Evaluación del desempeño y análisis del grado de seguridad entre un sistema de correos electrónicos tradicional con protocolo SMTP (Simple Mail Transfer Protocol) y un sistema de correo electrónico cifrado, con implementación de una firma digital usando el protocolo PGP (Pretty Good Privacy)

Gamboa Romero, Christian Andrés

Departamento de Eléctrica, Electrónica y Telecomunicaciones

Carrera de Ingeniería en Electrónica y Telecomunicaciones

Trabajo de titulación, previo a la obtención del título de Ingeniero en Electrónica y Telecomunicaciones

M.Sc. Romero Gallardo, Carlos Gabriel

19 de junio del 2023

Resultados de la herramienta prevención y/o verificación de similitud de contenidos

Informe de originalidad

NOMBRE DEL CURSO
TESIS

NOMBRE DEL ALUMNO
CHRISTIAN ANDRES GAMBOA ROMERO

NOMBRE DEL ARCHIVO
CHRISTIAN ANDRES GAMBOA ROMERO - Documento Tesis para comprobar originalidad

SE HA CREADO EL INFORME
10 may 2023

Resumen

Fragmentos marcados	5	0,6 %
Fragmentos citados o entrecomillados	1	0,1 %

Coincidencias de la Web

mailjet.com	4	0,5 %
victorhckinthefreeworld.com	1	0,1 %
docplayer.es	1	0,1 %

1 de 6 fragmentos
Fragmento del alumno MARCADO

Trabajo de titulación, previo a la obtención del título de Ingeniero en Electrónica y Telecomunicaciones

Mejor coincidencia en la Web

Para esto, **los servidores DNS** comprueban **con los registros SPF si la IP del servidor** desde el que **se envía tiene relación con el dominio**. ¿Que es el DKIM?

SPF, DKIM y DMARC: Por qué usarlos y cómo configurarlos - Mailjet https://www.mailjet.com/es/blog/entregabilidad/spf-dkim-dmarc-como-configurar/

5 de 6 fragmentos
Fragmento del alumno MARCADO

…**El objetivo** de este **protocolo** además de **demostrar que el nombre** del **dominio no ha sido** apoderado, **también** es **que** le **mensaje no** haya **sido alterado durante la transmisión**

Mejor coincidencia en la Web

El objetivo del **protocolo** DKIM no es sólo **demostrar que el nombre** de **dominio no ha sido** usurpado, sino **también que** el **mensaje no** ha **sido alterado durante la transmisión**. ¿Que es DMARC?

SPF, DKIM y DMARC: Por qué usarlos y cómo configurarlos - Mailjet https://www.mailjet.com/es/blog/entregabilidad/spf-dkim-dmarc-como-configurar/

6 de 6 fragmentos
Fragmento del alumno ENTRECOMILLADO

…Dentro **del** programa dirigirse **a** la **cuenta >> Configuración >> Cifrado Extremo a Extremo >> Administrador de claves OpenPGP**

Mejor coincidencia en la Web

Si tenemos la clave pública **del** contacto en un archivo en nuestro equipo en formato .asc para importar esta a Thunderbird deberemos ir **a** nuestra **cuenta**, en el menú de las barras horizontales: …

Importar una clave de cifrado en Thunderbird con OpenPGP https://victorhckinthefreeworld.com/2021/01/07/importar-una-clave-de-cifrado-en-thunderbird-con-openpgp/

Departamento de Eléctrica, Electrónica y Telecomunicaciones

Carrera de Ingeniería en Electrónica y Telecomunicaciones

Certificación

Certifico que el trabajo de titulación: "**Evaluación del desempeño y análisis del grado de seguridad entre un sistema de correos electrónicos tradicional con protocolo SMTP (Simple Mail Transfer Protocol) y un sistema de correo electrónico cifrado, con implementación de una firma digital usando el protocolo PGP (Pretty Good Privacy)**" fue realizado por el señor **Gamboa Romero Christian Andrés;** el mismo que cumple con los requisitos legales, teóricos, científicos, técnicos y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, además fue revisado y analizado en su totalidad por la herramienta de prevención y/o verificación de similitud de contenidos; razón por la cual me permito acreditar y autorizar para que se lo sustente públicamente.

Sangolquí, 16 de mayo del 2023

CARLOS GABRIEL ROMERO GALLARDO

Ing. Romero Gallardo, Carlos Gabriel

C. C 1712198066

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

Departamento de Eléctrica, Electrónica y Telecomunicaciones

Carrera de Ingeniería en Electrónica y Telecomunicaciones

Responsabilidad De Auditoría

Yo, **Gamboa Romero Christian Andrés**, con cédula de ciudadanía N°1727098533, declaro que el contenido, ideas y criterios del trabajo de titulación: **Evaluación del desempeño y análisis del grado de seguridad entre un sistema de correos electrónicos tradicional con protocolo SMTP (Simple Mail Transfer Protocol) y un sistema de correo electrónico cifrado, con implementación de una firma digital usando el protocolo PGP (Pretty Good Privacy)** es de mi autoría y responsabilidad, cumpliendo con los requisitos legales, teóricos, científicos, técnicos, y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, respetando los derechos intelectuales de terceros y referenciando las citas bibliográficas

Sangolquí, 16 de mayo del 2023

.....

Gamboa Romero, Christian Andrés

C. C.: 1727098533

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

Departamento de Eléctrica, Electrónica y Telecomunicaciones

Carrera de Ingeniería en Electrónica y Telecomunicaciones

Autorización de Publicación

Yo, **Gamboa Romero Christian Andrés**, con cédula de ciudadanía N°1727098533, autorizo a la Universidad de las Fuerzas Armadas ESPE publicar el trabajo de titulación: **"Evaluación del desempeño y análisis del grado de seguridad entre un sistema de correos electrónicos tradicional con protocolo SMTP (Simple Mail Transfer Protocol) y un sistema de correo electrónico cifrado, con implementación de una firma digital usando el protocolo PGP (Pretty Good Privacy)"** en el Repositorio Institucional, cuyo contenido, ideas y criterios son de nuestra responsabilidad.

Sangolquí, 16 de mayo del 2023

.....

Gamboa Romero, Christian Andrés

C. C.: 1727098533

Dedicatoria

Dedico el presente trabajo primero a Dios y a mis padres, Edguin y Lilia por su amor incondicional y su apoyo infinito, siempre estando a mi lado en todo momento y demostrando un verdadero ejemplo de superación, siendo una gran motivación para lograr cumplir mis objetivos. A mi hermano Eduardo por estar a mi lado en los momentos más difíciles, apoyarme con sus consejos y ser un ejemplo a seguir. Finalmente, a toda mi familia y amigos por ser una pieza fundamental para obtener este importante logro en mi vida profesional.

Este logro es para todos ustedes.

Christian Andrés Gamboa Romero

Agradecimiento

Agradezco en primer lugar a Dios por permitirme llegar a culminar una etapa más en mi vida, a mi padre y madre que con su amor incondicional me han apoyado para no abandonar mis estudios cuando las cosas se ponían difíciles, gracias por su apoyo y su guía para poder culminar una meta más en mi vida profesional.

A mi hermano que me ha apoyado en este largo camino, con sus consejos y enseñanzas, siendo un ejemplo que seguir, gracias por darme ánimos para poder concluir con mis estudios universitarios.

A mis amigos que fueron una pieza fundamental durante toda mi carrera universitaria, gracias por su amistad y por nunca dudar de mis capacidades durante todo este trayecto.

A la Universidad de las Fuerzas Armadas “ESPE” por formarme académicamente, a mis profesores que han sido un pilar importante durante mi etapa universitaria, a mi director de tesis, Ing. Carlos Romero, gracias por su confianza, paciencia y apoyo a lo largo de la realización del proyecto.

Christian Andrés Gamboa Romero

Contenido

Índice de Tablas

Índice de figuras

Resumen

El correo electrónico es el medio de comunicación más utilizado por las empresas para compartir información entre sus empleados, proveedores y clientes sea ésta de carácter público o privado, no obstante, el protocolo utilizado para dicho intercambio de información es SMTP, el cual transmite la información en texto plano a través de la red, lo cual lo vuelve vulnerable a ser interceptado durante su transporte. Dentro de los procesos de seguridad es imprescindible garantizar la privacidad, confidencialidad y disponibilidad de la información, más aún durante las comunicaciones entre colaboradores (ejemplo transmisión de contraseñas), es por ello por lo que se plantea la utilización de cifrado en ambos extremos mediante correo electrónico con GPG, es necesario realizar un análisis y comparativa entre los dos protocolos utilizados en los sistemas de correos electrónicos para verificar el sistema que brinda más seguridad dentro de una organización. Este sistema permitirá que todos los emails enviados desde cualquier cliente de correo configurado sean cifrados con las claves públicas de los destinatarios y solo podrán ser leídos por el personal que disponga de la clave privada de cada cuenta, de igual manera al recibir los correos electrónicos los destinatarios podrán confirmar mediante la firma digital la autenticidad del remitente. Para garantizar la seguridad de la información transmitida el objetivo de GPG es proteger los datos enviados del acceso no autorizado por parte de terceros o personas externas, por lo tanto, los correos electrónicos cifrados no serán legibles ni podrán ser visualizados si estos son interceptados en su transporte.

Palabras clave: Protección de privacidad, Correo Electrónico, Texto cifrado, Firma electrónica, Protocolo Simple de Transferencia de Correo

Abstract

E-mail is the means of communication most used by companies to share information between their employees, suppliers and customers, whether public or private, however, the protocol used for this information exchange is SMTP, which transmits information in plain text through the network, which makes it vulnerable to interception during transport. Within the security processes it is essential to ensure the privacy, confidentiality and availability of information, even more so during communications between collaborators (e.g. transmission of passwords), which is why the use of encryption at both ends through email with GPG is proposed, it is necessary to perform an analysis and comparison between the two protocols used in email systems to verify the system that provides more security within an organization. This system will allow all emails sent from any configured email client to be encrypted with the public keys of the recipients and can only be read by personnel who have the private key of each account, likewise when receiving emails the recipients can confirm by digital signature the authenticity of the sender. In order to guarantee the security of the transmitted information, GPG's objective is to protect the sent data from unauthorized access by third parties or external persons, therefore, encrypted e-mails will not be readable nor can they be viewed if they are intercepted in transit.

Keywords: Privacy Guard, Email, Cipher Text, Electronic Signature, Simple Mail Transfer Protocol

Capítulo I

Introducción

Antecedentes

El correo electrónico es el sistema de intercambio de información más popular desde inicios del internet, permite que dos o más personas intercambien todo tipo de datos digitales sean estos: textos, documentos, audios, imágenes o videos, y su uso se mantiene en activo en la actualidad a pesar de que existan otros métodos de comunicación electrónica que se basan en sistemas móviles. (Whittaker, Belloti, & Gwizdka, 2006)

El funcionamiento del correo electrónico es similar al del correo postal, ya que los dos intercambian información entre personas, pero de forma inmediata, no es necesario que el destinatario esté en línea para que reciba el mensaje. Muchas de las empresas actualmente implementan y gestionan sus propios servicios de correo electrónico designando una dirección para cada uno de los usuarios, esto facilita la identificación de los destinatarios, hay que tener en cuenta que existen plataformas que conceden estos servicios de email de manera gratuita, entre los más conocidos y populares son Gmail, Hotmail y YahooMail.

El crecimiento de los sistemas de información ha causado que existan nuevas características en los servicios de correo electrónico, como es la transmisión de datos en texto plano hasta la implementación de controles de seguridad avanzados los cuales permiten que la información sea únicamente accesible para los destinatarios autorizados, garantizando los principios de la tríada CIA (Integridad, confidencialidad y disponibilidad). (Fenrich, 2008)

Cada vez existen mayores amenazas a la seguridad de la información que es transmitida por correo electrónico, es por ello que es necesario crear mecanismos que garanticen la confidencialidad y autenticidad de los documentos electrónicos, esto es parte de una tecnología llamada Criptografía, esta permite mediante el uso de distintos procedimientos

alterar la información de tal forma que sea legible únicamente por la persona que conozca el proceso de descifrado, esta técnica se utiliza para la protección de datos, documentos electrónicos, protocolos de comunicación y cualquier otro tipo de información digital.

Las características principales de la criptografía dentro de la seguridad informática es la de garantizar la privacidad de la información, proteger la integridad de los datos durante la transferencia de información y verificar la autenticidad de los usuarios, un mensaje puede ser codificado utilizando dos tipos de criptografía, entre ellas está la simétrica y la asimétrica. Es necesario argumentar que la criptografía simétrica utiliza la misma clave para cifrar y descifrar la información, mientras que la criptografía asimétrica utiliza una clave para cifrar, llamada clave pública y una diferente para descifrar, llamada clave privada. (Mendoza J. , 2018)

Justificación e importancia

El correo electrónico o e-mail, es el sistema de intercambio de información más antiguo y popular desde la creación de internet, permite que dos o más personas compartan todo tipo de datos digitales sean estos: textos, documentos, imágenes, audio y video y su uso se mantiene en auge a pesar de que en la actualidad existen otros métodos de comunicación electrónica principalmente basados en sistemas móviles. (Whittaker, Belloti, & Gwizdka, 2006)

La mayoría de las empresas implementan y gestionan sus propios servicios de correo electrónico asignando una dirección para cada uno de sus usuarios, lo que facilita la identificación de los destinatarios, sin embargo, también existen plataformas que ofrecen los servicios de email de forma gratuita, los más populares son Gmail, Hotmail y YahooMail.

Este tipo de correos maliciosos son enviados de forma masiva a direcciones de correo electrónico que han sido publicadas por filtraciones de datos, sin embargo, en ocasiones estos correos son personalizados para dirigirlos a una empresa o persona específica, esto es conocido también como Spear Phishing. Ya que el correo electrónico es el medio de

comunicación más utilizado por las empresas para compartir información entre sus empleados, proveedores y clientes sea ésta de carácter público o privado, no obstante, el protocolo utilizado para dicho intercambio de información es SMTP, el cuál transmite la información en texto plano a través de la red, lo cual lo vuelve vulnerable a ser interceptado durante su transporte. (Dhamija, 2006)

Dentro de los procesos de seguridad es imprescindible garantizar la privacidad, confidencialidad y disponibilidad de la información, más aún durante las comunicaciones entre colaboradores

Por las razones expuestas anteriormente se propone crear e implementar un sistema de firma en línea y la utilización de cifrado en ambos extremos mediante correo electrónico con GPG, y así proteger el intercambio de información entre los usuarios de la organización, además se plantea ciertas técnicas de control que se encargan de verificar la autenticidad del remitente y el origen confiable del mensaje, de esta manera evitar futuras estafas y suplantaciones de identidad por medio de correos electrónicos.

Este proceso de cifrado es aplicable tanto para clientes de correo como para Webmails, siempre y cuando el navegador web permita la integración con GPG

Alcance

El presente proyecto tiene como finalidad investigar y analizar el desempeño que tiene un sistema de correos electrónicos tradicional, el cuál usa el protocolo SMTP, frente a un sistema de correos electrónicos con cifrado y firma digital el cuál usa PGP, analizar sus ventajas y desventajas al momento de utilizar ciertos protocolos, realizar pruebas de seguridad en los dos sistemas de correo y realizar un análisis de riesgos de las vulnerabilidades que existen en la actualidad en los servidores de correo e implementar las mejores técnicas para poder protegerse de las amenazas cibernéticas.

Así mismo diseñar un sistema que brinde seguridad y reduzca el riesgo de un ataque y suplantación de identidad por correo electrónico, implementando un sistema de cifrado y firma en línea para realizar un intercambio de información de manera segura y evitando las suplantaciones de identidad entre los usuarios.

El cifrado de los correos electrónicos y la implementación de una firma en línea aumenta la seguridad de una empresa evitando futuros fraudes dentro del sistema de correos electrónicos, implementando un sistema de firma en línea el cual utilice GPG, esta herramienta permite obtener firmas digitales, su cifrado se basa en PGP (Pretty Good Privacy) y es distribuido bajo una licencia de software libre permitiendo firmar correos electrónicos de los usuarios de la organización.

Objetivos

Objetivo General

Realizar un análisis comparativo del desempeño y del grado de seguridad entre un sistema de correos electrónicos tradicional que usa el protocolo SMTP (Simple Mail Transfer Protocol) y un sistema de correos electrónicos con cifrado y firma digital, usando PGP (Pretty Good Privacy) para el intercambio de información segura entre los usuarios de una organización

Objetivos Específicos

- Realizar una investigación y comparar entre el sistema de correos que envía información en texto plano frente al cifrado de correos electrónicos e implementación de firmas digitales mediante el uso de la herramienta GPG.
- Analizar ventajas y desventajas que presenta el correo electrónico con protocolo SMTP y compararlas con el correo electrónico cifrado que utiliza el protocolo GPG.
- Realizar pruebas de seguridad en sistemas de correos electrónicos tradicionales sin cifrado para verificar el grado de riesgo que corre la información al ser transmitida.
- Diseñar un sistema que brinde seguridad y reduzca el riesgo de un ataque por correo electrónico mediante el uso de la herramienta GPG (GNU Privacy Guard).
- Realizar un análisis de riesgos de las vulnerabilidades que existen en la actualidad en los servidores de correos electrónicos e implementar las mejores técnicas para protegerse de las amenazas cibernéticas.
- Implementar un sistema de firma en línea para aumentar la seguridad en los correos electrónicos dentro de una empresa.
- Verificar que protocolos utilizados en los sistemas de correos electrónicos brindan mayor seguridad a una empresa para realizar el intercambio de información de manera segura y sin suplantaciones de identidad entre los usuarios.

Capítulo II

Marco teórico

Correo electrónico

A los inicios del internet con “Arpanet” y a lo largo de la historia la comunicación entre las personas ha sido un pilar fundamental en la evolución de las tecnologías, permitiendo compartir mediante tecnologías de mensajería gran cantidad de información de una manera ágil independientemente de la zona geográfica en la que se encuentren.

En la actualidad las tecnologías de mensajería van desarrollándose y adaptándose a las necesidades que presentan continuamente los usuarios, principalmente permiten la interacción con dispositivos móviles, la mayoría de estos sistemas son dotados de forma gratuita diferenciándose por las características según su objetivo.

Al paso de los años el correo electrónico se ha vuelto una pieza fundamental en la comunicación de las empresas, instituciones, servicios financieros, industriales y muchos más, permitiendo a los usuarios intercambiar cualquier tipo de información como textos, documentos, archivos multimedia, etc. (Whittaker, Belloti, & Gwizdka, 2006)

Características

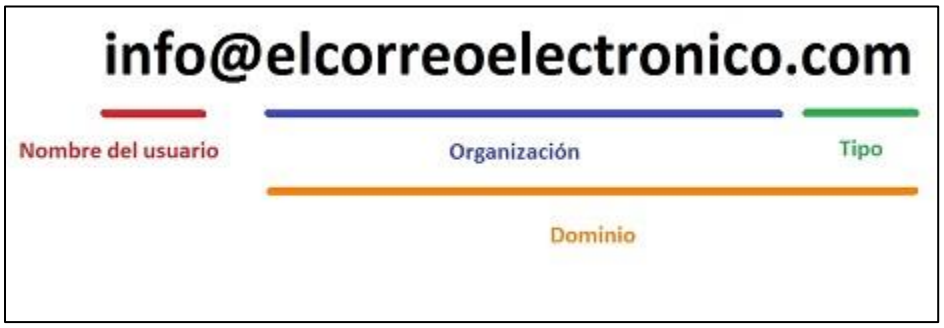
El correo electrónico es una herramienta muy utilizada en la actualidad, permite enviar como recibir mensajes a cualquier persona en el mundo, el email no solo permite enviar mensajes de texto, también facilita enviar archivos, imágenes, sonidos, etc.

Entre sus características más importantes se encuentra la de tener la facilidad y rapidez para compartir información, además de que es una de las herramientas más económicas para realizar estas acciones. Su rapidez se debe a que el proceso es inmediato, una vez que el emisor envíe el mensaje, su receptor lo recibe casi de forma instantánea. Hay que tener en

cuenta que este tipo de servicio se encuentra disponible los 365 días del año, salvo que exista algún fallo o inconsistencia en la red. Referente al aspecto ecológico se puede observar que no es necesario el uso de papel, por lo que este método ayuda a la sostenibilidad del medio ambiente.

Figura 1

Ejemplo de una dirección de correo electrónico



Nota: El gráfico representa un ejemplo de una dirección de correo electrónico. Tomado de: https://alfabetizaciondigital.fundacionesplai.org/mod/page/view.php?id=645

La dirección de correo electrónico está conformada principalmente de dos elementos:

- El nombre del usuario. Se sitúa a la izquierda del símbolo “@”, puede ser cualquier palabra que el usuario decida escoger siempre y cuando se encuentre disponible, es decir que otra persona no haya usado. Esto se debe a que no pueden existir más de dos direcciones de correo iguales, es única para cada usuario.
- El nombre del dominio. Está situada a la derecha del símbolo “@”, corresponde al servidor de correo electrónico donde está alojado, también se lo conoce como “host”.

Es importante destacar que los servidores de correo se clasifican de acuerdo con los niveles de dominio que conforman la dirección de correo electrónico. Entre ellos se encuentran los más conocidos como: "*.com*" (hace referencia a las entidades comerciales), "*.org*" (hace referencia a organismos no gubernamentales), ".gov" (para organismos gubernamentales), ".edu" (usados para instituciones educativas), ".net" (servicios de internet), entre otros.

El elemento final sirve para poder distinguir el país, son abreviaciones de dos letras, un claro ejemplo ".es" que identifica a España, o también ".co" para Colombia.

Protocolos de correo electrónico

Existen varios protocolos que permiten la comunicación de correos electrónicos, estos son encargados de establecer las conexiones necesarias de tipo cliente servidor y entre servidores:

Smtp: Protocolo simple de transferencia de email, este estándar está definido para el envío de correos electrónicos y permite comunicarse entre los servidores de correo mediante el puerto 25/TCP, los usuarios proceden a realizar una autenticación con el servidor antes del envío de los emails, este lo valida y reenvía a los destinatarios mediante los servidores de intercambio, definidos por los registros públicos de tipo Mail Exchanger. Se encuentra enfocado a la conexión en base al texto, esto quiere decir que tanto el remitente al igual que el receptor se comunican a través de secuencias de comandos y parámetros, proporcionando permisos y coordinando el tráfico de correos que se envían y reciben mediante el servidor SMTP.

Pop3: Post Office Protocol, este protocolo es el más utilizado por los clientes de correo electrónico para la lectura y recepción de emails, el servidor de correo entrega el correo al destinatario sin guardar una copia de este, es muy útil cuando se tiene varios GB de información por el almacenamiento de una gran cantidad de correos electrónicos, ya que en la

mayoría de los casos las cuotas de almacenamiento son limitadas, su puerto de comunicación es el 110/TCP.

