PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR SEDE ESMERALDAS

CARRERA:
INGENIERÍA DE SISTEMAS Y COMPUTACIÓN

TESIS DE GRADO

TEMA DE INVESTIGACIÓN:
INTEROPERABILIDAD DE MENSAJES PROTEGIDOS CON CRIPTOGRAFÍA UTILIZANDO EL PROTOCOLO PGP.

LÍNEA DE INVESTIGACIÓN:
REDES Y COMUNICACIONES

PREVIO A LA OBTENCIÓN DEL TÍTULO DE:
INGENIERÍA DE SISTEMAS Y COMPUTACIÓN

AUTOR:
FAVIO RONALDO ANDRADE MEZA

ASESOR:
Ms. C. WILSON CHANGO

ESMERALDAS, 2020

TRIBUNAL DE GRADUACIÓN

Trabajo de tesis aceptado luego de haber dado cumplimiento a los requisitos exigidos por el reglamento de Grado de la PUCESE previo a la obtención del título INGENIERÍA DE SISTEMAS Y COMPUTACIÓN

_____

Presidente del tribunal de graduación

_____

Lector 1 José Luis Carvajal

_____

Lector 2 Juan Casierra Cavada

_____

Director de Tesis Wilson chango

_____

Director de Escuela

Esmeraldas, …… del 2021

AUTORÍA

Yo, Favio Ronaldo Andrade Meza, declaro que la presente investigación, enmarcada en el actual trabajo de tesis, es absolutamente original, autentica y personal, y en virtud de eso declaro que el contenido de esta investigación es de exclusiva responsabilidad legal y académica del autor y de la PUCESE

_____

Favio Ronaldo Andrade Meza
C.I: 0802843201

AGRADECIMIENTO

A Dios ante todas las cosas, por ser mi guía para seguir adelante en todo lo que me plantee y quiera alcanzarlo, por darme la virtud de tener sabiduría, salud y firmeza para seguir con mis estudios.

A mi madre Tania Meza a mi tía Edith Suárez y a mi familia en general que son mi motivación cada día para seguir luchando con mi anhelo de graduarme, mi abuelita Mercedes Meza y demás familiares por el apoyo incondicional y humanístico, comprensión, que hace que quiera cada día a la profesión que escogí.

A mis compañeros, amigos que con paciencia en momentos de desesperación me supieron brindar palabras de alientos para seguir adelante en mi vida estudiantil.

A las autoridades de la Pontificia Universidad Católica de Esmeraldas y docentes quienes me ayudaron a mi formación académica para en un futuro poner en práctica todo lo aprendido.

FAVIO RONALDO ANDRADE MEZA.

DEDICATORIA

A mi mamá, mi familia, a mi tía Edith, que siempre han estado en los momentos más dificultosos de mi vida y por nada del mundo me han dejado caer, enseñándome a tener optimismo confianza en todos los pasos que doy, a quererme, a ser humilde, tener la capacidad de aceptar mis errores con la cabeza en alto.

Gracias a todos por no resaltar mis defectos y hacer sobresalir mis virtudes, siempre estuvieron conmigo para darme aliento en cualquier decisión que tome, dando lo mejor de ellos sus consejos, para poder culminar mi meta de terminar mi carrera profesional, y poder tener un futuro mejor.

FAVIO RONALDO ANDRADE MEZA.

CONTENIDO

INDICE DE FIGURAS

INDICE DE TABLAS

INDICE DE ANEXOS

FÓRMULAS

Título: Interoperabilidad de mensajes protegidos con criptografía utilizando el protocolo PGP.

1. Resumen

Se realizó el estudio con la técnica de criptografía para desarrollar mayor seguridad y confidencialidad en los datos de los usuarios, es decir, aplicar analizar los diferentes protocolos de encriptación como bitmessage, openpgp, extensiones de correo de Internet seguras / multipropósito (por sus siglas en ingles S/MIME). Está técnica se estudia por el motivo que puede determinar el gran riesgo que tienen las informaciones en los servidores de correos electrónicos, implementando el protocolo pgp para observar las necesidades actuales y la peligrosidad de la información de los correos electrónico. Para la evaluación de manera correcta se realizó mediante los métodos inductivo y deductivo, acompañado del diseño del experimento para evaluar los problemas que han tenido con el servidor actual.

Los resultados obtenidos en dicha investigación se pudieron notar que los servidores son más seguros si se contratan los servicios desde la nueve ya que estos implementan protocolos de seguridad más certeros y ayudan a que la integridad del servidor no sea vulnerada.

