de Gold premium, de la aplicación con supuestas nuevas herramientas y más funciones avanzadas.
  Cuando el usuario o victima da clic para realizar la descarga aparece en un sitio infectado en el que está expuesto a muchas amenazas.

- **GhostCtrl**

  Es una aplicación dedicada a el fraude, que se disfraza de la versión oficial de la red social WhatsApp.
  Normalmente sus víctimas son aquellos que descargan programas de ciertos sitios es decir son ilegales o de dudosa procedencia.
  La interfaz de GhostCtrl es igual al servicio de mensajería también tiene sus funciones sus características de que es un software legal.
  Pero al instalarlo en nuestro dispositivo los ciber delincuentes pueden ver la lista de contactos, nuestra localización por el GPS, el historial de navegación es decir las cosas que hemos visto en nuestro celular cuando hemos navegado en internet, el registro de nuestras conversaciones y mucho más también lo que pueden hacer es habilitar cámaras y hasta micrófonos de forma remota para espiarnos.
  En cualquier momento sin que nos demos cuenta por esta sencilla razón no se recomienda bajar las aplicaciones de páginas ilegítimas sino únicamente de las tiendas oficiales de iOS y Android.

- **Mensaje de voz perdido**

  Este virus de la red social WhatsApp ataca de manera muy extraña, pero a pesar de eso ha logrado mentir a muchas víctimas.

  Primero se recibe en su email la alerta de un supuesto mensaje de voz perdido con un enlace para escucharlo, después de que usted caiga en esta coartada.

  Se abrirá una página maliciosa con enlaces que ya están infectados, y los pasos para descargar o software malicioso cómo Browser de esta forma también puede ser atacado por Ransomware un virus que retiene su celular y pide un rescate para devolverlo.

- **Periodo de prueba**

  Un mensaje le da a conocer a la víctima que disponía de un periodo de prueba, totalmente gratuito de un año que ya no existe más pues expiró, de esta forma le mienten para que acceda a un portal del cliente donde debe ingresar sus datos personales, para poder seguir utilizando la red social WhatsApp, le piden agregar los datos de la tarjeta de crédito para darle un año de suscripción dejando el camino completamente despejado a los ciber delincuentes para cometer sus delitos financieros.

- **ZooPark**

  Este software peligroso troyano fue creado para acceder a los contactos y obtener toda la información posible, sobre las cuentas de la red social WhatsApp.

  Con el tiempo el software ha evolucionado y ahora es capaz de hurtar fotos, vídeos y lo que sea que se tenga almacenado en el celular,

acceder a los archivos, ver el historial de navegación hasta activar cámara y micrófono en tiempo real.

Este software tan malicioso accede a nuestro smartphone a través de páginas de descargas banners infectados o links sospechosos.

- **Tizi**

Es un virus de la red social WhatsApp que ataca a los equipos Android, para lograr tener una agenda de datos personales desde varias aplicaciones.
Hasta hace poco este virus spyware se obtenía en la tienda oficial de Play Store, por lo que muchas víctimas resultaron afectadas.
Tizi tiene como función principal robar el historial de los chats, grabar las llamadas y hurtar toda su lista de contactos.

- **Brata**

Los ciber delincuentes han logrado que brata este en alguna de sus actualizaciones de la aplicación, para poder espiar todas las actividades que hace la víctima chats, llamadas, videollamadas listas de contactos, ubicación, fotos, vídeos y demás.
La compañía puso en marcha el plan para evitar esta amenaza, te aconsejamos revisar entre los archivos descargados para descartar que haya sido infectado.

- **GIF infectado**

El Instituto nacional de ciberseguridad de España alertó que un grupo de personas estaban recibiendo muchos GIF maliciosos.

Estas imágenes enviadas por medio de WhatsApp pueden robar archivos, también pueden acceder a nuestras fotos, nuestros vídeos, grabar las llamadas y obtener tanto el historial de los mensajes de voz como los de texto.