Entre las ventajas principales que posee este protocolo, se encuentra que los mensajes solo se leen una vez y en el caso de no existir, el sistema se desconecta hasta la siguiente comprobación. A su vez potencia el uso del ancho de banda, los mensajes son almacenados de forma local, es por esta razón que se encuentran siempre a disposición del usuario.

Tabla 1

Ventajas y desventajas del protocolo POP3

VENTAJAS	DESVENTAJAS
- Potencia el uso de ancho de banda - El sistema se desconecta hasta la próxima comprobación de mensajes - Almacenamiento local - El espacio se limita en base al disco duro y no al del servidor	- Mayor probabilidad de que se infecte el dispositivo - Si falla el equipo se puede eliminar todos los mensajes - Al conectarse todos los mensajes se descargan automaticamente

Nota. En la tabla se muestra las ventajas y desventajas que posee el protocolo de correo electrónico POP3

Imap: Protocolo de Acceso a los Mensajes de Internet, este protocolo permite acceder al correo electrónico en cualquier ubicación que se encuentre y desde cualquier dispositivo, mediante una conexión por el puerto 143/TCP para la lectura de los emails, totalmente diferente a POP3. Es muy utilizado para la configuración en los dispositivos móviles ya que no es necesario disponer de una gran capacidad de almacenamiento. IMAP se diseñó como una moderna alternativa a POP.

Estos protocolos hablados anteriormente transmiten toda su información en texto plano, ya que su principal propósito no es proteger la información transmitida, sin embargo, es posible proteger la información mediante la utilización de TLS (Seguridad de la capa de transporte) y cifrar los datos en su transporte, los protocolos utilizados se los denomina SMTPS (587/TCP), POP3S(995/TCP) e IMAPS(993/TCP). (Lopez, 2009)

Su objetivo principal es permitir al usuario tener una gestión completa del buzón de correo mediante distintos clientes de emails. Este protocolo es perfecto si se desea utilizar sistemas de *webmail* y más de un cliente de correo diferente. De igual forma algunos servidores permiten que varios usuarios compartan el uso de carpetas. Algunos servicios de correo que utilizan este protocolo son: Outlook, Gmail o Yahoo.

Una de las principales ventajas que ofrece IMAP es que comunica si ha llegado un correo, esto es posible gracias a que funciona en modo conexión permanente. Sin embargo, tiene ciertas desventajas ya que se necesita de una conexión a internet para ver el mensaje.

Tabla 2

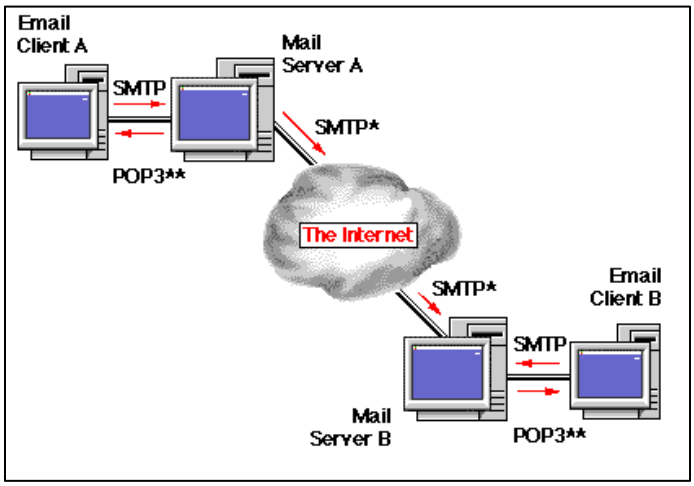
V*entajas y desventajas del protocolo IMAP*

VENTAJAS	DESVENTAJAS
- Mantiene conexión permanente - Alertas de mensajes - Almacenamiento local - Descarga de mensajes cuando el usuario lo requiera	- Necesita conexión a internet - Necesita transacción por cada mensaje - Las plantillas y borradores no podrán ser leídas con POP

Nota. En la tabla se muestra las ventajas y desventajas que posee el protocolo de correo electrónico IMAP

Figura 2

Diagrama de funcionamiento protocolos de correo electrónico



Nota: El gráfico representa el diagrama de funcionamiento de los protocolos de correo electrónico. Tomado de: https://sites.google.com/site/protocolopop3smtpms/introduccion/31.gif

Clientes correo electrónico

También conocido como MUA (Mail User Agent) son programas que permiten al usuario gestionar su correo electrónico de una manera organizada ya que son instalados en su dispositivo de forma local.

En la actualidad el uso de correo electrónico es esencial e indispensable, permite comunicarse de una manera rápida con otros usuarios, registrarse en alguna página web y compartir archivos con los demás. Se le puede dar una infinidad de usos, por ello es considerada una herramienta indispensable para el trabajo de cualquier persona. Para que una persona pueda aprovechar todas estas ventajas antes mencionadas es necesario que tenga una cuenta de correo electrónico, estas cuentas pueden ser de dos tipos y dependiendo del uso que la persona le vaya a dar. Se diferencia entre el correo electrónico personal y el correo electrónico empresarial o profesional.

El correo electrónico personal se caracteriza porque tiene una función no tan formal, es utilizada para la comunicación entre amigos o familiares, registros en páginas web, etc.

Por otro lado, el correo electrónico empresarial o profesional se caracteriza porque su función es formal, este es utilizado con fines empresariales para el trabajo, las empresas proporcionan estos servicios a sus empleados para que puedan llevar de mejor manera la información.

Existen varias diferencias entre estos dos tipos de correos, el personal se puede acceder mediante cualquier sitio, dispositivo o ubicación, mientras que los empresariales generalmente solo se puede acceder desde dispositivos proporcionados por la empresa y desde su trabajo. De igual forma este tipo de correo suele tener limitada la configuración para realizar cambios en el mismo. Un aspecto muy importante que destacar es su seguridad, generalmente se usa contraseñas más robustas y extensas por el hecho de evitar que la información sea sustraída por terceros, ya que esto puede ser crítico para las empresas. (Gargallo, 2021)

En fin, estas empresas ofrecen servicios tanto de envío como recepción de emails de manera automática. Existe una gran cantidad de proveedores para poder llegar a todos los tipos de clientes, cada uno ofreciendo características diferentes dependiendo la necesidad del usuario.

Servicios gratuitos y pagados

Ya visto los conceptos del software que ofrece gestionar los emails, también llamado como cliente de correo electrónico y la empresa que permite el medio para tener una cuenta de correo, llamada proveedor de correo electrónico. Es necesario aclarar que estos servicios se los puede encontrar de forma gratuita, sin embargo, se puede conseguir ciertos privilegios o

funciones si se opta por la opción premium. Estas características se encuentran detalladas a continuación.

Figura 3

Características de Gmail, Outlook y Thunderbird

	GMAIL	OUTLOOK	THUNDERBIRD
Creador	Google	Microsoft	Mozilla
Fecha de Lanzamiento	2004	1996	2003
Sede	Estados Unidos	Estados Unidos	Estados Unidos
Plataformas	IOS, Android y Navegador Web	IOS, Android, Windows, Navegador Web	Windows, Mac OS, Linux
Versión Gratuíta	Sí	Sí	Sí
Servicios Premium	Sí	Sí	No
Código Abierto	No	No	Sí
Almacenamiento	15Gb	15GB	Depende de la capacidad del disco del dispositivo
IMAP, SMTP y/o POP	Sí	Sí	Sí
Extras	Etiquetas, calendario, bloquear usuarios, filtros, listas de tareas	Calendario, lista de tareas, libreta de direcciones	Gran variedad de complementos, extensiones, temas

Nota: El gráfico representa las características de Gmail, Outlook. Y Thunderbird. Tomado de: (Gargallo, 2021)

Gmail

Es un servicio de correo electrónico más conocido en todo el mundo, ya que ofrece ciertas funciones de manera gratuita. Fue creado por la empresa Google y si lanzamiento fue en el año 2004. Una de sus características más importante y la cual le convirtió en uno de los servicios más conocidos fue la integración de un motor de búsqueda en el mismo correo

electrónico. Su almacenamiento tuvo un crecimiento hasta los 15 GB, estos relacionados con el servicio de Google Drive, todo esto de forma gratuita, sin embargo, ofrece un aumento de espacio por un costo adicional. Entre las características principales es que permite relacionarse con otros servicios de Google, facilita vincularse en otras cuentas desde otros dispositivos y es muy conocido por tener un buen filtro de spam. En la actualidad Gmail viene preinstalado en ciertos teléfonos con el sistema operativo Android.

Outlook

Outlook es otro de los servicios más conocidos y populares en la actualidad, ya que de igual forma es gratuito y ofrece un sin número de características para todos los usuarios. Este servicio fue creado por Microsoft en el año 1996, anteriormente se lo conocía como Hotmail. Al igual que Gmail, ofrece 15 GB de almacenamiento gratuito y permite enviar archivos adjuntos de hasta 20 MB. Su principal ventaja es que se puede sincronizar de una manera fácil y rápida con diferentes aplicaciones de Microsoft.

Thunderbird

Este servicio es uno de los más conocidos como alternativas de los hablados anteriormente, tanto para su uso personal como el profesional. Thunderbird fue creado en el año 2003 por la Fundación Mozilla. Una de sus ventajas principales es que es un correo electrónico multiplataforma gratuito, es decir que puede gestionar al mismo tiempo varias cuentas de correo electrónico. Su espacio de almacenamiento puede aumentar dependiendo del espacio libre que el usuario tenga en el disco del dispositivo. Entre sus características principales es que está formado por un proceso de código abierto, con la finalidad de proteger de mejor manera el correo. Otra de sus ventajas es que permite una gran capacidad de personalización, desde temas hasta extensiones.

Amenazas de correo electrónico

El correo electrónico en las últimas décadas se ha convertido en un servicio muy utilizado, es por ello por lo que también es un vector potencial de ataque a las empresas y persona, existen muchas amenazas a las que se enfrentan los usuarios, entre ellas están:

Spam: También conocido como correo basura, son todos los emails no solicitados o que no son deseados por el usuario, al día se envían miles de correos con publicidad, mensajes ofreciendo nuevos servicios, ofertas de productos y compras, que al ser reportados como no deseados por los destinatarios se los categoriza como SPAM para que los gestores de correos prevengan esta información a los receptores. Se los denomina como spammer a las personas que se dedican a enviar este tipo de correos

***Phishing*:** El término asocia al delito de engañar a las personas para que compartan información confidencial, ya sea contraseñas, números de tarjetas de crédito, o cualquier dato que pueda tener algún valor comercial, esta es la forma más sencilla de ciberataque y al mismo tiempo es una de las más peligrosas y efectivas, a diferencia de otros ataques el Phishing no requiere que el atacante tenga conocimientos avanzados y sofisticados, ya que existen programas y páginas web que brindan estos servicios pagando un valor económico. Este tipo de ataque no se centra en afectar al sistema operativo del dispositivo, si no que utilizan la ingeniería social para aprovecharse de la víctima.

Entre los casos más comunes son los correos electrónicos que se hacen pasar por entidades financieras, las cuales solicitan información a sus clientes, haciéndoles creer que deben actualizar sus datos y contraseñas de acceso a las bancas virtuales, las víctimas que caen engañados suelen verse afectados en los estados financieros por transacciones y consumos no autorizados. (Dhamija, 2006)

Estos correos electrónicos maliciosos suelen enviarse de forma masiva a correos que han sido publicados por varias filtraciones de datos, muchas de las veces esos correos son personalizados y dirigidos a una empresa o persona específica, esto es conocido como Spear Phishing.

***Bec*:** Conocido como el fraude del CEO, Business Email Compromise es una técnica avanzada de engaño y suplantación de identidad, que tiene como objetivo principal incursionar en las empresas.

Esta técnica consiste en que los ciberdelincuentes simulan ser de una fuente confiable y conocida, envían un correo solicitando se realice una acción, esto puede ser una solicitud de pago de una factura en una nueva cuenta, también puede ser que el director ejecutivo solicite al personal de finanzas se realice una transferencia de dinero a una cuenta externa de los delincuentes, o finalmente puede ser una oferta de compra con nuevos precios y descuentos atractivos para la empresa.

El atacante inicialmente identifica el objetivo, recoge información y perfila a los empleados, luego implementa técnicas de ingeniería social para atacar y engañar a los empleados, finalmente solicita información o transferencia de archivos o dinero y la victima accede a realizar lo solicitado completando de manera exitosa el ataque. Para lograr vulnerar los controles de los servidores de correo y llegar a cumplir el objetivo deseado, los atacantes realizan pequeñas modificaciones en los dominios o cuentas de correo, cambiando caracteres que se asemejan como las letras “i” por la “l”, “o” por “0”. (Rincón Nuñez, 2021)

***Email Hijacking*:** Esta es una de las técnicas avanzadas que se realiza mediante email, se basa en el secuestro de hilos de correo electrónico, un atacante puede utilizar una conversación de correo antigua para lograr obtener confianza y descuido de los usuarios y así

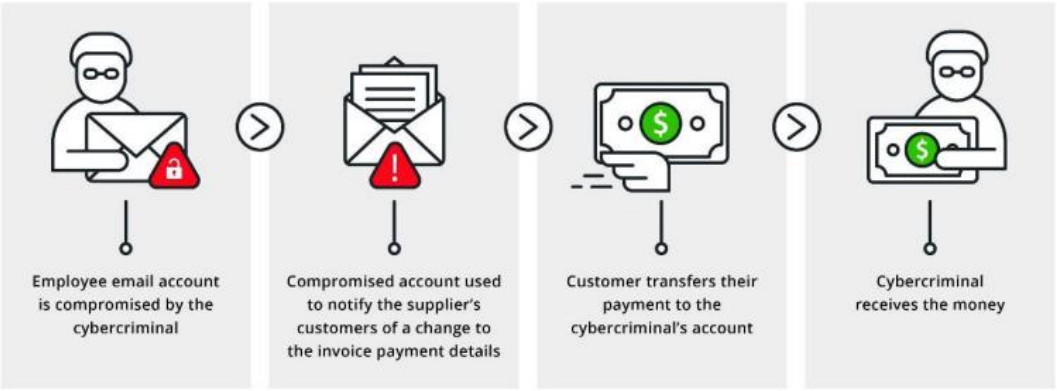
poder enviar archivos adjuntos maliciosos para obtener acceso a las cuentas y sus equipos de los empleados.

Se trata de simular una respuesta legítima de email a un hilo de conversación que ya existe, suplantando el nombre de alguno de los contactos a quien fue inicialmente enviado, al ser una respuesta a una conversación previa las víctimas asumen que es legítima, esto puede afectar gravemente a la seguridad de los equipos de una empresa.

En estos tipos de ataques es común ver archivos adjuntos de ofimática con nombres como, Reunión, Acuerdos, Facturas, y sus respectivas variaciones adaptándose al idioma de los diferentes países en donde se encuentre la empresa. (MITRE.ORG, 2021)

Figura 4

Business Email Compromise Attack



Nota: El gráfico representa el diagrama de funcionamiento de Business Email Compromise Attack. Tomado de: https://sysnetgs.com/wp-content/uploads/2018/09/Business-Email-Compromise-Attacks-and-How-to-Protect-Your-Business-08.jpg

***Spear Phishing*:** Este es un tipo de estafa que se realiza mediante correo electrónico a personas u organizaciones específicas, su objetivo principal es robar datos, sin embargo, los ciberdelincuentes también pueden tratar de instalar malware en el equipo de la víctima.

Estos ataques funcionan de la siguiente manera, al momento de que llega un correo electrónico, que parece ser de una fuente confiable y lo dirige al destinatario a un sitio web falso que contiene una gran cantidad de malware, estos correos utilizan tácticas avanzadas e inteligentes para poder captar la atención de los usuarios.

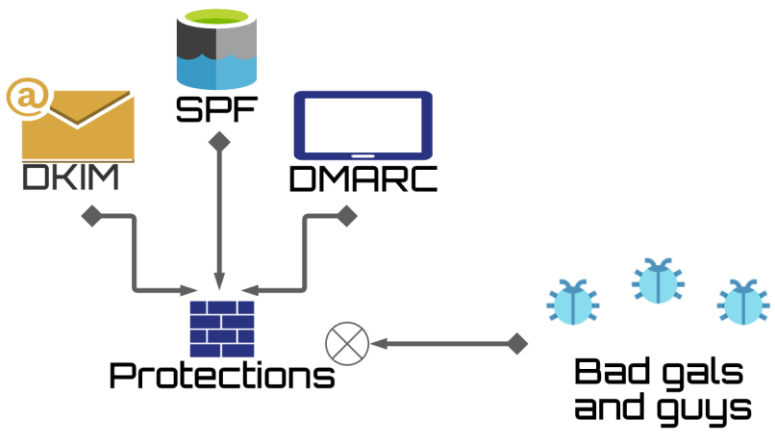
Los ataques son lanzados por ciberdelincuentes con la intención de obtener datos confidenciales y revenderlos a gobiernos o empresas privadas. Se aplica enfoques diseñados individualmente y tácticas modernas aplicando ingeniería social para poder personalizar de buena manera los mensajes y sus sitios web, estos correos pueden acabar siendo abiertos por altos ejecutivos, siendo esto crítico para la organización. (Kaspersky, 2022)

Seguridades de correo electrónico

Para poder prevenir varios de los ataques por correo electrónico presentados anteriormente existen algunos controles que se encargan de verificar la autenticidad del remitente y el origen confiable de la persona o entidad que envía el mensaje:

Figura 5

Protección de correos electrónicos



Nota: El gráfico representa los protocolos de seguridad de correos electrónicos (SPF, DKIM, DMARK). Tomado de: https://cdn.holvi.com/media/poolimage.image/2020/12/02/af6d8559fad6fb363dbdb12a5d76c272acfd75e4.png

***Spf*:** Sender Policy Framework es un estándar de autenticación el cuál vincula el nombre del dominio a una dirección de correo electrónico. Este protocolo consiste en definir cuál es el remitente que es autorizado para enviar correos con cierto dominio determinado. De esta forma los servidores de correo electrónico como Gmail u Outlook pueden comprobar que el email entrante proviene de direcciones IP o servidores autorizados. Para ello los servidores DNS verifican con los registros SPF si la IP del servidor del cuál se envía tiene relación con el dominio. Esta protección es configurada como un registro de DNS asociado al dominio del remitente y su estructura es de la siguiente manera: v=spf1 a mx -all. (Kontinen, 2020)

- Con la letra “a” se indica que la IP del dominio sea autorizada para enviar correos.
- Con “mx” se permite enviar correos desde las IP de los registros del dominio.
- El carácter “~” llamado softfail, indica que puede enviar un correo desde otra IP no especificada, sin embargo, este puede ir a no deseado.

Dkim: DomainKeys Identified Mail, este es un control que al igual que SPF se configura como un registro de DNS del dominio, el mismo hace uso del cifrado de claves público/privada para verificar la autenticidad del servidor de correo, a este se añade una firma que usa la clave privada y la misma es verificada por el destinatario usando la clave pública.

El objetivo de este protocolo además de demostrar que el nombre del dominio no ha sido apoderado, también es que le mensaje no haya sido alterado durante la transmisión del mismo. Los pasos para ocnfigurar DKIM son los siguientes:

- Se debe copiar la clave pública en los ajustes del correo electrónico
- Se accede al panel de control desde la cuenta de hosting
- Finalmente se crea un registro TXT, en el campo “value” se introduce la clave pública que se copió anteriormente.

La clave pública se encuentra en el campo TXT del registro DNS. Esta al ser utilizada el servidor del destinatario descifra la firma DKIM y posteriormente compara la información del contenido de correo, en el caso de que se encuentre alguna anomalía o inconsistencia el mensaje se dirige a la carpeta de Spam. (Kontinen, 2020)

***Dmarc*:** (Domain-based Message Authentication, Reporting and Conformance) es un estándar de autenticación de mensajes, informes y conformidad basada en dominios, este control es un registro DNS el cuál supervisa y monitorea el cumplimiento de los demás registros como es el SPF y DKIM, define las acciones a realizarse por el destinatario en caso de incumplimiento, puede elegir entre tres opciones diferentes: No hacer nada, marcar el correo como spam o simplemente rechazarlo. DMARC permite a los propietarios de dominio indicar a los proveedores de servicio de internet ya sus clientes de correo que realizar cuando un mensaje formado no se encuentra formalmente identificado por un estándar SPF o DKIM.

Estos protocolos se deberían implementar ya que ayudan a verificar la identidad de los remitentes, es una de las formas más efectivas y actuales para evitar que los phishers o estafadores suplanten la identidad de cualquier remitente legítimo. (Kontinen, 2020)

***Firma electrónica*:** La firma electrónica se la puede utilizar para verificar la autenticidad del remitente de correo, este se basa en el principio de no repudio, utiliza el cifrado de clave pública y privada para generar los certificados necesarios.

Los correos electrónicos son firmados digitalmente con la clave privada del remitente, por lo que esta clave es única y no debe ser compartida con nadie más, por otro lado, el destinatario necesita de la clave pública del remitente para así poder verificar la autenticidad del correo, asegurándose de que la persona que envía es la oficial. (Giron, 2022)

Criptografía

Se sabe que existe una gran problemática en las funciones de los correos electrónicos, es la falta de seguridad que brindan. Para poder combatir con esto surgió la criptografía aplicada a la informática, esta proviene del griego “kryptos” cuyo significado es oculto y “graphia”, escritura. La RAE lo define como el “Arte de escribir con clave secreta o de un modo enigmático” (ASALE, s.f.). El objetivo principal de esta técnica es conservar la confidencialidad, integridad y disponibilidad del contenido del mensaje enviado, así mismo dándole seguridad tanto al remitente como al destinatario, y evitar que exista modificaciones o que el mensaje haya sido manipulado durante el proceso.

Algoritmos de cifrado

La criptografía usa algoritmos complejos de cifrado para proteger la información, utilizan códigos y fórmulas matemáticas para convertir el texto plano en un texto cifrado que permite

que el contenido sea visible, pueda ser leído y procesado solo para quienes esté destinada dicha información. Se puede clasificar al tipo de cifrado en dos grupos principales: Simétrico y Asimétrico.

Función Hash: Esta también es conocida como función resumen, este algoritmo es utilizado sobre todo en mensajes o archivos de gran extensión, consiste en transformar un mensaje en una cadena de longitud de salida fija que siempre será del mismo tamaño. Estos resúmenes generados serán únicos para cada archivo o mensaje, este algoritmo usa cadenas que se forman con números del 0 al 9 y letras de A a la F. El usuario puede comprobar si el mensaje o el archivo ha sido alterado o se encuentra etiquetado con algún indicador de compromiso, no solo protege el mensaje, también aumenta la seguridad de las contraseñas y de las firmas digitales.