En comparación con los resultados de estudios anteriormente ejecutados por otros autores, se pudo notar que estos serán de mucha ayuda para otras instituciones debido a que en algunos estudios utilizaron la criptografía, utilizando distintas herramientas o instrumentos de investigación. Según los resultados se podría decir que se pudo evaluar de forma correcta los ataques al servidor de correos electrónicos.

Como conclusión de la investigación se preparó un prototipo de sistema de correo a través del protocolo guardia de privacidad GNU (por sus siglas en ingles GPG) con la herramienta openpgp, la cual permitió encriptar los mensajes brindando un aumento de seguridad considerable ayudando también a mitigar los varios ataques al servidor de correo. Por otro lado, se descartó la posibilidad del ataque *man in the mid* que generalmente se hacía cuando la información almacenada en la nube queda segura ya que se encontraría encriptada y solo el receptor podrá revelar su contenido. Mediante la verificación por contraseña solo el receptor identifique la identidad del usuario que esta enviado la información.

2. Abstract

The study was carried out with the cryptography technique to develop greater security and confidentiality in user data, that is, to apply analyze the different encryption protocols such as bitmessage, openpgp, S / MIME. This technique is studied for the reason that it can determine the great risk of the information on the email servers. Implementing the pgp protocol to observe the current needs and the dangerousness of email information. For the correct evaluation, it was carried out

using the inductive and deductive methods, accompanied by the design of the experiment to evaluate the problems they have had with the current server.

The results obtained in said research could be noted that the servers are more secure if the services are contracted from the nine since they implement more accurate security protocols and help to ensure that the integrity of the server is not violated.

Compared with the results of studies previously carried out by other authors, it could be noted that these will be very helpful for other institutions because in some studies they used cryptography, using different tools or research instruments. According to the results, it could be said that the attacks on the email server could be correctly evaluated.

As a conclusion of the investigation, a prototype of a mail system was prepared through the GPS protocol with the openpgp tool, which allowed the encryption of messages, which increased considerable security, also helping to mitigate the various attacks on the mail server. On the other hand, the possibility of the man in the mid attack was ruled out, which was generally carried out when the information stored in the cloud is secure since it would be encrypted and only the receiver will be able to reveal its content. By means of password verification, only the receiver identifies the identity of the user who is sending the information.

3. Introducción

1.1. Presentación de la investigación

Inicialmente el internet fue creado con el fin de mantener la comunicación entre las personas y organizaciones, pero con el pasar del tiempo, al ir evolucionando y al enviarse información privada y de alta importancia a nivel organizacional, industrial y personal, los sistemas han ido evolucionando de tal manera que deben incorporar mecanismos de seguridad y privacidad de datos cada vez sofisticados de manera que sean lo más seguros y confiables posibles para que los usuarios realicen cualquier comunicación a través del ciberespacio [1], estos mecanismos no solo buscan proteger equipos y datos sino también pretenden ganar la confianza de los usuarios para que ellos se sientan seguros y protegidos con estos mecanismos.

A lo largo del tiempo los usuarios han sido testigos de ataques a servidores de correo electrónico muy famosos, en los que se han extraído información muy valiosa. Está el caso muy famoso de "*WikiLeaks*", el ataque de *phishing* contra el principal asesor de campaña de Hillary Clinton John Podesta [2], donde se ha evidenciado mucha información proveniente desde servidores de correo electrónico. Así también se ha tenido registro de miles de sucesos parecidos en los que se ve violentada la privacidad

de una persona, estos usuarios lo que buscan en estos servidores de correo es seguridad; es decir, saber que pueden compartir información, debatir sobre un tema en específico sin correr el riesgo de que esta información sea violentada. Asimismo, se ha visto en algunos casos que se suelen realizar cambios en el contenido de la información para que el mensaje no llegue con claridad al receptor.

1.2. Planteamiento del problema

La seguridad en los correos electrónicos no está exenta de ser vulnerada. Por esto, cada vez se implementan nuevos protocolos de seguridad para proteger esta información, entre estos protocolos de seguridad existen los de encriptación como: bitmessage [3], Privacidad bastante buena (por sus siglas en ingles openpgp) [4], Extensiones seguras / multipropósito de correo de Internet (por sus siglas en ingles S/MIME) [5]. Estos protocolos protegen la mensajería de un sistema de correo electrónico encriptando los datos de los mensajes, para que nadie más aparte del destinatario lo puedan leer, estos mensajes son encriptados con una clave pública y desencriptados con una clave privada que es la del receptor.