Los expertos piden mantener la aplicación actualizada para no poder hacer atacados por este gusano.

- **Archivos Word, excel y PDF**

La Policía Nacional pone una alerta hace algunos años por un virus que está afectando a WhatsApp, que se estaría propagando en el formato de Word en el de Excel y PDF.

Por lo que pedían no abrir este tipo de archivos que vengan de contactos desconocidos.

Los archivos pueden ser identificados por varios nombres, puede ser un libro también un concurso para ganar dinero.

Pero lo que en realidad quieren los hackers, es entrar a su celular móvil y robarle todo el dinero que se les da posible.

- **Sorteo de un iPhone**

Son engañadas al momento que le llega a su celular un mensaje de felicitaciones por haberse ganado el celular o son agregados a un grupo, con números desconocidos haciéndoles creer que han ganado el sorteo.

Después de dar clic en un link manipulado, Son dirigidos a una página muy bien elaborada y esta le pide los datos de la tarjeta de crédito.

Para continuar así el proceso solo se necesitará tiempo, para que los cálculos de grandes cantidades aparezcan en su factura de la tarjeta de crédito.

Prevenciones

Para no ser víctima de ningún virus que puede atacar a WhatsApp:

- Se pide ser precavido con los mensajes que reciben en la aplicación de WhatsApp o en su correo electrónico.
- No ingrese a enlaces que dicen que son sorteos premios o promociones que le llegan de números que no tienen registrados.
- Por todos los ataques que puede existir deberá tener instalado un antivirus, en el cual usted tenga confianza que sepa que lo va a proteger de todos los peligros y los virus de la red.
- No ignore los virus de Phishing de Smishing o de Vishing estos son los delitos informáticos más usados por los hackers, ciber delincuentes o piratas informáticos y los más comunes en el momento

¿Cómo puede afectar todos los temas expuestos a la entidad asesorarte?

Puede afectar en mucho a la empresa con los virus mencionados pues las personas en la empresa no tienen conocimiento, acerca ni de los virus ni de los problemas que pueden traer, tanto en ellos como en sus clientes.

Sabemos que WhatsApp es una de las aplicaciones más utilizadas en la actualidad y en todo el mundo y “ASESORARTE” no es la excepción, pues usan la aplicación de WhatsApp para comunicarse entre ellos mismos y con sus clientes.

Cualquiera de los factores o de los problemas que se han mencionado anteriormente en esta guía, se pueden sufrir en la entidad ya sea un colaborador o un cliente, para evitar y prevenir esos problemas es que se ha elaborado esta guía.

Los virus que están mencionados no solo pueden afectar a nuestro WhatsApp por medio smartphones sino también a nuestro WhatsApp web.

Pues los mismos problemas que son presentados en los celulares también puede ser presentados en WhatsApp web, y es un problema en la entidad cuando llegan a trabajar los colaboradores cada uno tiene su propio ordenador, conectan allí WhatsApp web, y empiezan a trabajar comunicándose entre ellos y con sus clientes.

Conclusiones

- La elaboración de esta guía metodológica facilitara la comprensión de que son los virus y de qué manera pueden afectar a nuestra red WhatsApp.
- Esta guía metodológica es un instrumento que nos da a conocer información necesaria para orientar sobre cuáles son las prevenciones que debemos aplicar.
- No hay duda de que los ataques han sido terribles pues los delincuentes ganan mucha información, pero ahora se podrán resolver estos ataques con la guía.

Recomendaciones

- Para evitar que los ataquen no haga clic en los enlaces de dudosa procedencia o que le resulten sospechosos.
- No ignore las prevenciones esto le ayudara a resguardar su información de los hackers.
- Hay que poner en práctica la guía para evitar caer en estos ataques e informarse con que clase de virus y ataques pueden manejar los ciberdelincuentes para sus fines.