Cifrado simétrico**:** conocido como criptografía de clave privada es un método criptográfico en el que se utiliza una misma clave compartida entre Emisor y Receptor, para así Cifrar y Descifrar el mensaje transmitido. Este método es simple y suele ser utilizado para el cifrado de correos electrónicos, bases de datos, archivos y otros más. Esta clave que es utilizada para cifrar y descifrar puede ser de tipo alfanumérica y tener caracteres especiales. (Bjorkelund, 2022). Los algoritmos de criptografía simétrica más utilizados son los siguientes:

- **Blowfish:** este es un algoritmo simple de utilizar el cuál consiste en ocupar bloques de 64 bits y claves desde 32 bits a 448 bits, esto facilita encontrar un punto medio para tener alta velocidad y a su vez alta seguridad, está basado en la red de Feistel y cuenta con 16 rondas. Se necesita 521 ejecuciones del algoritmo para poder crear las subclaves.
- **Des Y 3des:** Data Encryption Standard, esta criptografía ha sido implementada en muchos de los productos comerciales, tiene una longitud de bloque de 64 bits

para texto y a su vez 64 bits para la clave de los cuales 8 son para paridad. La versión 3DES ocupa el triple de ciclos de cifrado.

- **Aes:** Advanced Encryption Standard, este algoritmo criptográfico reemplazó a DES luego de comprobar que era vulnerable, utiliza cifrado simétrico de bloque, con tamaños de bloques fijos de 128 bits y soporta claves de 128, 192 y 256 bits. En la actualidad es el más utilizado ya que no ha sido vulnerado por su complejidad.

Cifrado asimétrico**:** este tipo de cifrado también es conocido como criptografía de clave pública o de dos claves, este método utiliza el intercambio de claves público/privado para cifrar los datos (emisor o destinatario) y necesarias para que el mensaje pueda ser transmitido de forma cifrada y solo el destinatario logra descifrar la información con su clave privada. (Mendoza J. C., 2018)

- **Rsa:** es el primer sistema criptográfico de clave pública, este se basa en la dificultad computacional de factorización de números enteros grandes. Es usado mayormente para el cifrado y descifrado de archivos, de igual forma para la validación de la firma electrónica.

  Su seguridad se basa en la dificultad de factoreo de los números primos entre 10 y 100 cifras, estos son elegidos de manera aleatoria para obtener la clave de cifrado, tiene diferentes longitudes de claves como: 512, 768, 1024 o 2048 bits. Este algoritmo aún no ha sido vulnerado, esto se debe a que en la actualidad los sistemas computacionales no permiten realizar operaciones de factorización de números muy grandes. El funcionamiento de este algoritmo consiste en que el destinatario proporciona su clave pública al remitente, el mismo cifra el mensaje usando dicha clave proporcionada y envía al destinatario, a su vez el mismo recibe el mensaje y utiliza la clave privada para descifrar el mensaje, esto

permite que, si el mensaje es vulnerado e interceptado en el proceso de envío, no sea legible por otra persona.

En el caso del sistema de firma electrónica, el remitente se encarga de firmar el documento con la clave privada y procede a enviar al destinatario, éste lo recibe y comprueba su validez de la firma usando la clave pública del remitente.

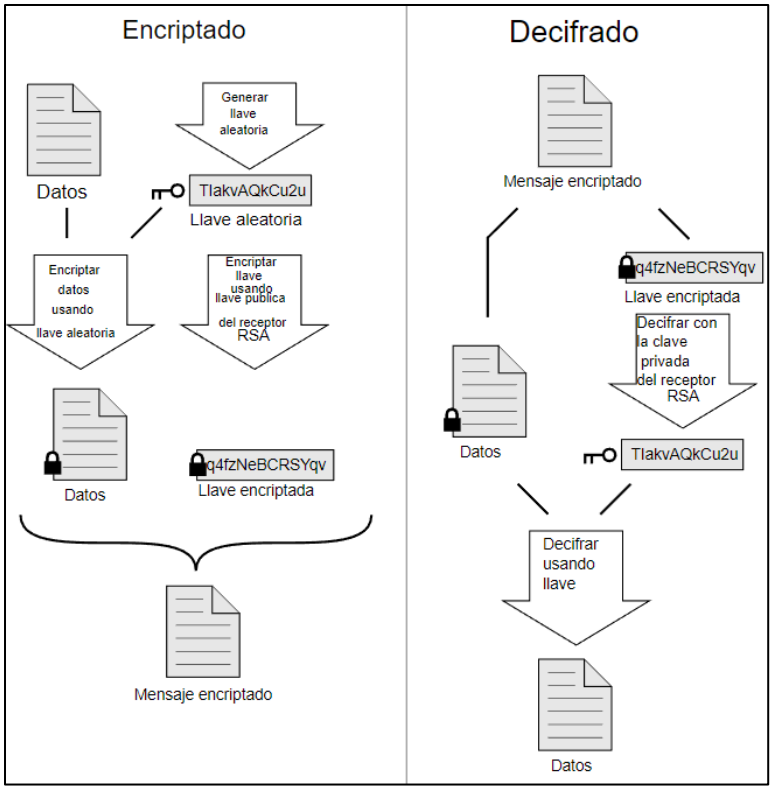
- **Pgp:** Llamado Pretty Good Privacy es un sistema criptográfico o también llamado de “llave pública” que fue desarrollado por Phil Zimmermann en el año 1991, su objetivo principal es proteger la información transmitida a través de internet mediante la utilización de técnicas de cifrado simétrica y de clave pública.

  Este sistema criptográfico permite cifrar documentos, textos, emails o discos duros completos y a su vez ayuda a proteger los datos para que no puedan ser vistos por personas no autorizadas. Cuando se cifra archivos con este sistema híbrido, el programa genera una clave aleatoria, que se la conoce como clave simétrica la cual cifra la información, esta a su vez es cifrada usando la clave pública del destinatario mediante RSA, finalmente se comprime los datos en un solo archivo cifrado el cual contiene la información y la clave simétrica, estas dos cifradas con un método distinto.

  Pretty Good Privacy se desarrolló como un software privativo con licencia de uso de PGP Inc, sin embargo, dada la importancia de utilizar este tipo de cifrado para las comunicaciones la organización Free Software Fundation creó una versión gratuita del programa GNU Privacy Guard, GnuPG o GPG. (Garfinkel, 1995)

Figura 6

Cifrado/descifrado con PGP



Nota: El gráfico representa el proceso de cifrado/descifrado con PGP. Tomado de: https://upload.wikimedia.org/wikipedia/commons/7/70/PGP_diagramES.svg

- **OpenPGP:** Esta es la versión gratuita de PGP, posee compatibilidad con la mayoría de los clientes de correo electrónico existentes en la actualidad, de igual forma con varias plataformas de sistemas operativos, este sistema ofrece mecanismos para cifrado, descifrado y firma electrónica.
- **Servidores de claves:** Las claves que se generan en un sistema GPG/PGP se encuentran asociadas a un nombre de usuario y un correo electrónico, en cada

una de estas se generada por un usuario se usa el algoritmo RSA teniendo como resultado la clave privada y de uso exclusivo para el mismo, de igual forma la clave privada que puede ser compartida libremente. Existen servidores gratuitos que facilitan la compartición de claves públicas, se puede registrar estas claves y se encuentran disponibles durante la vigencia de las mismas. Entre los servidores de claves públicas más conocidos están:

- ✓ Keys.openpgp.org
- ✓ pgp.mit.edu
- ✓ keyring.debian.org
- ✓ keyserver.ubuntu.com
- ✓ attester.flowcrypt.com
- ✓ zimmermann.mayfirst.org

Kleopatra

Es un software que se creó por medio del proyecto Agypten, el cuál trabaja en el desarrollo de medios gráficos para la implementación del cifrado con GPG.

Esta herramienta que es soportada por múltiples sistemas operativos gestiona certificados X.509 y OpenPGP, es un programa para cifrar carpetas y archivos desde Dolphin, el gestor de archivos predeterminados en el escritorio KDE y también se lo puede utilizar en Debian.

Kleopatra permite cifrar y proteger archivos o documentos mediante una interfaz gráfica y con un solo click.

Figura 7

Kleopatra

Nota: El gráfico representa el logo del software Kleopatra. Tomado de:

https://www.gpg4win.org/img/kleopatra_logo.png

Capítulo III

Análisis, Diseño y Desarrollo

Introducción

En este capítulo se indica las herramientas y metodologías a usarse para la implementación del sistema de seguridad para correos electrónicos, el objetivo principal es realizar una comparación del desempeño y del grado de seguridad entre un sistema de correos electrónicos tradicional y un sistema que cifre la información mediante PGP y a su vez que implemente una firma digital.

Para ello se utilizará el software “Kleopatra”, este es un administrador de claves GPG/PGP que fue desarrollado por la organización GNUPG. Entre las funciones más importantes está la de crear e importar claves públicas y privadas dentro del mismo sistema, utiliza una interfaz amigable hacia el usuario (GUI).

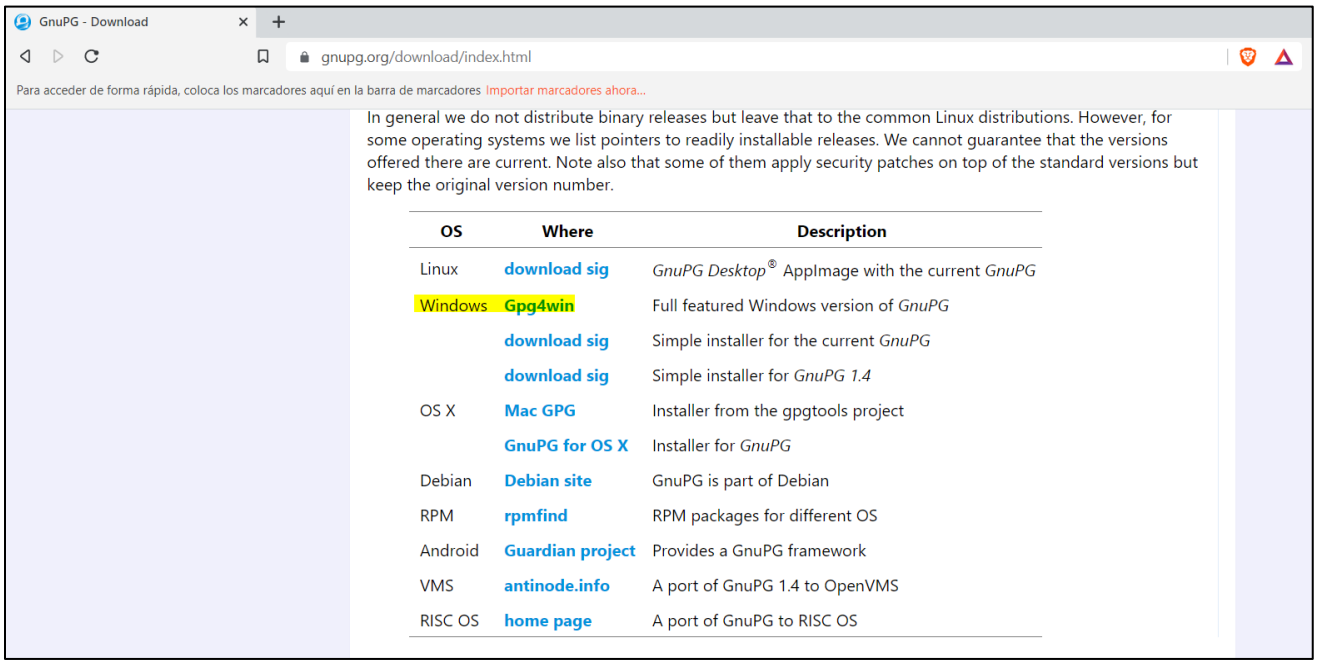
Kleopatra es soportado por varios sistemas operativos y puede integrarse a través de plugins con todos los clientes de correos, adicionalmente en sistemas operativos Windows se integra al menú contextual, esto facilita cifrar archivos desde cualquier ubicación sin requerir el acceso al programa.

Instalación de GPG para Windows

1. Descargar el aplicativo para generación de claves GPG4win.exe desde el portal de GnuPG.ORG en (URL: https://gnupg.org/download/index.html)

Figura 8

Gpg4win



Nota: El gráfico representa el lugar para descargar GPG4win.exe.

Es muy importante descargar los archivos desde páginas oficiales de la marca, así evitamos infectar el equipo con programas o softwares maliciosos que puedan dañar la computadora a corto o largo plazo. En este caso se procede a descargar del sitio oficial el cual es confiable. De igual forma se debe seleccionar de manera correcta el sistema operativo, en este caso es Windows.

2. Ejecutar el archivo descargado para instalar el software Kleopatra y GPG

Figura 9

Instalación Gpg4win

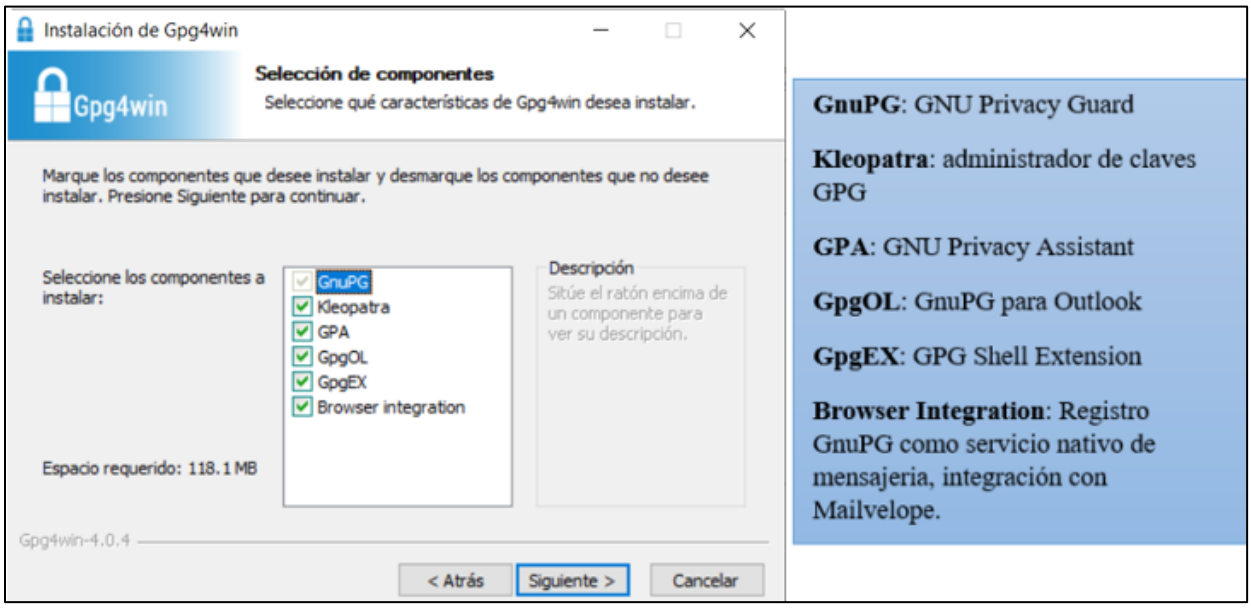
Nota: El gráfico representa la instalación de GPG4win.exe.

Una vez que se ha descargado el archivo se procede con la instalación del mismo, es recomendable empezar el proceso de instalación como administrador, para este caso se da clic derecho en el archivo y ejecutar como administrador. Seguido de esto se avanza paso a paso leyendo las opciones que permita cambiar o aprobar el programa según los requerimientos que sea necesarios.

3. Seleccionar los componentes de instalación

Figura 10

Selección componentes Gpg4win



Nota: El gráfico representa la instalación de los componentes de GPG4win.exe.

En este paso se puede seleccionar los componentes necesarios dependiendo el uso que se vaya a dar, para este caso se selecciona todos, ya que, próximamente se usará el administrador de claves de kleopatra, el registro de GnuPG como servicio nativo de mensajería, integración con Mailvelope en los diferentes navegadores a utilizar. De igual forma para la plataforma de Outlook se utilizará el GnuPg.

4. Proceso de instalación.

Figura 11

Instalación de componentes Gpg4win

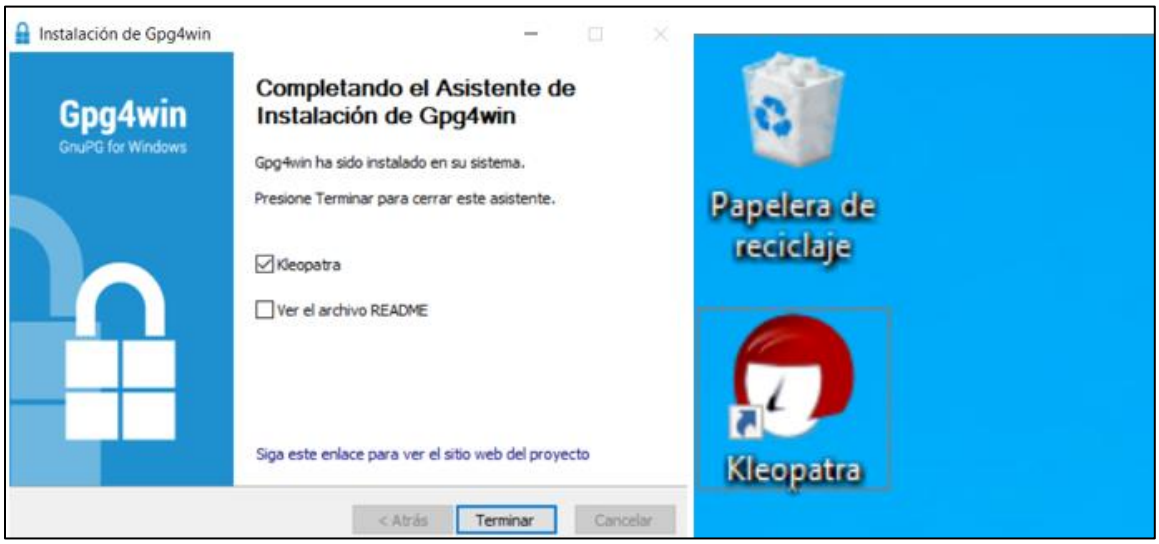
Nota: El gráfico representa la instalación de los componentes de GPG4win.exe.

Una vez seleccionado todos los componentes deseados, nos mostrará en pantalla los íconos de las herramientas que se instalarán. Como se puede observar pertenecen a los componentes agregados en el paso anterior. Adicional mostrará una barra que indica el el porcentaje aproximado de instalación.

5. Al finalizar el proceso se creará un ícono en el escritorio, es el acceso al programa Kleopatra

Figura 12

Instalación finalizada



Nota: El gráfico representa la instalación finalizada de GPG4win.exe.

Una vez que el programa se ha instalado correctamente en el sistema mostrará el gráfico anterior, finalmente se debe dar clic en “Terminar” para cerrar el Asistente de Instalación de Gpg4win y poder abrir el programa instalado previamente.

Creación de claves de cifrado (pública/privada)

La creación de claves de cifrado, tanto la pública como al privada se la realiza en el software instalado anteriormente llamado “Kleopatra”, para lo cual se debe seguir una serie de pasos que se detallan a continuación.

1. Abrir el programa Kleopatra
2. Se debe seleccionar en “nuevo par de claves”

Figura 13

Crear nuevo par de claves

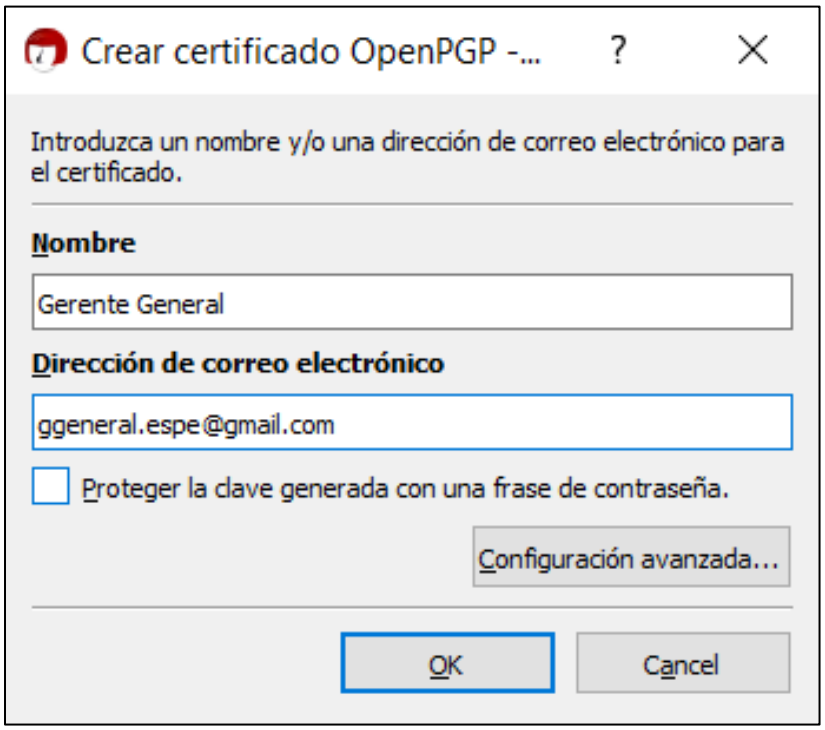
Nota: El gráfico representa el proceso de creación de par de claves.

Mediante Kleopatra que es una interfaz para el software de cifrado GnuPG se procede con la creación de un nuevo par de claves OpenPGP, seleccionando en crear un nuevo par de claves.

3. Introducir el nombre de correo electrónico la que se asociará las claves

Figura 14

Detalles personales a los que se asociarán las claves



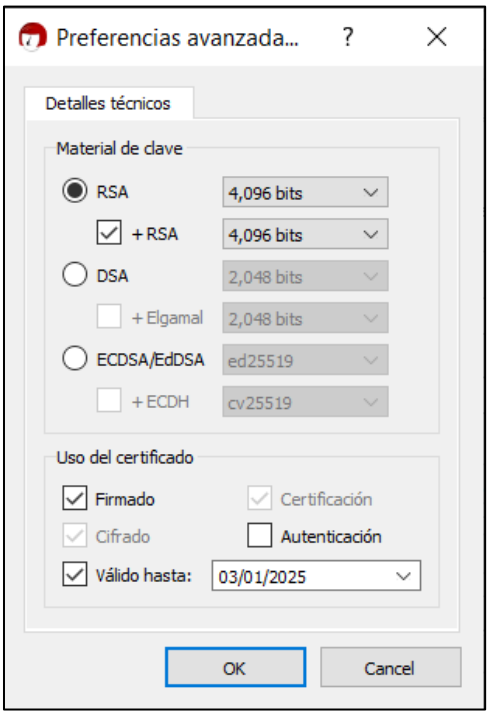
Nota: El gráfico representa el proceso de colocar los detalles personales de la cuenta.

En este paso se asigna el nombre de la cuenta y la dirección de correo electrónico para el certificado, de igual forma brinda la opción de añadir una configuración avanzada para la creación del certificado.