La interoperabilidad de los mensajes en los servidores de correo electrónico es importante para todo servidor de correos electrónico. Se deben ahondar esfuerzos para brindar un grado elevado de seguridad para sus usuarios, esta seguridad puede ser en el ámbito de las verificaciones, los cortafuegos, la protección contra spam, pero en esta investigación se busca demostrar por qué es tan importante obtener una buena encriptación de los correos electrónicos para proveer un servicio de mensajería de correo electrónico seguro y altamente confiable que pueda ser empleado por organizaciones y a nivel personal. Este aspecto es sumamente importante en la sociedad actual, sobre todo cuando después de la pandemia, muchas de las comunicaciones se están realizando a través de mensajería de correo electrónico.

Todo lo antes expuesto nos lleva preguntas como: ¿Cómo se pueden proteger tu información utilizando el protocolo pgp?

La criptografía tiene como objetivo proteger documentos y datos que trabajan a través del uso de cifras o códigos para escribir algo oculto en documentos y datos confidenciales que circular en redes locales o en el internet. Su utilización es tan

antigua como la escritura. Los romanos utilizaban códigos para esconder sus proyectos de guerra de aquellos que no debían conocerlos, con el fin de que sólo las personas que conocían el significado de estos códigos interpreten el mensaje oculto. Con la ayuda del protocolo pgp se puede brindar un componente de autenticación para algunas comunicaciones y corregir la privacidad de estas, tiene una enorme importancia debido a que es el sistema criptográfico de calidad más usado en el mundo. El pgp también sobrelleva firmas digitales, lo que permite comprobar la integridad y autenticidad de un mensaje para saber si este realmente fue enviado por quien dice, y saber si no fue alterado en el camino [4].

Sin embargo, la criptografía se ha encargado de formular el algoritmo criptográfico más seguro desde sus inicios comenzando por simples desplazamientos de letras del alfabeto hasta la actualidad, teniendo métodos con posibilidades de facilitar claves de hasta 256 bits y varias iteraciones para encriptar la información, siendo la unión de muchos algoritmos criptográficos la mejor opción para el resguardo de la información. En 2017, Medina [6], manifiesta que a nivel mundial la utilización de criptografía hoy en día se ha vuelto parte esencial de los sistemas informáticos de empresas u organizaciones, siendo los elementos la confidencialidad, disponibilidad e integridad y no repudio las que hacen el estado seguro de la información.

A nivel nacional, las empresas tienen como garantía que los sistemas sean interoperables significa que se pudo acceder a más información y funcionalidades útiles desde un único entorno de manera práctica y fiable. Posibilitando la eficiencia, rentabilidad, garantía de las conexiones abiertas de los productos de una empresa con mayor flexibilidad en los formatos de los documentos, la interoperabilidad es un elemento muy importante para el desarrollo de información, donde se realiza el intercambio oportuno de datos, documentos y objetivos entre sistemas de información. En la actualidad las normas y estándares nacionales han creado nuevas propuestas donde se desarrollan principalmente por federaciones de redes internacionales como federación internacional de asociaciones e instituciones de bibliotecas (por sus siglas del inglés IFLA), centro de biblioteca de la universidad de Ohio (por sus siglas del inglés OCLC), los cuales se basan en el intercambio y apoyo de la interoperabilidad [6].

En la ciudad de Esmeraldas se implementó un plan estratégico informático de tecnología donde el gobierno autónomo provincial descentralizado de Esmeraldas (GAPDE) estableció estructuras organizacionales que reflejan las necesidades institucionales, la cual es examinada de manera periódica para concordar estrategias internas que permitan satisfacer los objetivos planeados y puedan soporten los avances tecnológicos. A nivel de tecnologías de la información y la comunicación (TIC) el único medio de comunicación es la página web, cuyo dominio es: www.prefectura.gob.ec y contiene material producido por la Dirección de Relaciones Públicas, la cual ha estado al mando de la administración del sitio web hasta el 8 de mayo del 2012 mediante un memorando GADPE-RP-2012-238 otorgando las claves para que la dirección de TIC realice los cambios técnicos, previo requerimiento de ellos. El profesional tiene y usa correos electrónicos privados de libre registro, por falta de correo institucional, por tal motivo que se gestionó la adquisición de correos con el nombre www.gadpe.gob.ec, que permite una comunicación interna y externa [7].

1.3. Justificación

Esta investigación es fundamental para las empresas que utilizan correos electrónicos las cuales corren el riesgo de que la información sea violentada y su privacidad sea afectada, por ese motivo este estudio implementó un sistema informático de seguridad que permite reconocer con exactitud quién remite el mensaje. El mismo que tiene como ventaja alcanzar un impacto de satisfacción a los que hagan uso de ello.