4. Se selecciona en configuración avanzada los parámetros de cifrado y validez del certificado.

Figura 15

Configuración avanzada (Cifrado: RSA, Tamaño: 4096, Duración: 2 años)



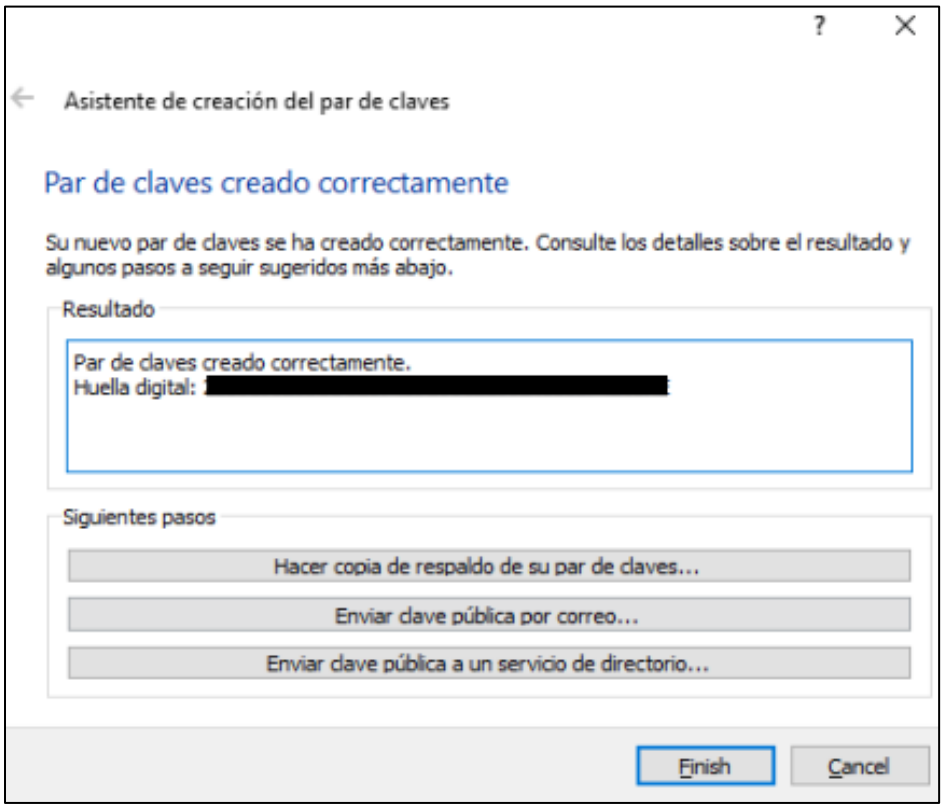
Nota: El gráfico representa el proceso de configuración de las claves.

Dentro de la configuración avanzada, el software Kleopatra permite seleccionar el material de clave, para este caso se seleccionará RSA de 4,096 bits, así mismo se escoge la fecha de caducidad de la clave, que será en este caso de 2 años.

5. Resultado de la creación correcta de las claves.

Figura 16

Clave pública y privada creadas



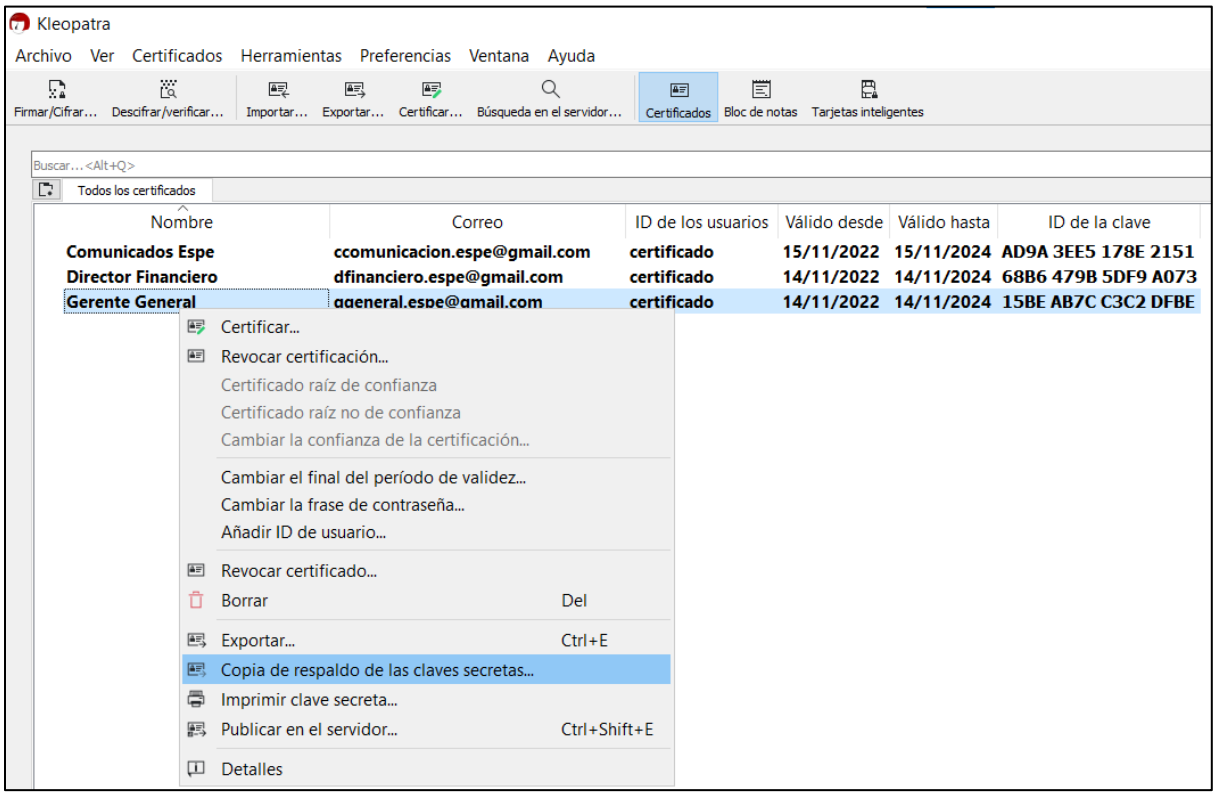
Nota: El gráfico representa la huella digital del par de claves creados correctamente.

Los pasos vistos anteriormente se deben repetir por los usuarios de la organización para todos los correos de la empresa. Si el proceso se lo realizó correctamente al final mostrará la ventana anterior indicando la huella digital.

6. Finalmente se debe exportar las claves (confidencial), se selecciona la Copia de respaldo de las claves secretas.

Figura 17

Exportación claves (confidencial)



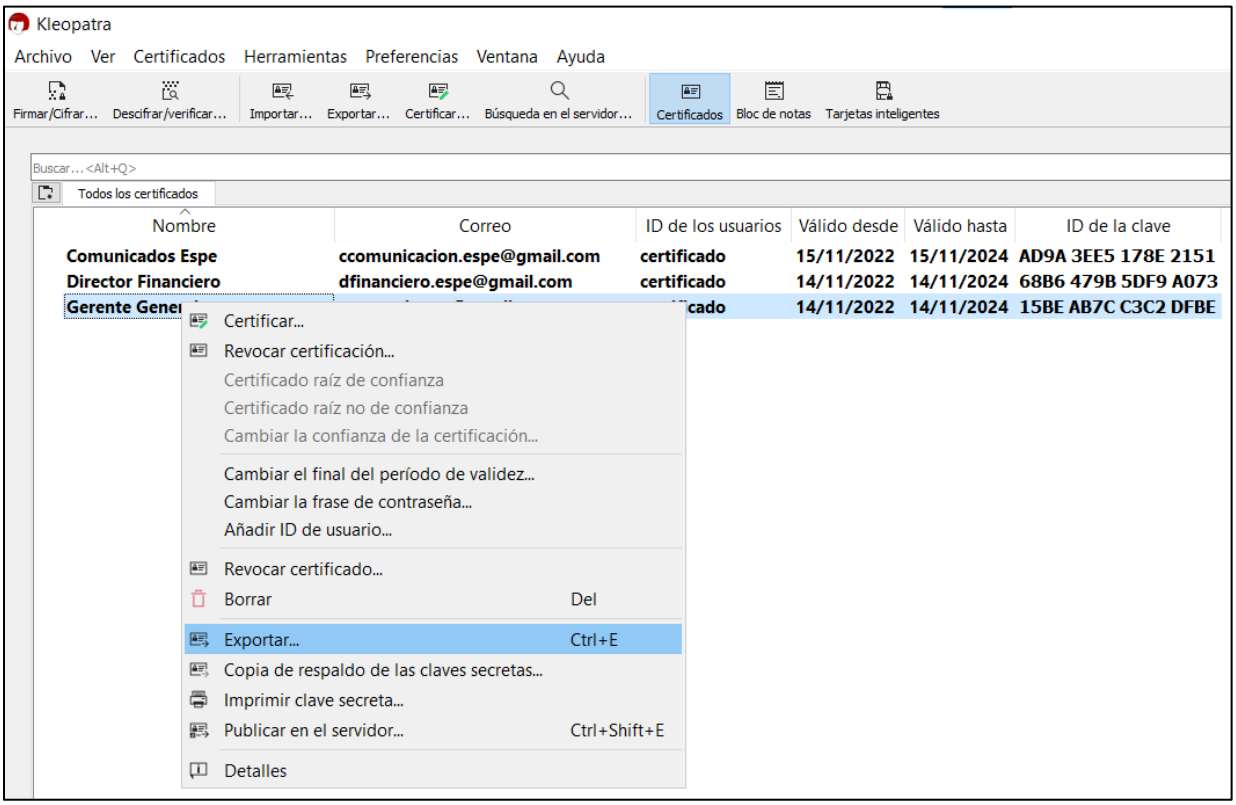
Nota: El gráfico representa la exportación de las claves (confidencial).

Se necesita exportar las claves, para ello se realiza una copia de respaldo de las claves secretas, donde se tienen que guardar los archivos generados en un lugar seguro para el usuario, ya que esta información es confidencial.

7. Exportar la clave pública, seleccionando en la opción exportar.

Figura 18

Exportación clave privada y pública



Nota: El gráfico representa la exportación de las claves privada y pública.

Es importante que todos los remitentes dispongan de las claves públicas de todos los destinatarios, esto permite intercambiar información cifrada mediante el correo electrónico. Se debe diferenciar la clave pública de la privada para poder enviar estos archivos que han sido generados.

Figura 19

Archivos de las claves: pública y privada

Nota: El gráfico representa los archivos de las claves privada y pública.

Es necesario aclarar que las claves públicas no contienen información confidencial, es por esta razón que se puede subirla a un servidor público de claves para poder compartirla en cualquier momento para cualquier remitente.

Las claves públicas deben ser importadas al software Kleopatra y a los diferentes clientes de correo electrónico para que sea posible el envío de emails cifrados.

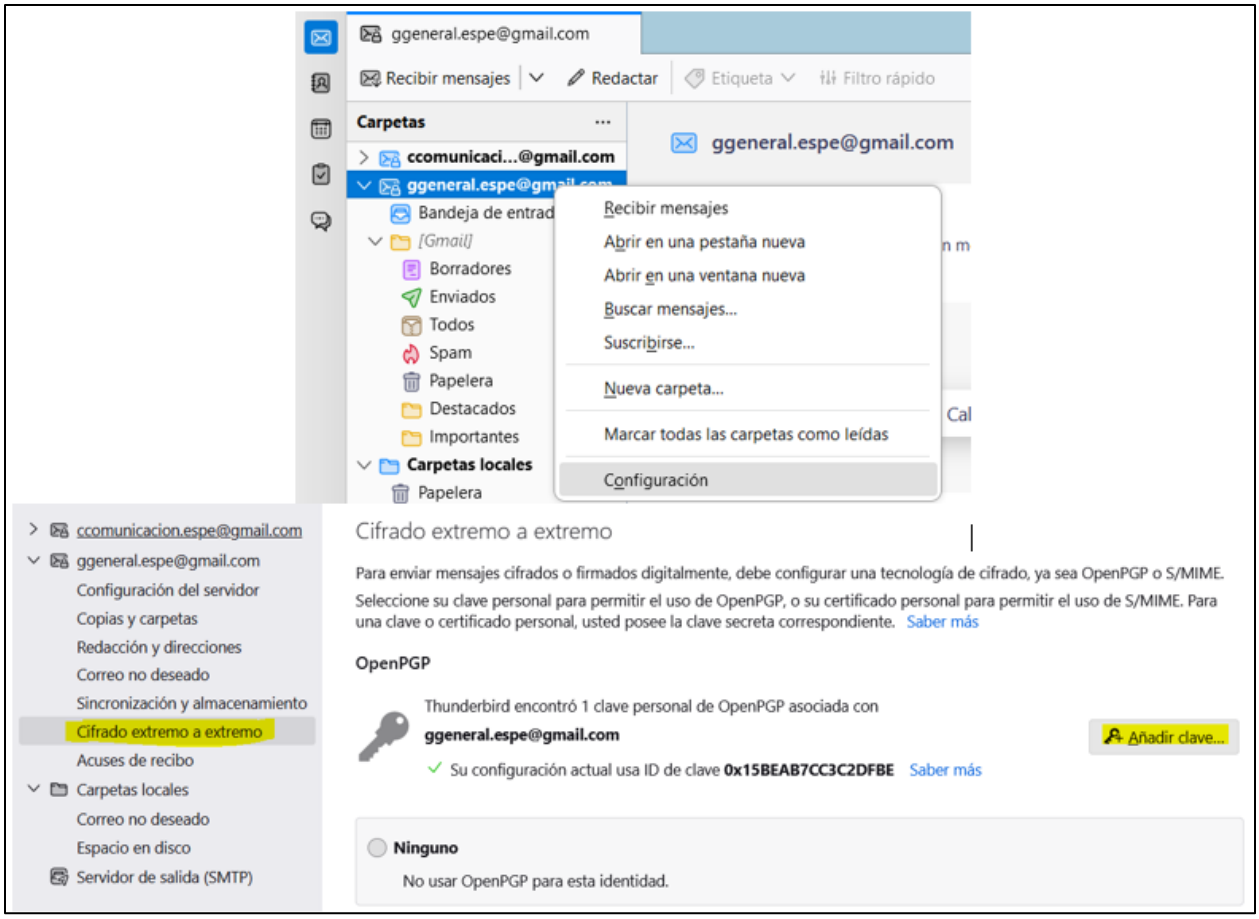
Para poder descifrar los emails recibidos es necesario configurar las llaves privadas dentro de los clientes de correo, ya sea Outlook o Thunderbird.

Importe de la clave privada en el cliente de correo electrónico Thunderbird

1. Descargar e instalar el cliente de correo Thunderbird, seguido se debe ingresar con la cuenta de correo electrónico.
2. Clic derecho en la cuenta >> Configuración >> Cifrado Extremo a Extremo >> Add Key

Figura 20

Importe de clave privada en el cliente de correo electrónico Thunderbird

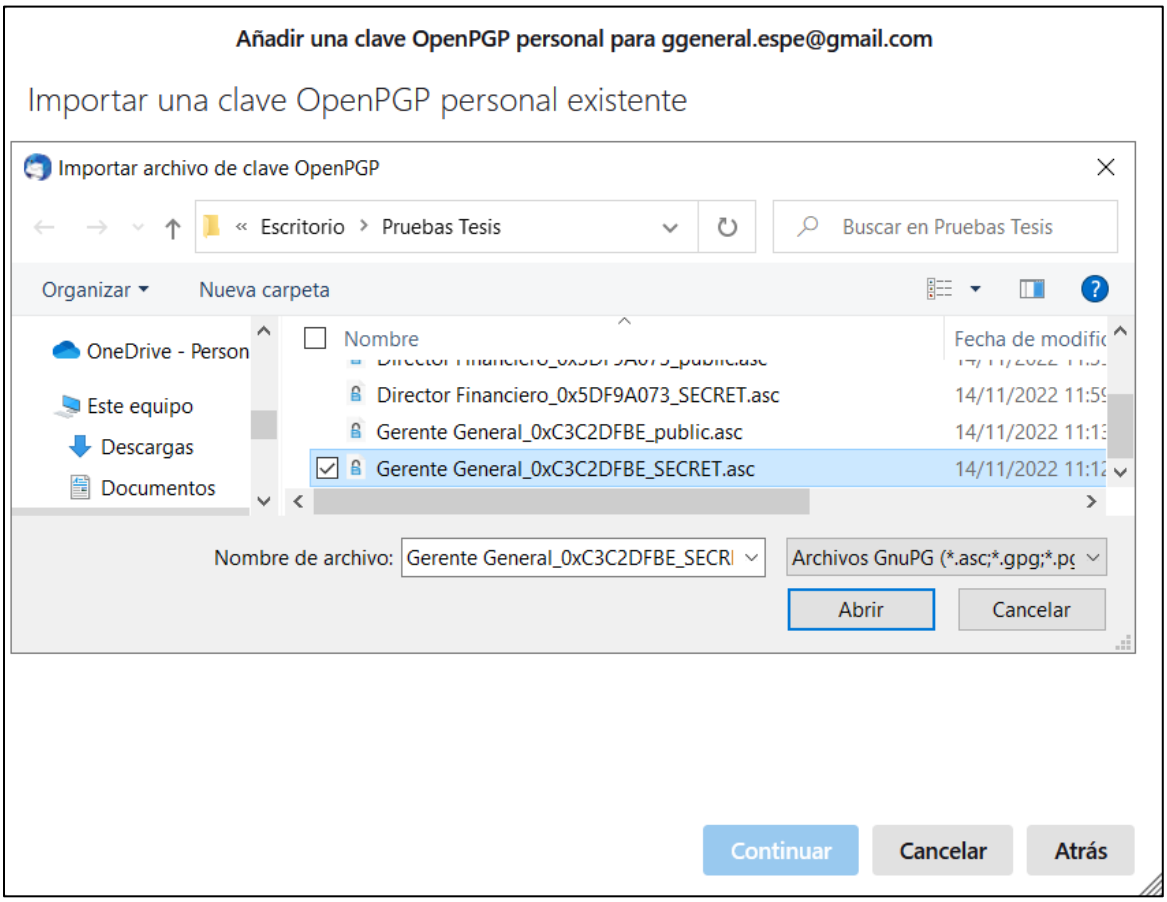


Nota: El gráfico representa el proceso para el importe de la clave privada en el cliente de correo electrónico Thunderbird.

3. Seleccionar el archivo de la clave privada asignado para la cuenta de correo electrónico.

Figura 21

Añadir la clave privada para la cuenta de correo electrónico



Nota: El gráfico representa el proceso para importar la clave privada de la cuenta de correo electrónico.

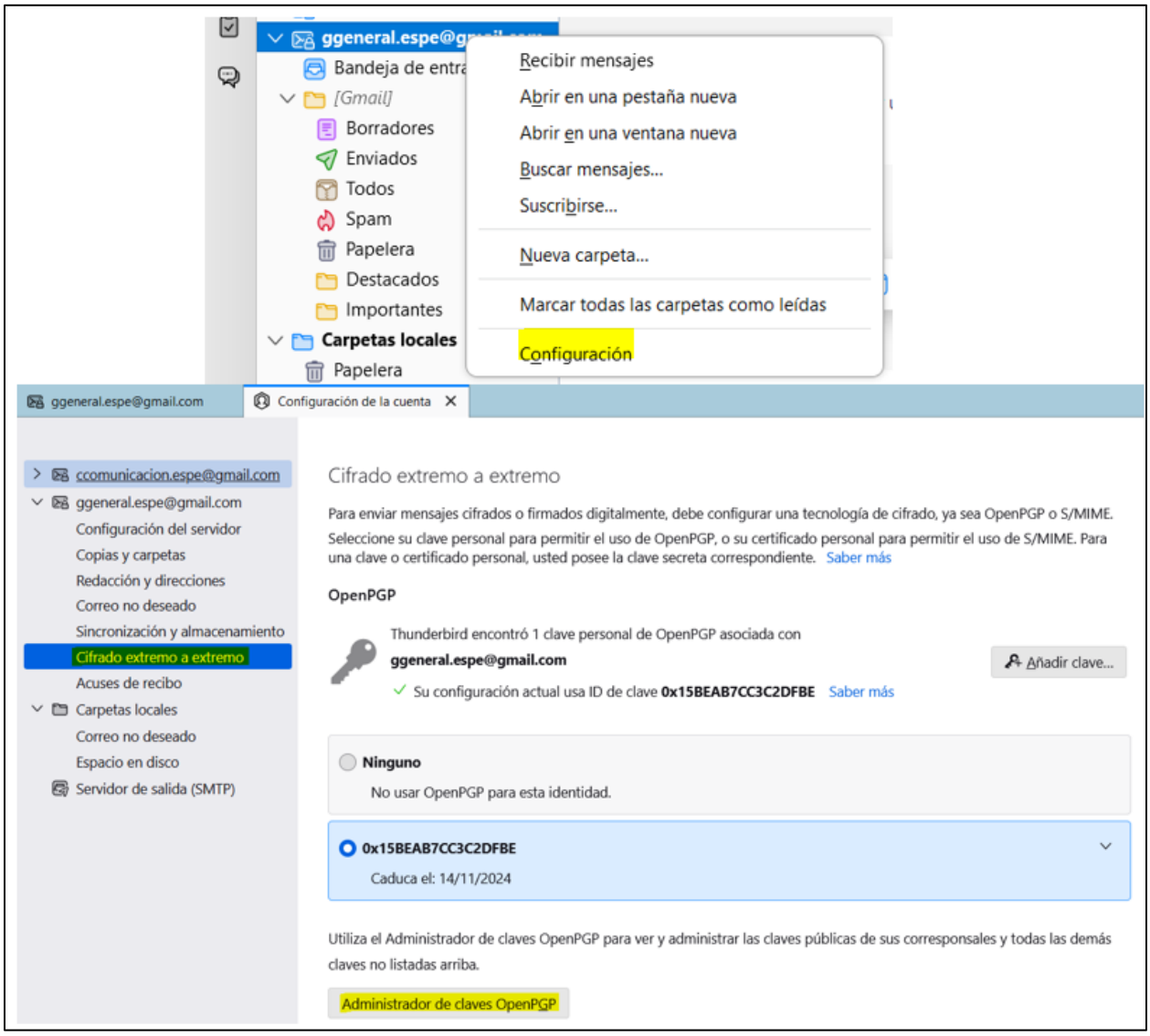
Una vez que se importó correctamente la clave privada de la cuenta respectiva, es importante importar las claves públicas de cifrado para las cuentas de correo de los destinatarios.

Proceso de importación de Claves Públicas en Thunderbird

1. Como primer paso se debe ingresar al cliente de correo Thunderbird
2. Dentro del programa dirigirse a la cuenta >> Configuración >> Cifrado Extremo a Extremo >> Administrador de claves OpenPGP

Figura 22

Proceso de importación de claves públicas



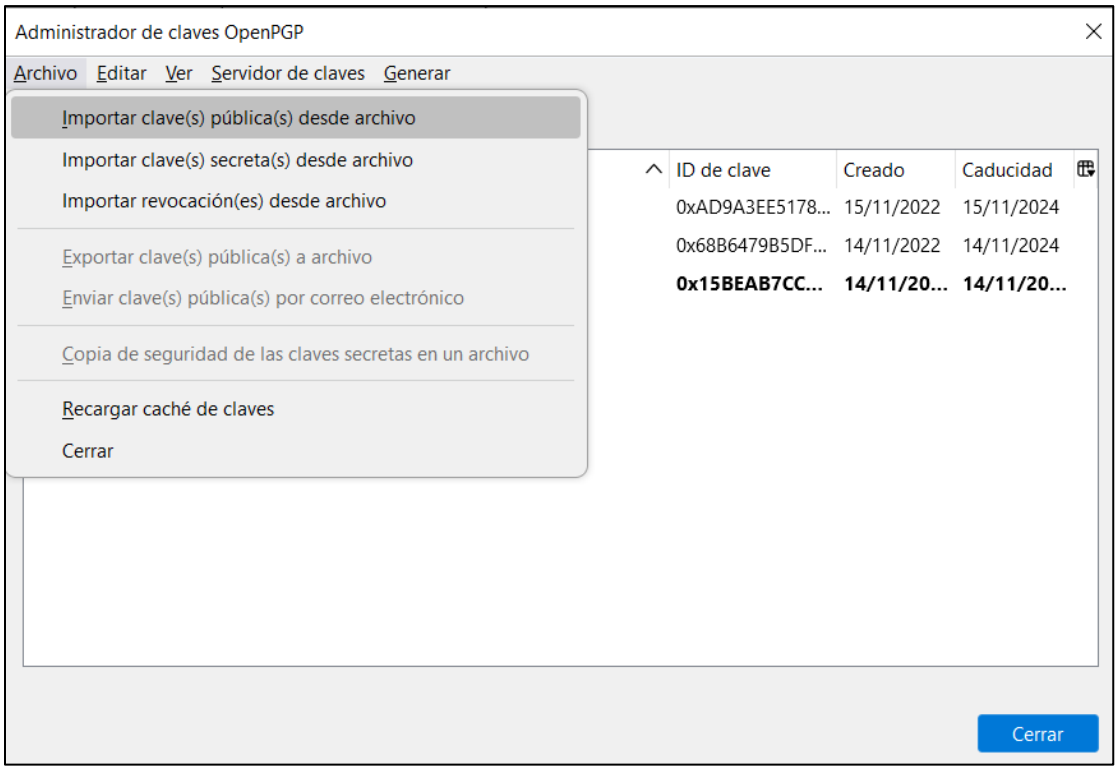
Nota: El gráfico representa el proceso para importar las claves públicas.

Dentro de este apartado se muestra los correos a los cuales ya se ha importado la clave pública, de igual forma si se desea agregar más claves públicas.

3. Se agrega las claves públicas adquiridas por los destinatarios, hay que dirigirse a Archivo >> Importar clave(s) públicas(s) desde archivo

Figura 23

Proceso de importación de claves públicas



Nota: El gráfico representa el proceso para importar las claves públicas desde un archivo, estos archivos son proporcionados por los destinatarios.

Una vez que ya fueron agregadas las claves públicas de todos los destinatarios requeridos, se debe cerrar la lista y activar la opción Requerir cifrado por defecto para que se active el cifrado para los mensajes nuevos.

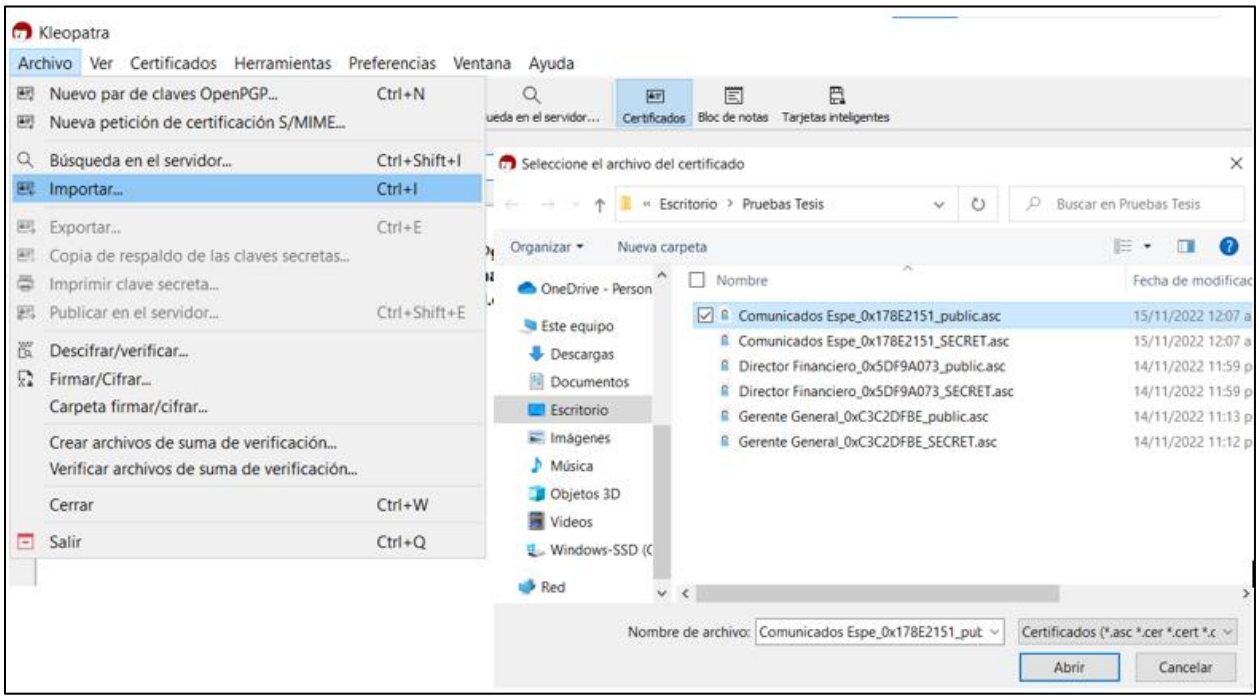
Importe de las claves públicas/privadas para el cliente de correos electrónicos Outlook

En el cliente de correo Outlook la aplicación toma los certificados añadidos al cliente GPG por defecto en el sistema, es por esta razón que los certificados de clave pública como privada se los tiene que agregar mediante el software Kleopatra. Es necesario aclarar que para ambos casos el proceso es el mismo.

1. Abrir el software Kleopatra y acceder a Archivo >> Importar >> Y seleccionar las claves públicas de todos los destinatarios deseados.

Figura 24

Proceso de importación de claves públicas en kleopatra



Nota: El gráfico representa el proceso para importar las claves públicas desde un archivo en el software Kleopatra, estos archivos son proporcionados por los destinatarios.

2. Claves públicas agregadas de forma satisfactoria.

Figura 25

Claves públicas agregadas correctamente

Nota: El gráfico representa que las claves públicas de los destinatarios están agregadas correctamente.

Una vez realizado todos los pasos se presentará como en la figura anterior, en la cual indica que las claves públicas de todos los destinatarios fueron agregadas correctamente y la aplicación de Outlook podrá leerlas de forma satisfactoria. De igual forma se puede ver el nombre, correo, id de los usuarios, la fecha tanto de creación como la de vencimiento y finalmente el id de la clave.

Importe de las claves pública/privada en Webmail

En el caso de los clientes de correo electrónico que se basan en Webmail, se necesita agregar una extensión llamada Mailvelope dentro del navegador de preferencia, ya sea Chrome, Microsoft Edge o Firefox.

Para poder agregar esta extensión hay que dirigirse a configuración >> Extensiones>> Buscar Mailvelope >> Añadir

Figura 26

Extensión Mailvelope

Nota: El gráfico representa la extensión Mailvelope

Para este caso se está usando el navegador Chrome, dentro del cual se tiene que buscar la extensión Mailvelope, la cual ayudará y permitirá importar las claves, tanto pública como privada de la cuenta. Una vez encontrada la extensión se procede a añadirla al navegador.

Esta extensión se encarga de tomar los datos de la cuenta de correo electrónico para poder descifrar de forma automática los correos que lleguen y se encuentren cifrados con GPG. Para ello hay que seguir ciertos pasos que se detallarán a continuación.

1. Se debe dar clic en el ícono de la extensión de “Mailvelope” >> Luego a administración de llaves >> Finalmente a importar llave.

Figura 27

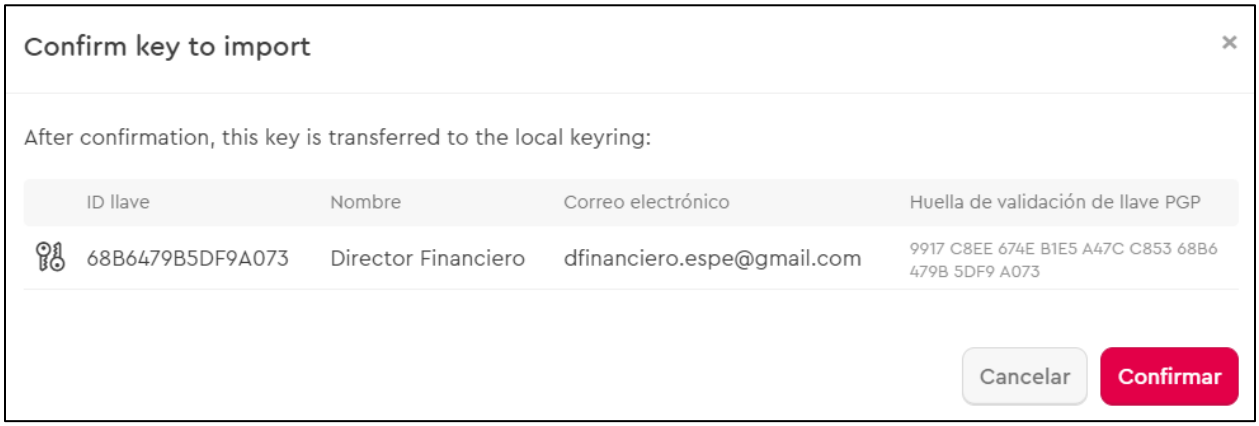
Extensión Mailvelope – Importación de llaves

Nota: El gráfico representa el proceso de importación de llaves en la extensión Mailvelope.

2. Seleccionar el archivo de clave privada descargado anteriormente de la cuenta de correo que se va a utilizar, finalmente clic en confirmar.

Figura 28

Extensión Mailvelope – Importación de llaves privada



Nota: El gráfico representa el proceso de importación de llaves privadas.

3. Se debe realizar el mismo proceso para importar las claves públicas de los destinatarios.

Figura 29

Extensión Mailvelope – Importación de claves públicas y privadas

Nota: El gráfico representa el proceso de importación de llaves privadas.

Finalmente, una vez que se importó tanto la clave pública como privada, en la sección de administrador de llaves se muestra todas las claves importadas.

Funcionamiento

Luego de realizar todo el procedimiento de creación e importe de claves, tanto pública como privada, todos los emails que serán enviados desde cualquier cliente de correo previamente configurado serán cifrados con las claves públicas de los destinatarios, permitiendo que toda la información solo pueda ser leída por los usuarios que dispongan de la clave privada en su propia cuenta.

De igual forma, cada usuario al recibir los correos electrónicos podrá constatar la autenticidad del remitente con la clave pública gracias a la firma digital.

Se va a realizar un ejemplo para evidenciar el funcionamiento correcto de las claves pública y privada, para que dichos correos sean cifrados y firmados correctamente, evitando que, al ser interceptados por terceras personas, estos no sean visibles para los ciberdelincuentes.

Tabla 3

Correos y clientes de correo a usar

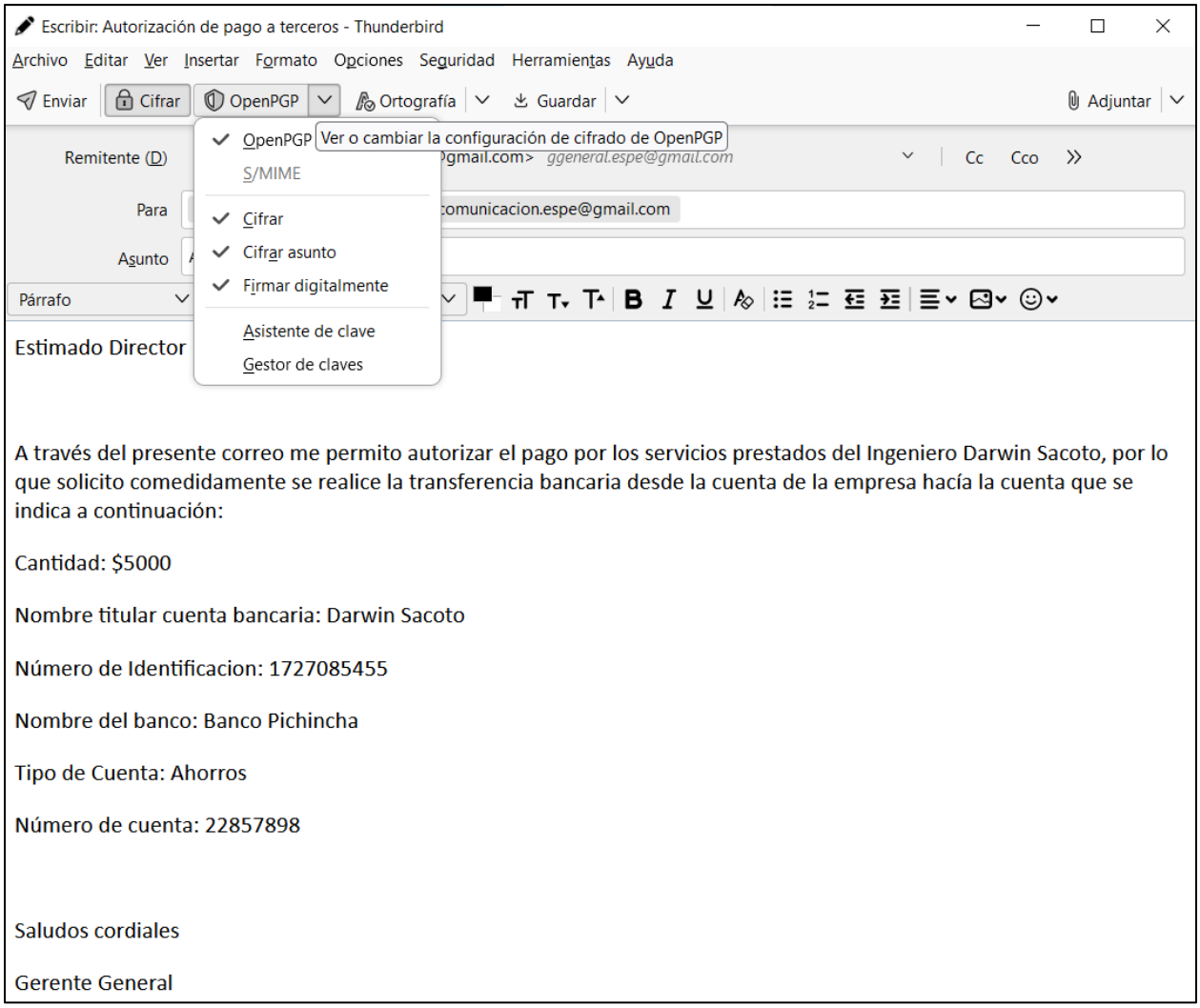
Remitente	Cliente de correo electrónico envío	Destinatario	Cliente de correo electrónico destinatario
ggeneral.espe@gmail.com	Thunderbird	ccomunicacion.espe@gmail.com	Outlook
		dfinanciero.espe@gmail.com	Webmail (Gmail)

Nota. En la tabla se observa los correos electrónicos y sus respectivos clientes para realizar las pruebas de cifrado y firma digital.

En el cliente de correo electrónico Thunderbird, al momento de enviar un nuevo email ya viene seleccionado por defecto la función de cifrar y firmar digitalmente para cada uno de los destinatarios.

Figura 30

Envío de correos por medio de Thunderbird

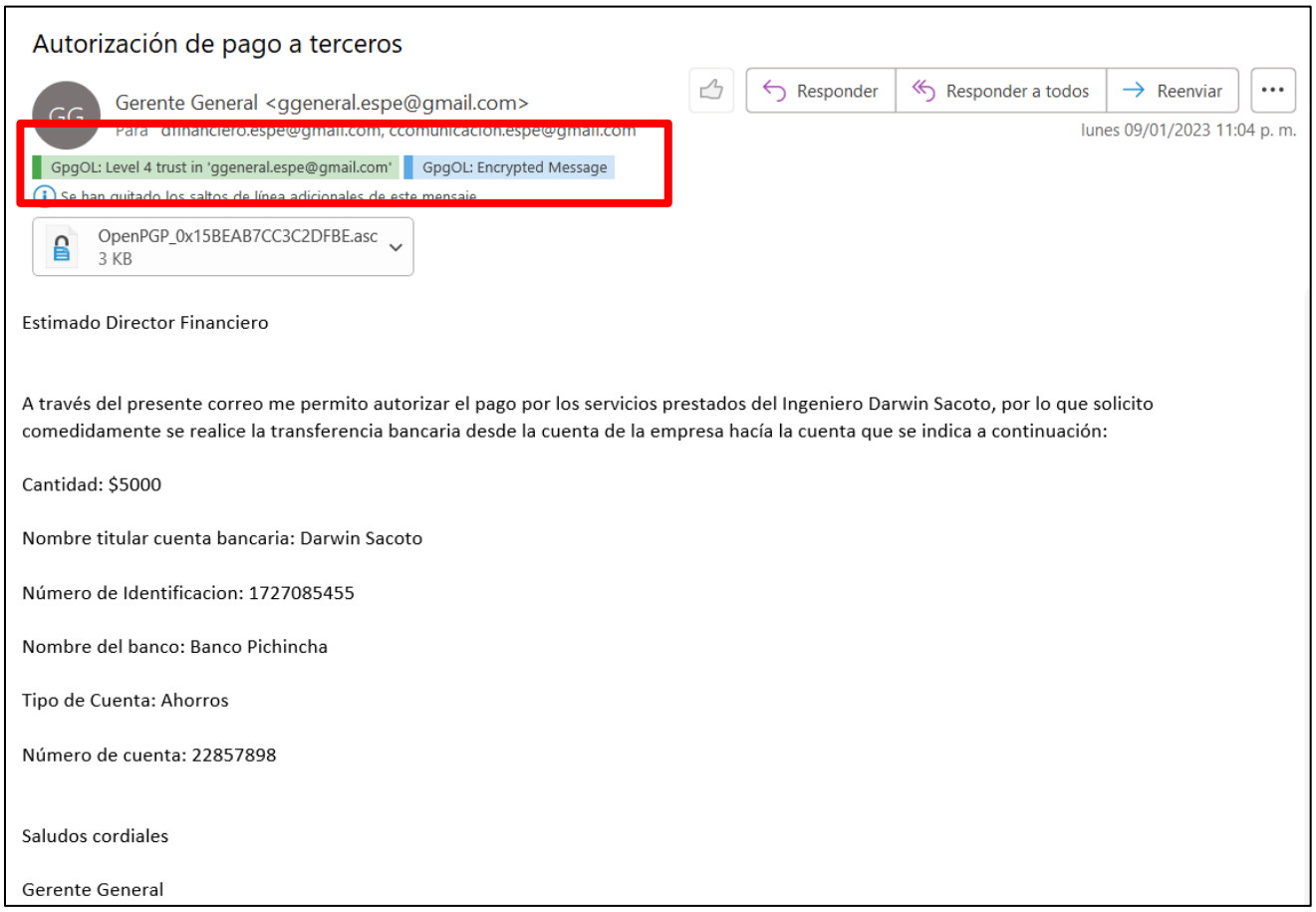


Nota: El gráfico representa el envío de un correo electrónico por medio del cliente Thunderbird, el cual permite cifrar y firmar digitalmente un email para evitar suplantaciones de identidad.

En este caso se ha simulado un correo electrónico enviado por parte del Gerente General de la empresa, en el cual autoriza un desembolso de dinero para una persona externa por ofrecer sus servicios prestados a la organización. A su vez el cliente de correo electrónico permite cifrar y firmar el email para que el destinatario pueda comprobar que efectivamente es el Gerente General quién envía el mensaje.

Figura 31

Recepción del mensaje en el cliente Outlook



Nota: El gráfico representa la recepción del correo electrónico en el cliente Outlook.

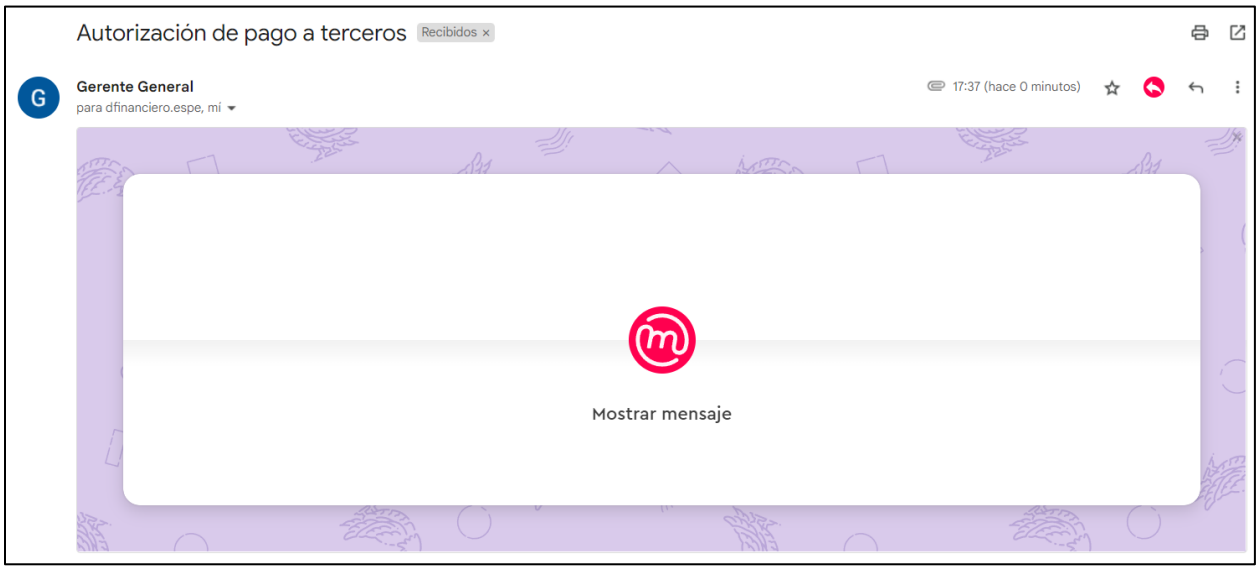
El destinatario puede verificar que efectivamente el correo electrónico enviado por el Gerente General se encuentra firmado y cifrado de manera correcta. Como se evidencia en la figura anterior, el cliente de correo Outlook, permite visualizar dos cuadros, uno de color verde el cual indica que el correo se encuentra firmado y pertenece al Gerente General, y el segundo de color azul que asegura la encriptación del mensaje para que solo pueda ser leído por el destinatario que dispone de su clave privada.