Una vez obtenido los resultados será de mucha ayuda para instituciones públicas o privadas para el mejoramiento de seguridad en el uso de la información por medio de correos. Al observar la falta de seguridad que existe en la empresa Zamarino S.A se utilizará la metodología pertinente para poder observar y analizar cuáles son las problemáticas que presenta y así poder resolverlas por medio de protocolos de seguridad como es el protocolo pgp.

El uso contenedores entre ellos docker ayudará a que las aplicaciones se desplieguen con mayor rapidez y la información que se transmita por el servidor de correo electrónico sea más eficaz, también se acortarán los tiempos de ejecución de los

procesos al permitir una conexión directa entre la base de datos y el servidor de correo electrónico. Con la implementación de esta herramienta se puede separar la base de datos en un contenedor y el servidor de correo electrónico en otro contenedor obteniendo la independización de ambos procesos.

1.4. Objetivo

Objetivo general

Desarrollar la interoperabilidad de mensajes de correos electrónicos mediante el uso de criptografía para brindar mayor seguridad y confidencialidad en los datos de los usuarios.

Objetivos específicos

1. Analizar los diferentes protocolos de encriptación como bitmessage, openpgp, S/MIME.
2. Preparar un prototipo de sistema de correo que implemente el protocolo pgp a través de poste.io.
3. Valorar el nivel de seguridad del prototipo de correo propuesto y la buena aplicación de la triada cia.

2. Marco teórico

2.1. Bases teóricas-científicas

En la siguiente sección, se presentan algunas definiciones que permitirán saber y comprender de forma conceptual el caso de estudio presentado. Para esto en la sección uno se hablará sobre la seguridad y encriptación de los mensajes en que nos puede ayudar encriptar los mensajes y como el hecho de tener una buena seguridad puede proteger nuestra integridad. En la sección dos se determinará los protocolos de encriptación se realizará una comparativa entre los protocolos donde se determinará ventajas y desventajas del uso de cada uno de los protocolos. En la sección tres se tiene una evaluación de seguridad del prototipo de servidor de correo electrónico donde se analizará el funcionamiento, se valorará su nivel de seguridad y se llegará a una conclusión de los resultados. En la sección cuatro se hablará de los desafíos de

los usuarios con el uso del prototipo propuesto se realizarán pruebas con distintos usuarios y veremos qué tan amigable es el sistema con el uso también en esta sección llegaremos a una conclusión de la usabilidad del sistema.

2.1.1. Seguridad y encriptación de mensajes

La falta de seguridad en los servidores de correo electrónico ha sido conocida desde hace muchos años, esto ha provocado que mucha información valiosa. Estos acontecimientos han hecho que muchas empresas obtén por manejar su propio servidor de correo y así ellos mismos hacerse carga de la seguridad de sus mensajes, poder proteger su información. Con el pasar el tiempo el tema de la seguridad ha cogido más fuerza, por ello se han creado varios protocolos de programación entre ellos; bitmessage, openpgp (Privacidad bastante buena), Extensiones seguras / multipropósito de correo de Internet (por sus siglas en el inglés S/MIME).

El formato del mensaje de correo electrónico, tal como se describe en la declaración del problema de optimización de rutas de movilidad de red [6], consta de dos secciones, los campos de encabezado y el cuerpo. Los campos de encabezado son líneas que comienzan con un nombre de campo, seguidos de dos puntos (':') y el cuerpo del campo. Cada campo de encabezado comienza en una nueva línea y los nombres más comunes son: De, Para y Asunto[8]. Lo que significa que permite encriptar el mensaje por bloques, haciendo esta separación del mensaje y poder procesarlo de una manera más sencilla.

Cuando se envía un correo electrónico desde un servidor de correo privado a un servidor de correo público como Gmail, Outlook, etc. Estos mensajes que salen del remitente, tiene que pasar primero por el Agente de Transferencia de Correo (MTA), del servidor de correo de ellos, por ejemplo: La empresa Tecno Bits manda un correo electrónico a uno de sus clientes este correo primero pasa por el MTA del servidor de correos de Tecno Bits, en el cual se guardan copias del mensaje, tenemos que el cliente tiene un correo en Outlook, este mensaje antes de llegar al cliente pasa por otros MTA de Outlook, tiene que pasar por el MTA para analizar si es Spam o no, cada uno de estos MTA es una oportunidad para que se violente la seguridad y se

pueda revelar información privada del usuario como se puede observar en la FIGURA 1 *Proceso de envío de mensaje tomado de [2]*.