De esta manera el Director Financiero puede constatar que el mensaje es legítimo y realizar el desembolso a la persona solicitada, sin embargo, es recomendable que de ser posible exista una llamada telefónica de por medio para constatar y aprobar estos casos.

El segundo destinatario usa el cliente de correo electrónico Webmail, en el cual se utiliza la herramienta Mailvelope para el cifrado y descifrado de los correos.

Figura 32

Recepción del mensaje en el cliente Webmail

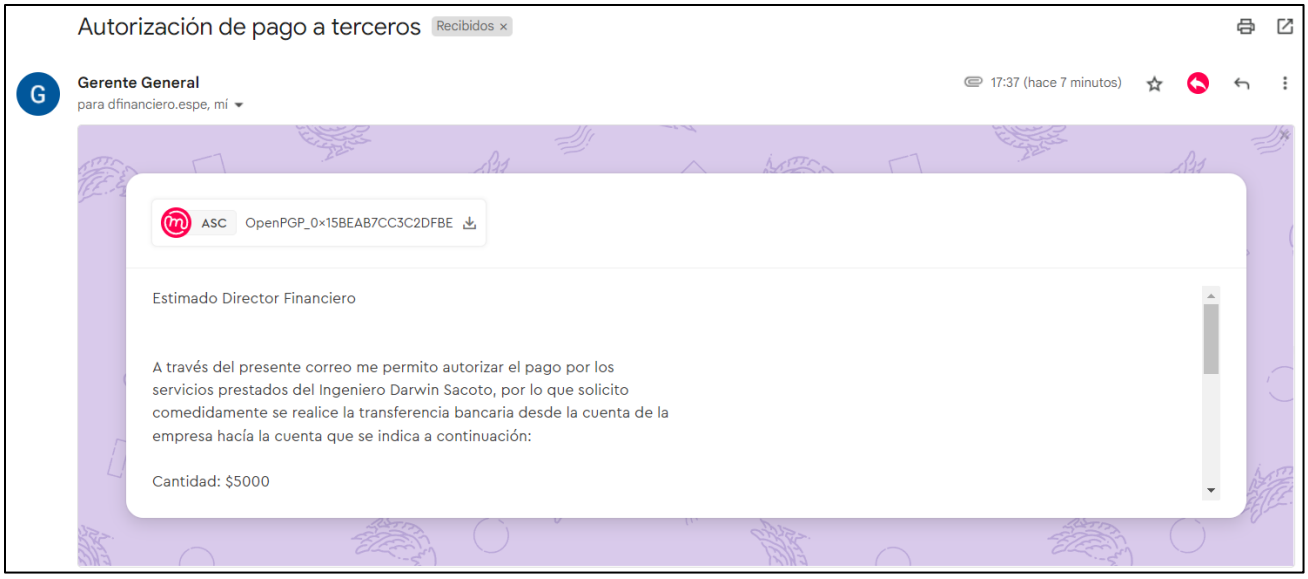


Nota: El gráfico representa la recepción del correo electrónico en el cliente Webmail.

Como se observa en la figura anterior, el correo electrónico llega encriptado y la herramienta Mailvelope permite desencriptar el mensaje y poder visualizar su contenido dando un clic en “Mostrar mensaje”

Figura 33

Recepción del mensaje en el cliente Webmail-Mostrar mensaje



Nota: El gráfico representa la recepción del correo electrónico en el cliente Webmail, desencriptando el mensaje.

De igual manera que en el anterior cliente de correo electrónico se puede evidenciar el mensaje desencriptado de manera satisfactoria, donde el destinatario puede leer el mensaje y proceder con la petición del Gerente General.

Para garantizar la seguridad de la información transmitida mediante correos electrónicos, el objetivo de GPG es proteger la información enviada del acceso no autorizado de terceros, es por esta razón que los correos electrónicos que sean cifrados no podrán ser legibles ni visibles en los siguientes casos:

- En el caso de que el correo electrónico se reenvíe a otro destinatario diferente a los definidos en un inicio por el remitente.
- El correo electrónico sea interceptado mediante su transporte hacia los destinatarios.

- El correo electrónico fuese recibido por un cliente de correo que no posea la configuración previa de las respectivas claves, tanto pública como privada de GPG.
- Si el correo electrónico es abierto en otro dispositivo donde no exista la configuración previa de las claves.

Prueba de funcionamiento de las firmas y cifrado de correos electrónicos mediante un ataque simulado de phishing

Una vez que se ha realizado todo el proceso de creación y configuración tanto de la clave privada como de la pública en cada cliente de correo electrónico es necesario realizar una prueba de funcionamiento para verificar la validez de las firmas y el grado de seguridad que brinda esta configuración para una empresa.

La idea es clonar la página del cliente de correo electrónico (gmail), hacerla lo más parecida posible a la original, una vez que se ha creado la página engañosa se debe enviar un correo electrónico aplicando las mejores técnicas de ingeniería social a un usuario importante dentro de la empresa, haciéndole creer que necesita ingresar sus credenciales de acceso para poder loguearse en su correo electrónico, como la página es muy similar a la original, el usuario no podrá verificar el error que está cometiendo. Una vez que la victima ingrese sus datos personales, las credenciales llegarán al dispositivo del atacante para que pueda cometer el delito, acceder a la información de la víctima y tratar de suplantar su identidad.

Para dicha prueba se utilizará el sistema operativo Kali Linux, esta es una distribución de Linux basada en Debian, la cual fue específicamente diseñada para temas de seguridad ya que contiene herramientas para realizar pruebas y análisis.

La herramienta principal que se utilizará para realizar el ataque simulado de Phishing es “Zphisher”, gracias a ella se puede generar más de 30 plantillas de phishing en este caso se utilizará para la clonación de la página de correo electrónico (Gmail).

Instalación de la herramienta Zphisher

Dentro del sistema operativo Kali Linux se debe ingresar una serie de comandos y pasos para su respectiva descarga e instalación.

1. Se utiliza el siguiente comando “ git clone https://github.com/htr-tech/zphisher.git” para descargar la herramienta del repositorio de github.

Figura 34

Descarga de la herramienta Zphisher en Kali Linux

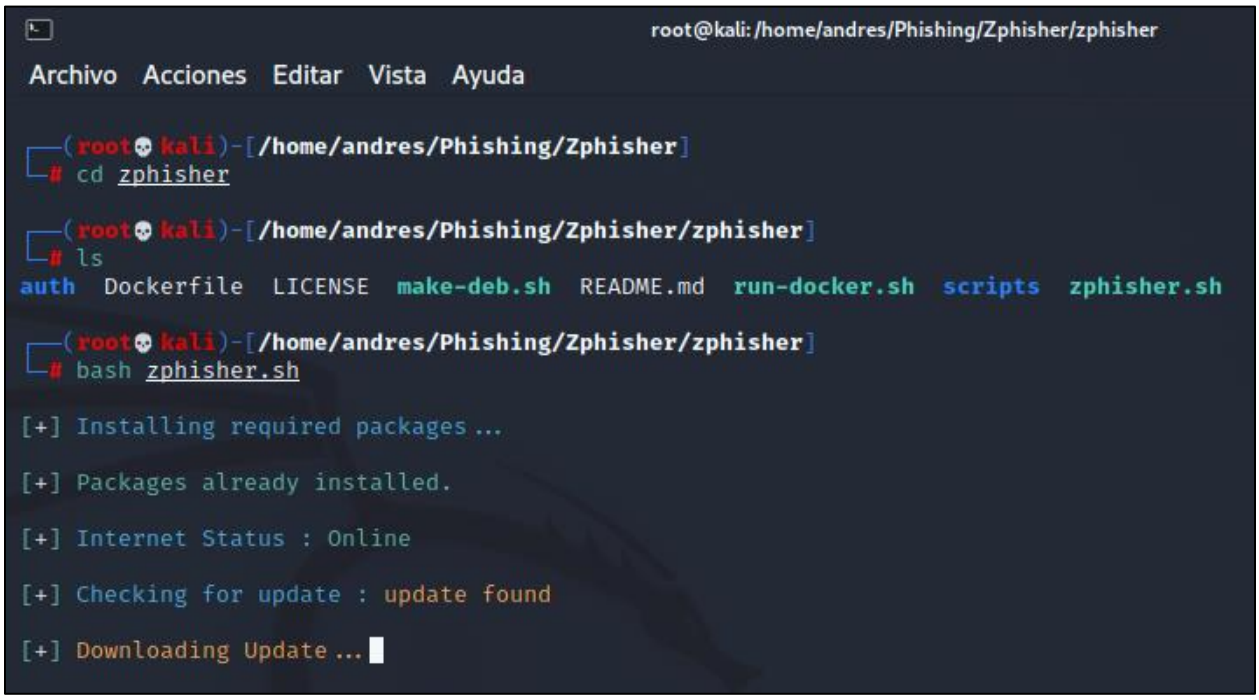
Nota: El gráfico representa el comando para descargar la herramienta Zphisher.

Este comando permite descargar la herramienta Zphisher directamente al Kali Linux desde el repositorio github.

2. Se debe acceder a la carpeta clonada “cd zphisher” y ejecutar el comando “bash zphisher.sh”.

Figura 35

Instalación de la herramienta Zphisher en Kali Linux



Nota: El gráfico representa los comandos para instalar la herramienta Zphisher.

Para utilizar Zphisher en Linux es necesario ubicarse en la carpeta donde se realizó la clonación de la herramienta y se ejecuta el bash zphisher.sh, esto permite que la herramienta se instale y actualice de manera correcta.

Creación del sitio web engañoso (Phishing)

Una vez que se ejecutó los comandos anteriores, la herramienta retorna las opciones de diferentes sitios web para su elección. En este caso se usará la plantilla de gmail para la simulación del ataque programado.

Figura 36

Sitios web a elegir

Nota: El gráfico representa las opciones de sitios web que brinda la herramienta Zphisher.

Para este caso se selecciona la opción 3, la cual pertenece a la página de Inicio de sesión de Gmail, seguido se elige la opción 1, que es la plantilla que más se asemeja a la original para que la víctima no pueda sospechar.

3. Se debe seleccionar la opción 3 y escribir el puerto que se desee fijar.

Figura 37

Elección del servidor

Nota: El gráfico representa la elección del puerto y servidor.

Es el momento de seleccionar el servidor, en el caso de que se requiera hacer la prueba dentro de una red local se debe seleccionar la opción 1, para este caso se requiere hacer la prueba fuera de la red local, para ello se puede usar tanto el servidor Ngrok.io como Cloudflared, se selecciona la opción 3. Seguido de ello la herramienta pide ingresar un número de puerto, para ello se coloca el puerto “8080”

4. Se selecciona la opción para enmascarar la url del sitio clonado.

Figura 38

Enmascaramiento de la url

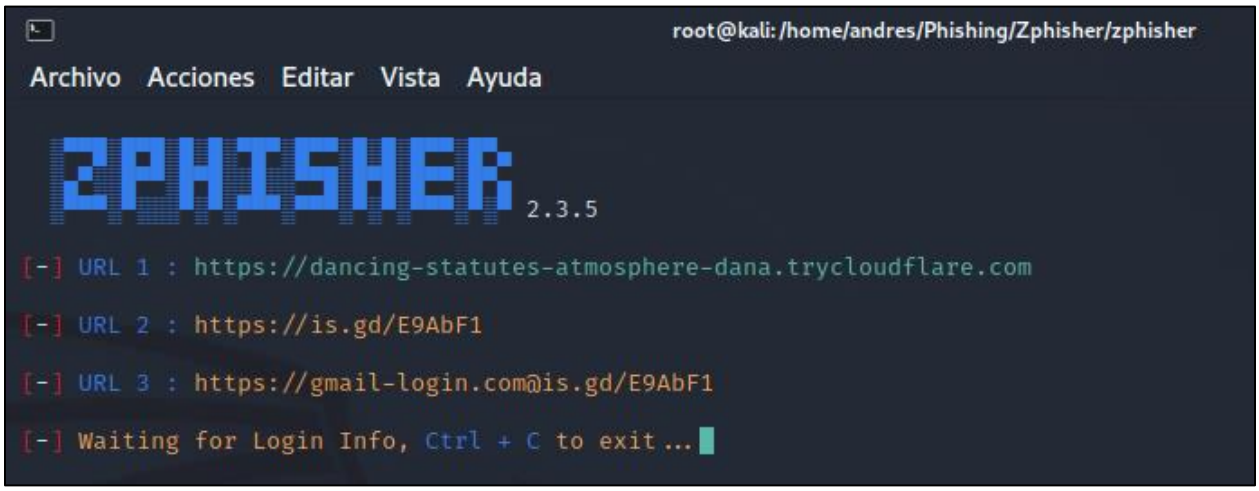
Nota: El gráfico representa la opción para enmascarar la url del sitio clonado.

Zphisher brinda la opción de poder enmascarar la url del sitio clonado, esto con el fin de que la víctima no tenga sospechas del ataque el cuál se encuentra simulando. Para ello se escribe “https://gmail-login.com”.

Finalmente, la herramienta crea 3 url para la página clonada, la que se asemeja más a la url de la página original es la tercera, la cual fue enmascarada.

Figura 39

Url generadas



Nota: El gráfico representa las tres url generadas por la herramienta Zphisher.

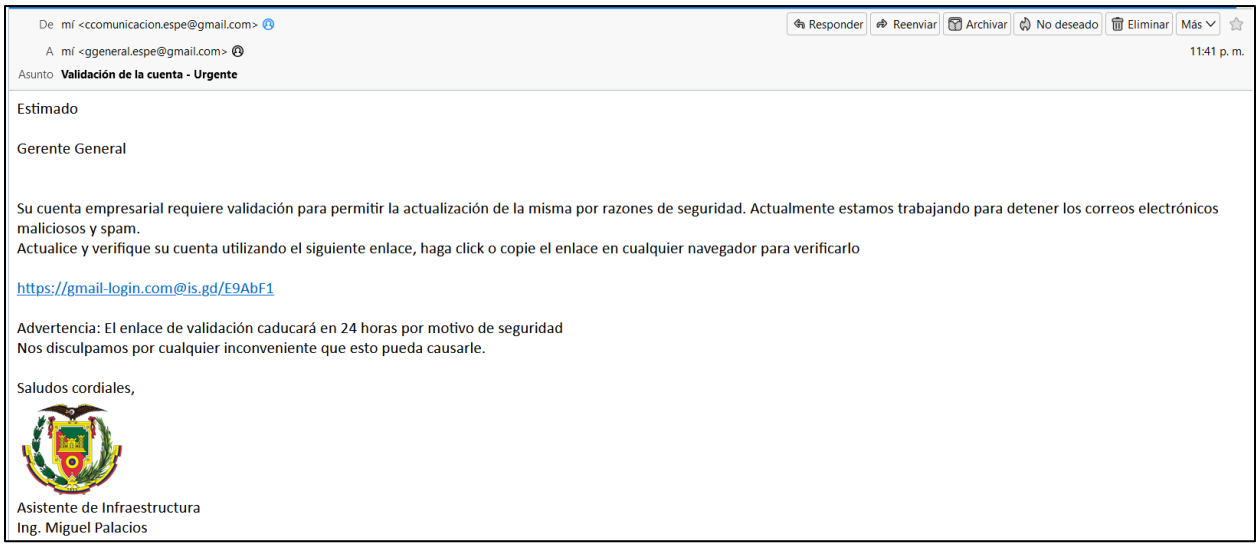
Una vez que se ha generado la url que será enviada a la víctima, se procede a crear el correo electrónico aplicando ingeniería social para que el usuario pueda ser una víctima más de suplantación de identidad.

Para ello hay que dirigirse a cualquier cliente de correo electrónico y redactar el email correspondiente, para este caso quedaría de la siguiente forma.

Ataque enviado por correo electrónico

Figura 40

Correo electrónico – ataque simulación

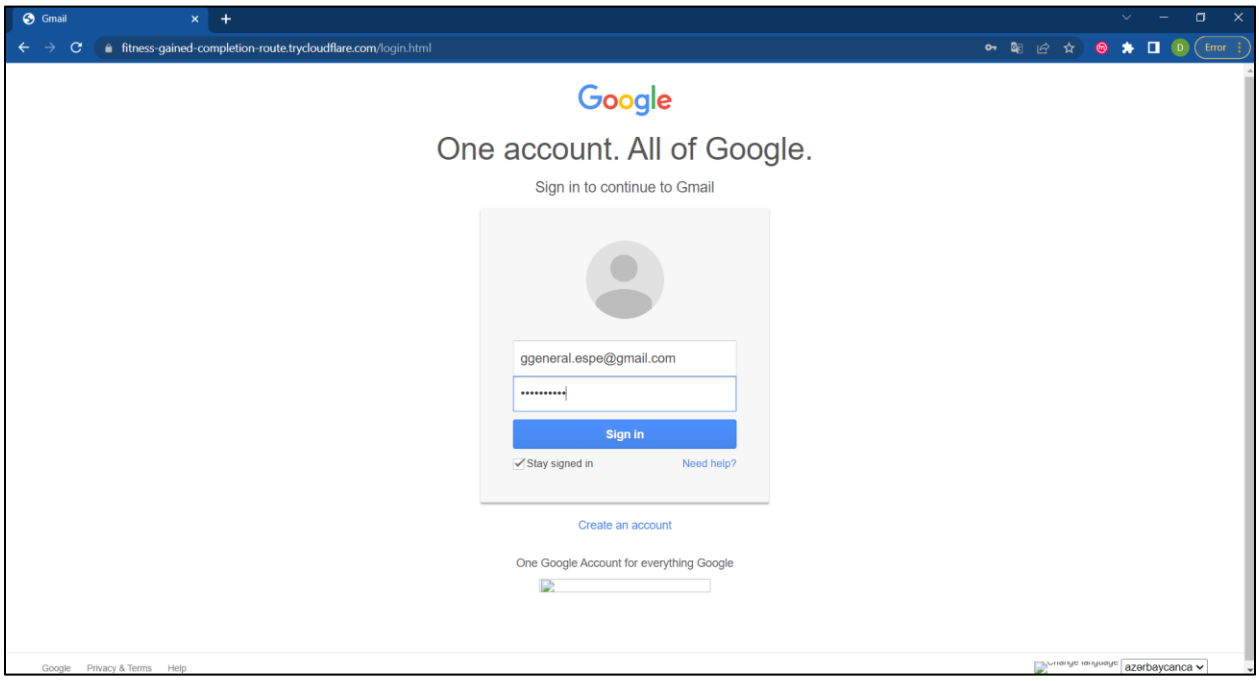


Nota: El gráfico representa el correo electrónico enviado al Gerente General.

Por parte de la víctima al abrir el enlace malicioso le redirigirá a una página muy parecida a la original, en la cual pedirá sus credenciales para iniciar sesión en la cuenta de correo electrónico.

Figura 41

Página clonada por parte del atacante



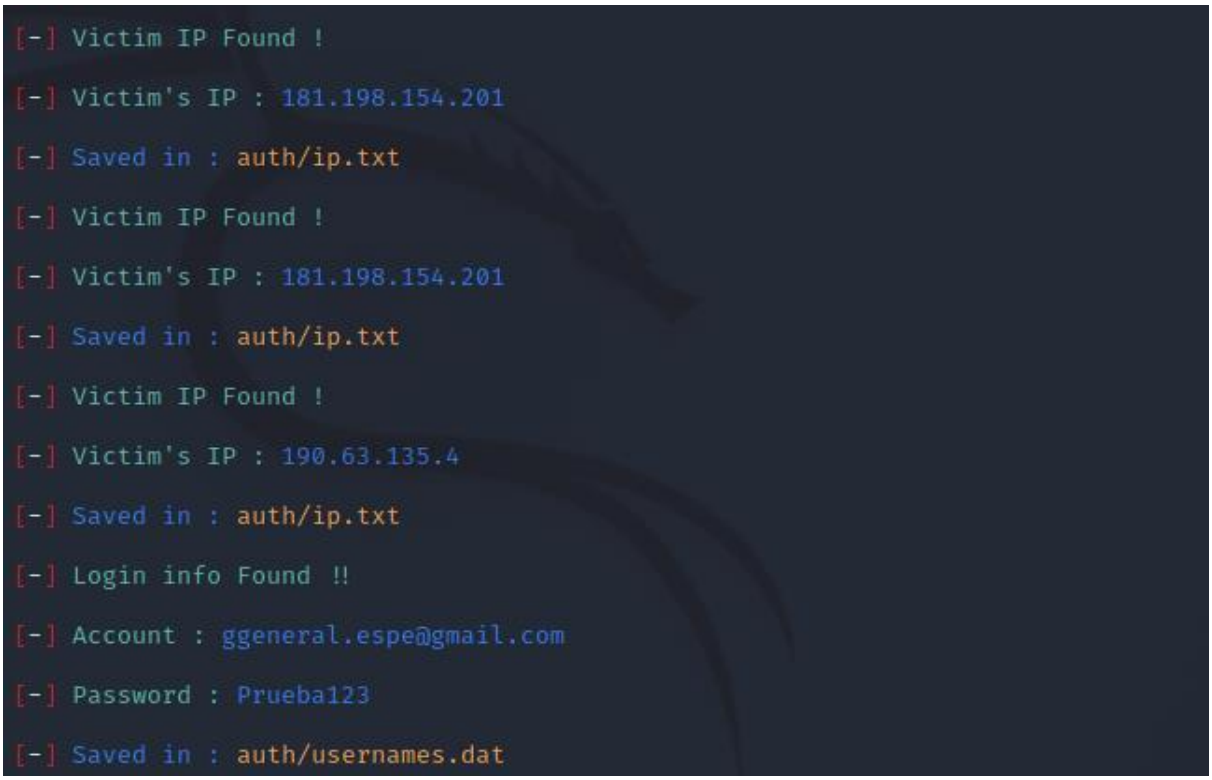
Nota: El gráfico representa la página clonada por el atacante.

Al momento que la víctima ingrese a dicha página y coloque sus credenciales personales, automáticamente el atacante recibirá dicha información en su sistema operativo, como se puede ver a continuación.

Obtención de credenciales personales por parte del atacante

Figura 42

Datos obtenidos por el atacante



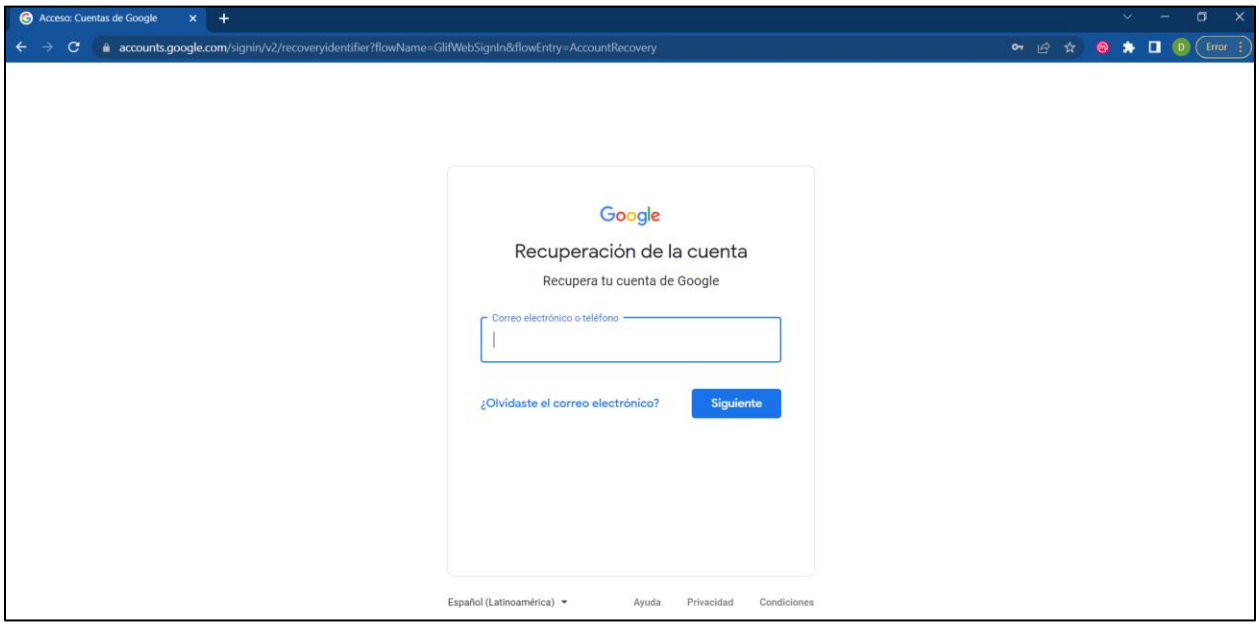
Nota: El gráfico representa las credenciales robadas por parte del atacante.

Como se observa en la figura anterior, la herramienta ha conseguido la IP de la víctima cuando abrió el mensaje y posteriormente las credenciales cuando fueron ingresadas. Toda esta información se guarda en los archivos “ip.txt” y “usernames.dat”.

Una vez que la persona haya sido víctima del ataque, será redirigida a la página oficial de la plataforma para evitar alguna sospecha por parte del destinatario.

Figura 43

Redirección del enlace malicioso



Nota: El gráfico representa la página a la que fue redireccionado la víctima luego de ingresar sus datos personales.

Capítulo IV

Captura y análisis comparativo de los resultados obtenidos

El presente capítulo tiene como fin presentar y analizar los resultados obtenidos del sistema de seguridad implementado para correos electrónicos para posteriormente comparar el desempeño y el grado de seguridad entre un sistema de correos tradicional y un sistema de correos electrónicos cifrado, usando PGP.

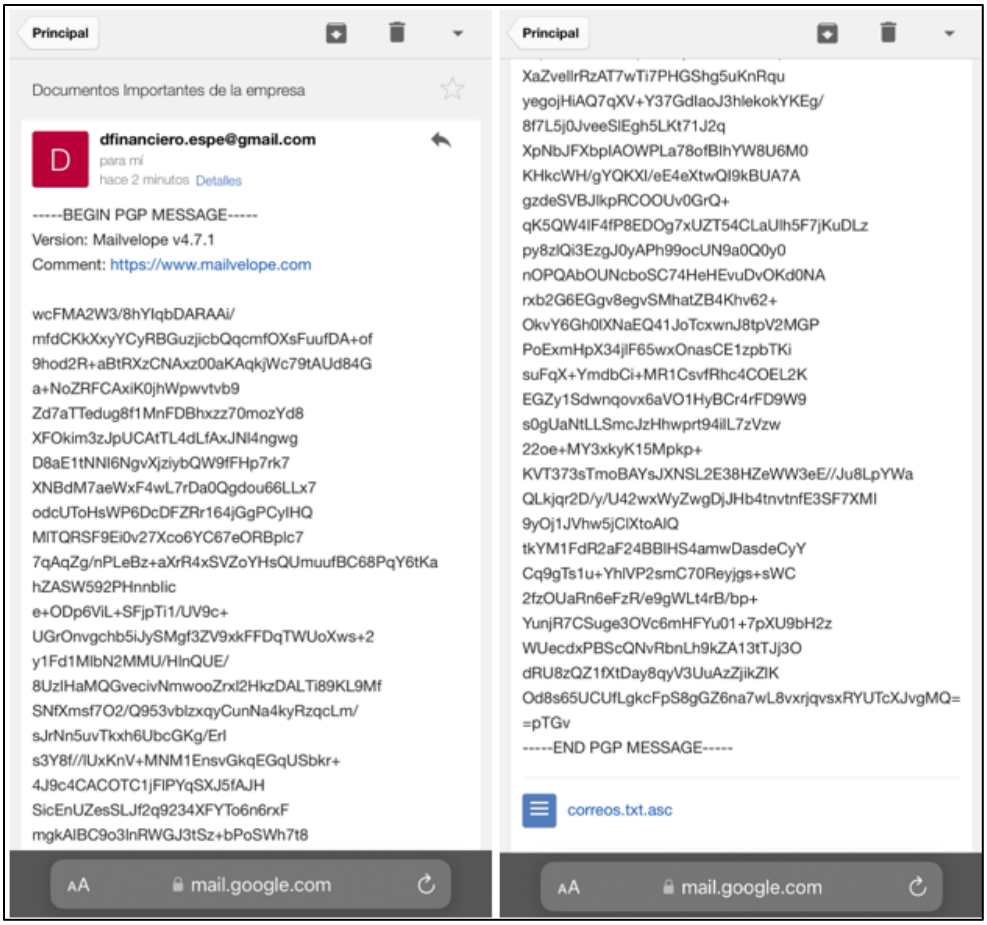
Prueba de efectividad en correos electrónicos cifrados.

Una vez que el atacante se haya apoderado de las credenciales personales del usuario víctima, procederá a ingresar a la cuenta de correo electrónico para leer y robar información importante para la empresa, y de alguna forma poder extorsionarlos con dicha información.

El atacante puede ingresar a la cuenta fácilmente, sin embargo, cuando proceda abrir algún correo electrónico importante no podrá ser leído ya que no posee la clave privada del usuario para poder descifrar el contenido del mensaje. Por lo tanto, lo único que podrá visualizar el ladrón cibernético es lo siguiente.

Figura 44

Correo electrónico encriptado



Nota: El gráfico representa el correo electrónico encriptado de parte del atacante.

Ya que el ladrón cibernético no posee la configuración previa de la clave privada del propietario de la cuenta, no podrá ver el contenido del correo electrónico, ya que, este se encuentra cifrado con GPG.

De igual forma, cuando el atacante decida enviar un correo electrónico desde dicha cuenta vulnerada, los destinatarios podrán darse cuenta de que no es el dueño legítimo de la cuenta, ya que, no será legible la firma electrónica por falta de configuración de la clave privada del remitente.

Análisis para evitar ataques de Phishing

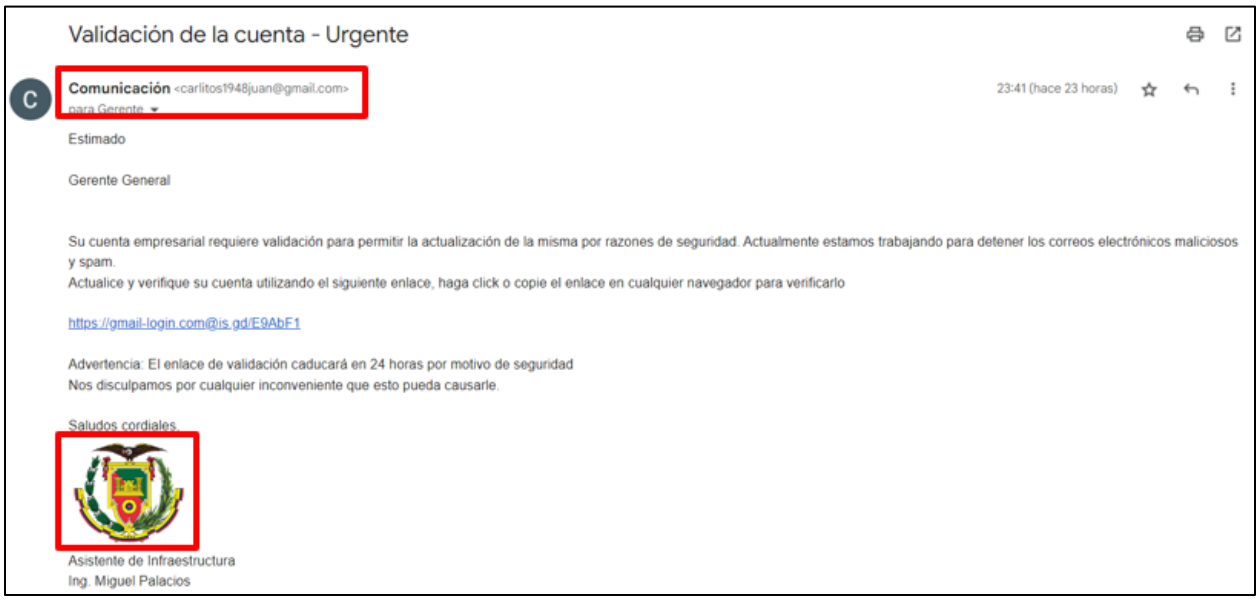
El Phishing es una técnica que usan los ciberdelincuentes para engañar al usuario y poder obtener información personal y confidencial. Los atacantes usan principalmente los correos electrónicos para lanzar este tipo de ataques, en los cuales pueden incluir un enlace malicioso que lleva al usuario a un sitio web conocido, pero que es una clonación del original donde se solicita información personal.

De esta manera las víctimas se confían y acceden a estos sitios que simplemente buscan robar su información, es por esta razón que es importante aprender a identificar claramente los correos electrónicos sospechosos. Para ello se puede seguir ciertas recomendaciones.

Una de las más populares es la que se puso en práctica anteriormente, enviar un correo haciéndose pasar por alguna empresa o persona y enviar una url que redirija a la víctima al sitio de phishing. Para estos casos es muy importante verificar que el correo del remitente sea el correcto, dependiendo de la empresa o persona que envía el email. Adicional se debe verificar que los logos de la empresa que envía el mensaje sean los correctos y los actualizados.

Figura 45

Prevención contra el Phishing de correos electrónicos



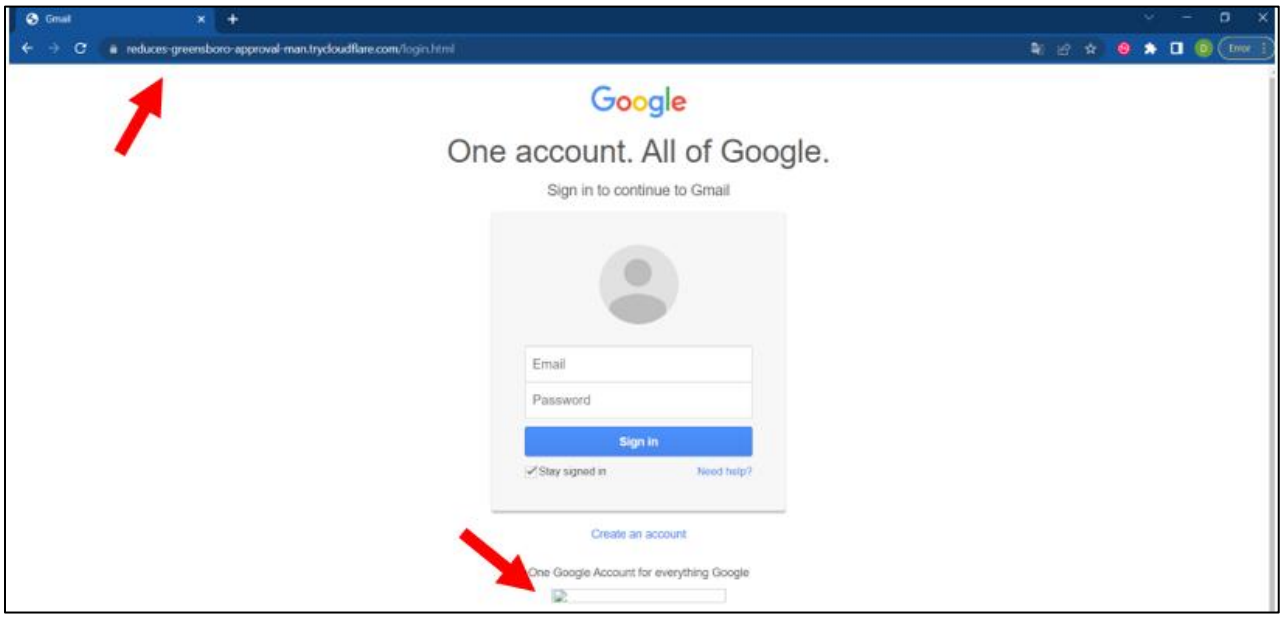
Nota: El gráfico representa las observaciones que se debe tener para no caer en la trampa del Phishing mediante correo electrónico.

También es posible analizar la página a la cual se ha redirigido mediante la url recibida. Dentro del sitio web es muy importante revisar que la “url” sea exactamente la misma a la original, por lo general los sitios que son phishing tienen pequeños cambios en la dirección, sean letras o números, tratando de ser lo más engañoso posible, un claro ejemplo puede ser “www.gmailk.com/login”, sabiendo que la página oficial es “www.gmail.com”, como se puede observar cambia solo una letra, haciendo que la víctima no tome en cuenta esos pequeños detalles.

Centrándose en el ataque de ejemplo realizado anteriormente, se puede verificar ciertas falencias en el correo que pueden ayudar a detectar que un sitio web no es el oficial y que está suplantando la información para poder abusar de la inocencia de los usuarios y robar credenciales o información importante para las personas.

Figura 46

Prevención contra el Phishing de sitios web



Nota: El gráfico representa las observaciones que se debe tener para no caer en la trampa del Phishing en un sitio web.

Observando la figura anterior es fácil darse cuenta de que la url del sitio web es muy diferente a la del sitio original, desde ese punto ya se puede catalogar y sospechar de este sitio web, de igual forma las imágenes son desactualizadas y no cargan correctamente. Finalmente se puede llegar a la conclusión que efectivamente esta página está suplantando la identidad de Gmail y phishing.

Análisis de la cabecera de correo electrónico

Se analiza la cabecera ya que este es el registro de los detalles técnicos que existe en un correo electrónico, dentro de este apartado se encuentra información tanto del emisor como

del receptor permitiendo conocer toda la trayectoria que ha tenido el correo, desde un principio hasta el final, incluyendo los distintos servidores por los que ha pasado.

Estas cabeceras pueden parecer complejas y difíciles de interpretar, pero si se las analiza de una manera detenida y entendiendo cada parámetro no son tan complicadas como parecen, sin embargo, existen herramientas que parsean toda esta información para poder tener un mejor entendimiento de estas.

Para este caso se ha enviado dos correos electrónicos exactamente iguales, con el mismo contenido, con la diferencia que uno se encuentra cifrado mediante GPG y con una firma digital mientras que el otro no está cifrado.

Figura 47

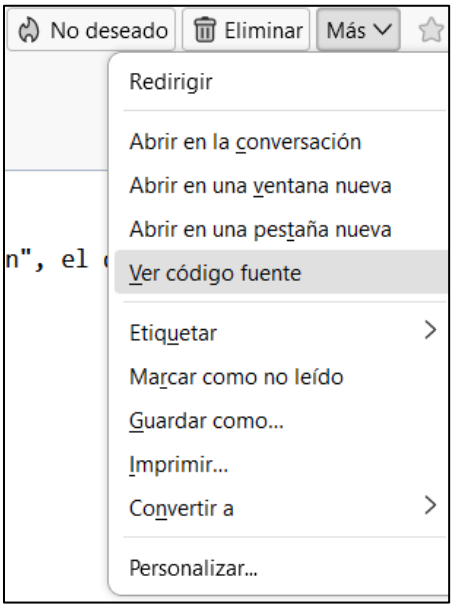
Correos enviados (Cifrado y sin cifrar)

Nota: La figura representa los dos correos electrónicos enviados, con el mismo contenido. Uno cifrado y el otro sin cifrar.

Como se observa en la figura anterior, se ha enviado dos correos con el mismo contenido, el primero cifrando el correo electrónico y el segundo sin cifrarlo. Esto con el fin de comparar las diferencias que existen entre los dos. Para poder realizar dicho análisis se verifica el encabezado de los correos.

Figura 48

Ver código fuente



Nota: La figura representa la opción para ver el encabezado del correo electrónico, dando clic en "ver código fuente".

De esta manera se obtiene la información para analizar correspondiente a los dos casos presentados anteriormente.

Figura 49

Encabezado correo cifrado con PGP

```
Delivered-To: ccomunicacion.espe@gmail.com
Received: by 2002:a50:6241:0:b0:1f4:ab8e:a3ef with SMTP id k1csp106640ech;
        Sat, 14 Jan 2023 16:03:24 -0800 (PST)
X-Received: by 2002:a05:6102:3204:b0:3d2:422f:77ac with SMTP id r4-20020a056102320400b003d2422f77acmr807651vsf.1.1673741004577;
        Sat, 14 Jan 2023 16:03:24 -0800 (PST)
ARC-Seal: i=1; a=rsa-sha256; t=1673741004; cv=none;
        d=google.com; s=arc-20160816;
        b=j8n/RAQLp7fL40+kOvT+zIrEK9bbZyp4QoghnK0Os2c+k/2ljS95FBX1GThDGujlKW
         1qCHnPYDUVPXIpF9QnJ7ZsMfEp3+dCarQoZL2ealOxwDAg6qEPC355cdsdbiVYdI38YP
         GsYJU8zAEcaUf3bIKkYnCWr/G+N7N/x3fE1YM9MXiOHC6zRN4QSngpaK8y7oDJdAex4o
         87lIeHhQiiaDab7YdrUtJhyLHDzMCVZVzwCiN6hOLBu+ROab68f8FSjIerRXTIkqxr0v
         ops2gu0tDvSp2vSc1XA0GVG+Jdi+5AajRTzUGOWk/x7HbD+w0MO1BXjRfpP2wtq5L+IW
         Tk5g==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
        h=subject:autocrypt:from:to:user-agent:mime-version:date:message-id
         :dkim-signature;
        bh=Sbm4Lx2+WW2EMIyL6Lvivrz67OMepO2DDA0k9wILdwc=;
        b=PP5XZ+0aBQwRaMX16i7GOrj8BjSC+G2NpfD7QLdC37RdCnE11lB64OXrjqNTCjJvXJ
         dR8KnNfUzOPxCsWwkWD3mSpH/EcYkQmyivnmLxYiBjm8D5B6YW6l6V3ZUCsSzQjOqxZ+
         KqQthLIjSfZYNe3lcfOXTYtZQUZ6A+uMQu7aaC30+gJhQMBPhTMtG0lcEyEOOAhpwBHZ
         uXa2XP1BOFHBRPd6RRyB7V43I3QQ3pMfUC9k40IVNhFzFTyI2mdckDerfotRzFTNpQhm
         yq0wEvSfEgxbmGC137qzd4FSrifwyXxl/f2rQYFXfP2QI3rmvwsnBeBCvZ7XHGS2i6Aw
         pWcQ==
ARC-Authentication-Results: i=1; mx.google.com;
       dkim=pass header.i=@gmail.com header.s=20210112 header.b=GxWChDUG;
       spf=pass (google.com: domain of ggeneral.espe@gmail.com designates 209.85.220.41 as permitted sender) smtp.mailfrom=ggeneral.espe@gmail.com;
       dmarc=pass (p=NONE sp=QUARANTINE dis=NONE) header.from=gmail.com
Return-Path: <ggeneral.espe@gmail.com>
Received: from mail-sor-f41.google.com (mail-sor-f41.google.com. [209.85.220.41])
        by mx.google.com with SMTPS id l26-20020a056102051a00b003d1eb40667fsor1881364vsa.68.2023.01.14.16.03.24
        for <ccomunicacion.espe@gmail.com>
        (Google Transport Security);
        Sat, 14 Jan 2023 16:03:24 -0800 (PST)
Received-SPF: pass (google.com: domain of ggeneral.espe@gmail.com designates 209.85.220.41 as permitted sender) client-ip=209.85.220.41;
Authentication-Results: mx.google.com;
       dkim=pass header.i=@gmail.com header.s=20210112 header.b=GxWChDUG;
       spf=pass (google.com: domain of ggeneral.espe@gmail.com designates 209.85.220.41 as permitted sender) smtp.mailfrom=ggeneral.espe@gmail.com;
       dmarc=pass (p=NONE sp=QUARANTINE dis=NONE) header.from=gmail.com
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
```

Nota: La figura representa el encabezado del correo electrónico cifrado con PGP.

Es una gran cantidad de información la cual es necesario analizarla de forma detenida para poder entender todos los campos que brinda.

Figura 50

Encabezado correo sin cifrado

```
Delivered-To: ccomunicacion.espe@gmail.com
Received: by 2002:a50:6241:0:b0:1f4:ab8e:a3ef with SMTP id k1csp106930ech;
        Sat, 14 Jan 2023 16:03:54 -0800 (PST)
X-Received: by 2002:a67:ef01:0:b0:3d0:d9a3:fdc2 with SMTP id j1-20020a67ef01000000b003d0d9a3fdc2mr11073356vsr.28.1673741034690;
        Sat, 14 Jan 2023 16:03:54 -0800 (PST)
ARC-Seal: i=1; a=rsa-sha256; t=1673741034; cv=none;
        d=google.com; s=arc-20160816;
        b=ylD8jMV8Wc/oNmeGyvNfMKwfmFAJctvgPeOdv5fth3QlQdnByi3EfY2gPw+7LkCnFT
         eHzUEjWnE2QfJXLJBwvAFIHFxDCmhsSmF5dvZvYM40TQZ9svp/4fYfpF4lzfxH1Ji48y
         5V6eJXoAQ/V8t8XfatxQ0q0h/3MCC/AIHTvGus7aDh2XWAZV7FBgzmH4R1kqvTPchB3k
         jCV+PbgHF+cEjO0JjvrmQ61HIQ2njZFHCNVNuLsgoSqTd8zPO643MHRiuwbx0uuaoE8Z
         iQ4nMtNW+CDBzkQIf5nzGAHZzLxaQlKwpMe0P4l5KlaSyMWpouFkeNpjOa6EyzJ9y1MR
         jc5w==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
        h=content-transfer-encoding:subject:from:to:user-agent:mime-version
         :date:message-id:dkim-signature;
        bh=6ZVxfN78vALfy9yDVIQEr3sRLQQ+NCvEIypwQocsx9g=;
        b=fYjB88chfjOpAKxBxEscu2CmDW7+2HZn63xr+UInKgj+WxJ6n6xQhlLOLF1aDudIjf
         a36k6LaC8pZRpyxnQRNMZ4qjHqQdHm7LpmvCSfJ8fhMQrWNu++/dJXv933eX9vDWmBrb
         CDrKX/iTVfRScEKNo3QdRPMBkKZaMSdP1/GAuwU6DZ0p1lR/oJe3gEpJ+AagGkJkV9Ya
         VQy0+S+eVkKllZD4Eotu4eWHkdAxdDQc46mYUhuwOPl3H/jHMGOKijrAWvcA3PffKhKR
         kaBl+v1Le/MqOZFcBilZFp/spR3Bn4UOxfvSqgVDrURN73wT+duc7droTa/hNuV8T/h+
         /ZOQ==
ARC-Authentication-Results: i=1; mx.google.com;
       dkim=pass header.i=@gmail.com header.s=20210112 header.b=OapIjNiH;
       spf=pass (google.com: domain of ggeneral.espe@gmail.com designates 209.85.220.41 as permitted sender) smtp.mailfrom=ggeneral.espe@gmail.com;
       dmarc=pass (p=NONE sp=QUARANTINE dis=NONE) header.from=gmail.com
Return-Path: <ggeneral.espe@gmail.com>
Received: from mail-sor-f41.google.com (mail-sor-f41.google.com. [209.85.220.41])
        by mx.google.com with SMTPS id h25-20020a67c599000000b003d0cce40bf1sor879456vsk.88.2023.01.14.16.03.54
        for <ccomunicacion.espe@gmail.com>
        (Google Transport Security);
        Sat, 14 Jan 2023 16:03:54 -0800 (PST)
Received-SPF: pass (google.com: domain of ggeneral.espe@gmail.com designates 209.85.220.41 as permitted sender) client-ip=209.85.220.41;
Authentication-Results: mx.google.com;
       dkim=pass header.i=@gmail.com header.s=20210112 header.b=OapIjNiH;
       spf=pass (google.com: domain of ggeneral.espe@gmail.com designates 209.85.220.41 as permitted sender) smtp.mailfrom=ggeneral.espe@gmail.com;
       dmarc=pass (p=NONE sp=QUARANTINE dis=NONE) header.from=gmail.com
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
```

Nota: La figura representa el encabezado del correo electrónico sin cifrado.

A simple vista toda esta información puede parecer muy compleja, se puede analizar cada línea o en este caso ayudarse con la herramienta Mxtoolbox, que en su página web posee un analizador de encabezados en línea. Teniendo como resultado los siguientes parámetros a analizar.

Tabla 4

Ventajas y desventajas del protocolo POP3

Correo electrónico cifrado con PGP	Correo electrónico sin cifrado
Return-Path: <ggeneral.espe@gmail.com> Message-ID: <46837a1d-f3f3-01f0-a1ae-f3dd1752c930@gmail.com> Date: Sat, 14 Jan 2023 19:03:21 -0500 MIME-Version: 1.0 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Thunderbird/102.6.1 To: ccomunicacion.espe@gmail.com From: Gerente General <ggeneral.espe@gmail.com> Autocrypt: addr=ggeneral.espe@gmail.com; keydata= xsFNBGNzESYBEADRhdDgeF6ercTdu88eeogSTFq42Grv8rr3SkaFmuUfD7PHvCSHaq9VqAr+ ECAW7I7lwc9nrwGN5xTR14umXZVl1+h9Vg4xbEFss1kElHicgRwSi+nctpT1vFp39bFMRFJu /xKAYZw0h/mfV5lfQx5kPJsWVZFsP6KU0shtED8KTjyccNB2COqd7zA5SkEAbrq2Cg0iYmLM 6r6cV7YA8iky5kXJ6e+HjSg5Q3XhBxcFZmSeuOeq1lmGf9GrLhjemH4r7iqHem6Cb9qULZej pWTXcawN7DOD5Y5Ub6TUelRzjnSbxBdNZO9xQyn3/MUJFdxCm2pJTiui/UB1AZEvxHygFh0F cjEVL7SO5VS5mWGqbWDM96Bz9F6UJ8BmKvCRlfGEFKSY10esIkiyYejT41lMcC6F4Gp4t5yo tloLtmc4fisrtCOSkSxLy6luaRoPeczzK+BnFusMj2RZBujzIAq2nuc5tWK4WZDJ9Yyqwkbg cA0rkR4wrtHhtZfvpqlxEU8EWnxFMXEVm9tLTMuSr7/ptafAIQCi9PARezQIJqjhV/y9eezB Uap/1wsYBbVH4oFbScsUdOYmimc7nheXweHiDyQguU6V3tdKGLaTUTFjpEgqcKUBVSsYrN5e ztxWLnQlAzrl4GQXcoM8th/qFGSxvzY3rTBOkAVn6qjeaEsRawARAQABzSlHZXJlbnRlIEdl bmVyYWwgPGdnZW5lcmFsLmVzcGVAZ21haWwuY29tPsLBlwQTAQgAQRYhBEtGTkVKylmVjyEY tRW+q3zDwt++BQJjcxEmAhsDBQkDwxtqBQsJCAcCAiICBhUKCQgLAgQWAgMBAh4HAheAAAoJ EBW+q3zDwt++rN8P/R2nG/ye8wE4Pla4sEgaXl3ib3SyKno4tTkMnEi+Woxcrtlzfwp3Q+p AbsRU7thqb95c4Wfj1AQqJX3vVW/m1Ji8vQHhFxf1WeG2ewFa43WawUb/ryPPYC7n5dWRAVH hppfMh9AI4bOA6BfgQ279xMqRKx8UwX1UAUgWHFcLC8UsQpreDTKOTwbTlOjy7uoGrCs/d+R tPmCu2jFFXqeoLTXA03aFnXH4ioUjlNxTSjukUnXJ0WdF8NbWgTmLPr0J/0xJsRH0bG4zzuD gp+LzaDxiJumm+V89m/DaepEiRVo7e78WPSLupGcduh0nfKbkTkldSZxUjoZHRbUOtbJPdVP 3aUsaYvymAzt6uzGqWB	Return-Path: <ggeneral.espe@gmail.com> X-Gm-Message-State: AFqh2krEAb9m6/2HwJXdkAehkYfEHDB1ayoAZjH1Fsn6qKyDqhS73iQdWNzhvKp5Jvv8+d/8O5iHTmjfnoVBxZl= X-Google-Smtp-Source: AMrXdXuiqngYfRtksTZhknefevCy9VkB2PrjMI1WgfL26hjejxYbwGCYHIHaHKc0grErUv72+CobvA== Message-ID: <0203d2aa-6e3f-bca5-aea6-2ec7562b05c7@gmail.com> Date: Sat, 14 Jan 2023 19:03:52 -0500 MIME-Version: 1.0 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Thunderbird/102.6.1 To: ccomunicacion.espe@gmail.com From: Gerente General <ggeneral.espe@gmail.com> Subject: Convocatoria cena de navidad Content-Type: text/plain; charset=UTF-8; format=flowed Content-Transfer-Encoding: 8bit
Subject: ... Content-Type: multipart/encrypted; protocol="application/pgp-encrypted"; boundary="----------7ts7wx4Wqp1so5jNB0RD0maK"	

Nota. En la tabla se muestra los encabezados parseados por la herramienta Mxtoolbox

Dentro de esta cabecera se analiza la siguiente información:

- **From:** Este apartado contiene la información del remitente. Es necesario tener en cuenta que los atacantes suelen clonar o falsificar las direcciones de correo electrónico en este campo, es por eso que es necesario revisarlo. Para estos casos se puede visualizar que el campo es el mismo.

- **To:** Se muestra la dirección del correo electrónico del destinatario, adicionalmente suele incluirse las direcciones de correo electrónico de la copia de seguridad (CC) y copia oculta (CCO). Para estos dos casos igualmente se verifica que son los mismos.
- **Fecha:** Este campo muestra cuándo se envió exactamente el correo electrónico, por lo general el formato que utilizan es (hh:mm:ss)
- **Return-Path:** Este campo es importante, ya que, proporciona la dirección de correo electrónico a la cual el sistema enviará su menasje.
- **Subject:** Aquí se puede verificar una de las primeras diferencias entre estos dos correos, como se puede observar en el correo cifrado, el asunto de igual forma se encuentra encriptado, por lo que no se lo puede visualizar. Por otro lado, el correo no cifrado muestra claramente el asunto con cuál fue enviado el mensaje.
- **Message – ID:** Al momento de redactar un mensaje, se crea una serie de letras y números, estas pueden ser alteradas por los ciberdelincuentes.
- **MIME-version:** Multi-Purpose Internet Mail Extensions. Es una extension del protocolo de correo electrónico, este permite enviar y recibir varios tipos de archivos de datos, sean fotos, videos o audios.
- **Content-Type:** En este campo se puede ver una diferencia importante entre los dos sistemas, esta área especifica si el correo electrónico se encuentra escrito en formato de texto plano o si se encuentra encriptado. Como se puede observar en la anterior tabla, uno muestra que se encuentra encriptado mediante el protocolo pgp, mientras que el otro transmite su información en texto plano.

Identificar toda esta información es sumamente necesario e importante, ya que estos campos proporcionan identificadores críticos del mensaje, sin esta información no se puede determinar de quién procede el mensaje y cuál fue su recorrido, así mismo ofrecen una descripción detallada de la dirección IP del remitente, lo que ayuda a verificar el origen del mensaje y de este modo resulta mucho más fácil detectar si el mensaje es fraudulento o enviado por un ciberdelincuente.

Análisis del retraso recibido

Al momento de realizar las pruebas anteriores, se verificó que el sistema que contiene cifrado y el que no, entre estos no existe gran diferencia en el retraso de la transmisión del correo electrónico, ya que, el correo no era tan pesado y no contenía algún archivo adjunto. Sin embargo, esto cambia cuando existe una gran transmisión de datos, para ello se ha realizado el envío de dos correos con archivos adjuntos iguales y del mismo tamaño, con la diferencia que un correo electrónico es cifrado mediante PGP y el otro no.

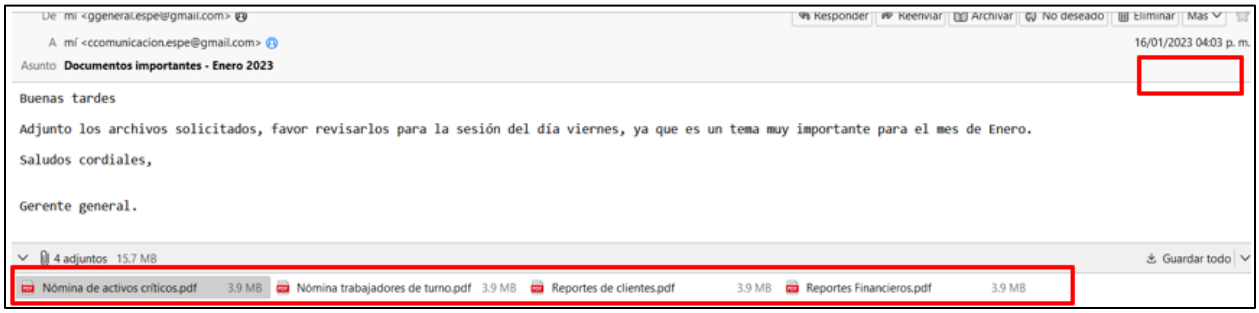
Figura 51

Correo electrónico con archivos adjuntos - cifrado

Nota: La figura representa un correo electrónico con archivos adjuntos y cifrado.

Figura 52

Correo electrónico con archivos adjuntos – no cifrado



Nota: La figura representa un correo electrónico con archivos adjuntos y que no se encuentra cifrado.

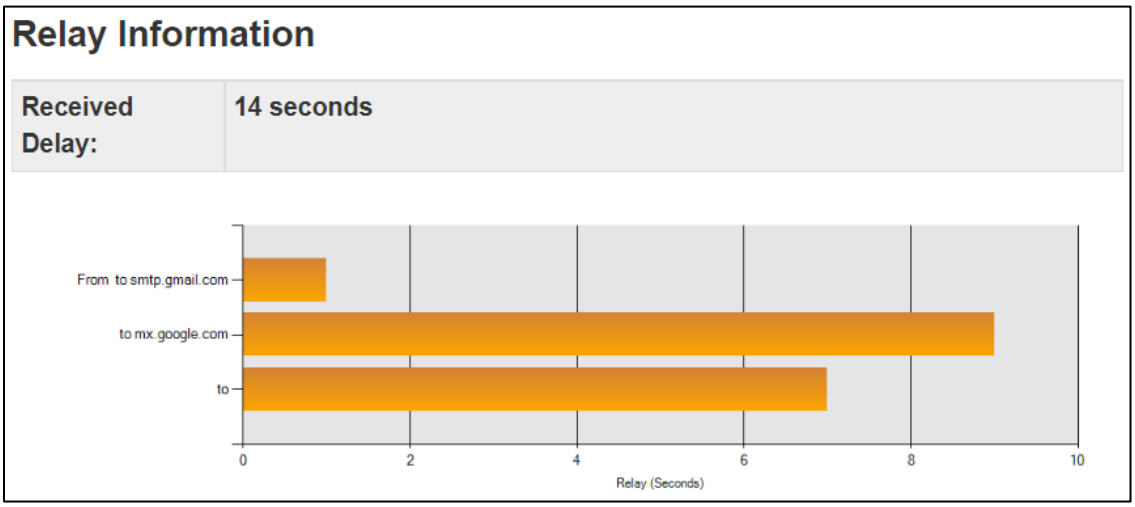
En las dos anteriores figuras se observa los correos que se han enviado al destinatario, los dos contienen la misma información y los mismos archivos adjuntos, con la única diferencia que uno se encuentra cifrado con PGP, mientras que el otro no.

Analizando los encabezados tanto del correo cifrado como del no cifrado en la herramienta Mxtoolbox, se puede verificar la información de retransmisión. Teniendo como resultado lo siguiente.

Para el correo electrónico cifrado se puede evidenciar que existe un retraso de 14 segundos. Esto puede ser debido a que al momento de cifrar un correo con PGP, este tiende a ser más pesado por lo que puede provocar un congestionamiento en la red y una demora en la recepción del mismo. A su vez el correo contiene archivos adjuntos, lo que hace que exista una demora en la entrega.

Figura 53

Información de retraso en correo electrónico – cifrado

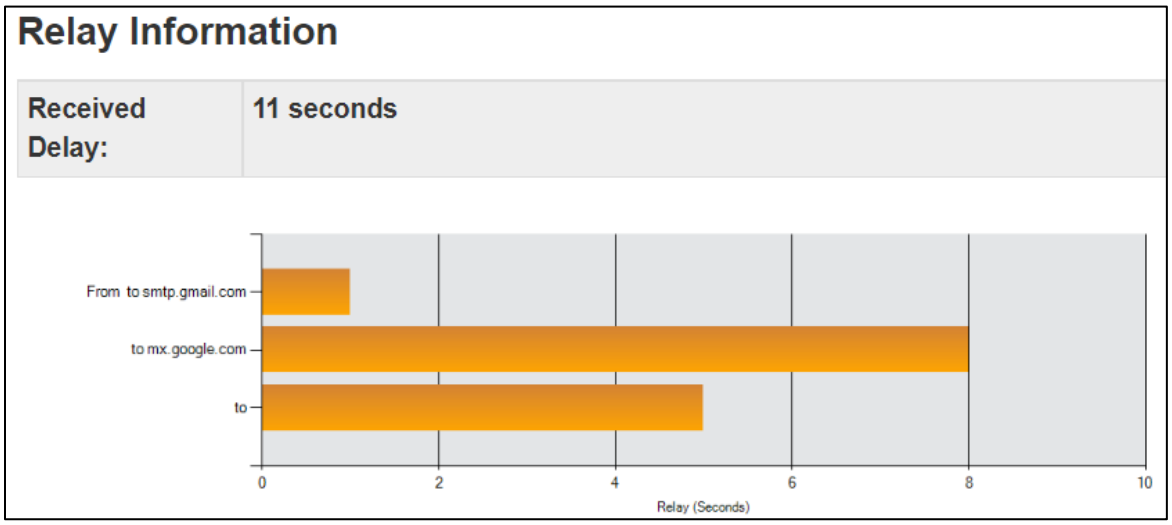


Nota: La figura representa el retraso que existe en la recepción de un correo electrónico cifrado con PGP.

Por otro lado, el mismo correo electrónico sin cifrar tiene una demora de 11 segundos, tiempo menos que el correo cifrado. Esto se debe a que el tamaño de transmisión de datos es menor, ya que la información no se encuentra encriptada.

Figura 54

Información de retraso en correo electrónico – no cifrado



Nota: La figura representa el retraso que existe en la recepción de un correo electrónico que no se encuentra cifrado.

En términos generales se sabe que la informática no es una ciencia exacta y el tiempo en que un correo llega a su destino depende de muchos más factores adicionales a los que se evidenció anteriormente, en muchos casos depende de la ruta que hace por los servidores.

Capítulo V

Conclusiones y Recomendaciones

Conclusiones

Se realizó un análisis comparativo entre un sistema de correos electrónicos cifrado frente a uno no cifrado, donde se logró comprobar las ventajas y desventajas de cada uno de ellos, llegando a la conclusión que cifrar los mensajes de correo electrónico es sumamente importante dentro de una organización, ya que de esta manera se puede proteger los datos y evitar suplantaciones de identidad.

En base al análisis realizado en el presente trabajo se ha comprobado que la confidencialidad, integridad y disponibilidad es un engranaje indispensable para la seguridad de la información, es por esa razón que para poder cumplir con estos tres principios fundamentales es necesaria la implementación de PGP en los correos electrónicos, además de una firma electrónica que ayuda a verificar la autenticidad del remitente.

Los ataques de simulación de phishing fueron realizados en el sistema operativo Kali Linux, dentro de los cuales se pudo verificar el correcto funcionamiento del cifrado y firma digital en los correos electrónicos, a pesar de que la víctima entregó sus credenciales mediante un engaño, el atacante no puede tener acceso a la información de los correos ya que esta se encuentra encriptada y para poder desencriptarla es necesario disponer de la clave privada.

Se optó por usar el software Kleopatra para la creación de las claves tanto pública como privada, ya que es una herramienta que soporta múltiples sistemas operativos, permite cifrar y proteger archivos o documentos con la ayuda de una interfaz gráfica interactiva con el usuario.

Se logró realizar un sistema de cifrado y firma digital para correos electrónicos, el cual brinda seguridad e integridad y disminuye el riesgo de impacto de un posible ataque por correo electrónico.

Mediante el análisis realizado en este proyecto se puede llegar a la conclusión que un sistema de correos electrónicos cifrado y que cuente con una firma digital posee un grado de seguridad mucho más elevado que un sistema de correos que no sea cifrado, ya que este se transmite en texto plano, es decir que, si el mensaje es interceptado por un atacante, este podrá ver todo el contenido sin ningún problema, caso que no sucederá con el sistema que tiene implementado PGP.

Una de las principales desventajas que tiene el cifrado PGP es la complejidad y la curva de aprendizaje que este pueda causar, ya que suele ser intimidantes y un poco más complejos de entender para usuarios con poco conocimiento en el área, por lo que esto demanda la implementación de capacitaciones continuas a los empleados.

Recomendaciones

Se recomienda que dentro de la organización se proporcione a los empleados capacitaciones en el área de ciberseguridad, esto con el fin de evitar que el usuario pueda ser víctima de ataques de phishing dentro de los cuales entreguen información valiosa o a su vez credenciales que puedan ser críticas para la empresa.

Se recomienda verificar todos los campos que existen dentro de la cabecera de correo electrónico, para que de esta manera se evite caer en intentos de suplantación de identidad y se entregue credenciales o información que sea de gran valor para la empresa.

Es muy importante que al momento de generar las claves públicas como privadas, estas se almacenen en un lugar seguro que ninguna otra persona pueda tener acceso. Esto con el fin de que ninguna persona externa al usuario original pueda acceder a la información que contiene el correo electrónico.

Para implementar este tipo de sistemas es necesario considerar la facilidad de uso para los usuarios que van a manejar estos métodos, por esta razón es recomendable elegir un

software que cuente con una interfaz visual fácil de manejar, permitiendo que el usuario no tenga complicaciones al momento de usarla.

Dentro de una empresa es muy importante realizar campañas de concientización mensualmente a los empleados, con el objetivo de verificar si los usuarios se encuentran asistiendo a las capacitaciones otorgadas por la empresa y de igual manera si se encuentran adquiriendo los conocimientos de forma satisfactoria.

Bibliografía

ASALE. (s.f.). *REAL ACADEMIA ESPAÑOLA*. Obtenido de https://dle.rae.es/criptograf%C3%ADa

Bjorkelund, M. (2022). Evaluación y mejora del proceso para configurar. 32-35.

Dhamija, R. (2006). Why phishing works. *Proceedings of the SIGCHI conference* , 581-590.

Fenrich, K. (2008). Securing your control system: the "CIA triad" is a widely used benchmark for evaluating information system security effectiveness. *Power Engineering, 112*(2), 44-49.

Garfinkel, S. (1995). *PGP: Pretty Good Privacy.* O'Reilly & Associates, Inc.

Gargallo, B. (2021). Correo electrónico y firma digital. *Universidad Jaume*, 20-24.

Giron, I. (2022). Aplicaciones de la Criptografía en Ciberseguridad. *Núcleo de Investigación en Inteligencia Artificial y Data Science*, 5-8.

Kaspersky. (2022). *¿Qué es el spear phishing?* Obtenido de https://latam.kaspersky.com/resource-center/definitions/spear-phishing

Kontinen, V. (2020). Preventing email forgery in Finland : Research on the current SPF and DMARC implementations.

Lopez, B. (2009). Cómo funciona el correo electrónico? Protocolo SMTP. *Universidad Nacional Autónoma de México*.

Mendoza, J. (2018). Demostración de cifrado simétrico y asimétrico. *Revista de Ciencia y Tecnología, 3*, 46-53.

Mendoza, J. C. (2018). Demostracion de cifrado simétrico y asimétrico. *Ingenius: Revista de Ciencia y Tecnología*, 46-53.

MITRE.ORG. (2021). *Compromise Accounts: Email Accounts*. Obtenido de https://attack.mitre.org/techniques/T1586/002/

Rincón Nuñez, P. (2021). Impacto de los ataques de ingeniería social en Colombia desde el año 2016 hasta el año 2019. *Repositorio Institucional UNAD*.

Whittaker, S., Belloti, V., & Gwizdka, J. (2006). Email in personal information management. *Communications of the ACM*, 68-73.