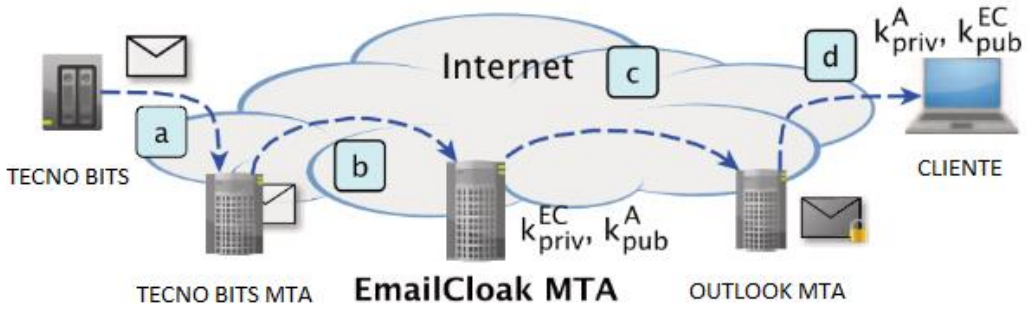


FIGURA 1 Proceso de envío de mensaje tomado de [2]

Para evitar esto y con la intención de que los usuarios cada día más confíen en los servidores de correo y que las empresas se decidan a implementar su servidor de correo y hacerse cargo de su propia seguridad se implementa la encriptación mediante protocolos estos protocolos hay unos de código como lo son: Bitmessage, Openpgp, S/MIME, TLS.

La criptografía de clave pública nos permite una mayor usabilidad en los protocolos de encriptación, al ser un cifrado de extremo a extremo se tiene la garantía de mantener la integridad de los datos y que no se vayan a corromper en el camino. Aparte no requiere de terceros de confianza uno de los más claros ejemplo de esto es Openpgp y S/MIME [4].

2.1.2. Protocolos de encriptación

La inseguridad en la navegación web día a día va en aumento y la información que se maneja en los servidores web específicamente en los servidores de correo, los usuarios buscan seguridad y las empresas de igual manera, una empresa que maneje un sistema de correo privado debe preocuparse por la seguridad que pueda implementar en este, para que la integridad de la información que se transmite por estos correos no se vea afectada, ya que vivimos en un mundo globalizado y todo debe de estar al alcance de todos, y que mejor manera de hacerlo con la web.

No solo basta con colocar la información en la web también a esta información debemos darle seguridad al ser transportada y ¿Cómo le damos esta seguridad? Pues con la implementación de los protocolos de encriptación.

Existen varios protocolos de encriptación que se han creado a lo largo del tiempo al ver la necesidad de la seguridad en la web y hablaremos de los más conocidos como: Openpgp, S/MIME, bitmessage.

2.1.2.1. Estructura de los protocolos

Openpgp

Es un protocolo de encriptación que adopta un modelo distribuido como web de confianza (por sus siglas en ingles WoT), este modelo nos va a proporcionar una fuente de confianza mediante las claves públicas con las cuales se puede saber con certeza que solo esa persona verá el mensaje a enviar, mediante este protocolo también permite usar las firmas digitales que funciona como doble seguridad la cual le da más veracidad a la información.

En 2017 Barenghi [3] manifiesta que “El WoT se basa en la llamada "suposición del mundo pequeño": dado un gráfico donde los nodos representan a las personas y los bordes modelan las relaciones personales entre ellos”. Esta suposición ayuda a entender de mejor manera este modelo porque va a permitir un mejor manejo del modelo y mejor privacidad de la información.

Cada usuario consta de una clave pública y una clave privada, también cuenta de un correo y su clave personal, esta clave publica esta autofirmado conocida como *self signed public key*, también se pueden añadir subclaves que deben estar enlazadas a esta clave principal estas subclaves servirán para firmar los documentos en las conversaciones privadas y así servir de una doble autenticación para los usuarios.

Openpgp tiene un esquema de mensajes híbridos donde se genera una clave por sesión, luego esta clave es usada para cifrar el mensaje que emplea un cifrado simétrico, para luego cifrarse con una de las subclaves del receptor, todas las subclaves están enlazadas a la clave pública principal mediante una firma enlazada con la clave privada principal [9].

Cada cliente openpgp tiene su propio almacenamiento local para certificados, conocido como llavero del propietario. Junto con el llavero, un almacenamiento adicional, el trustDB, contiene el "nivel de confianza" del propietario hacia los usuarios vinculados a los certificados en su llavero cuando actúan como una CA.

En 2017 Barenghi [4] manifiesta que la codificación de los paquetes que openpgp consta de dos partes el encabezado del paquete, este encabezado consta de un único byte denominado *tag packet* seguido de un campo de longitud variable denominado *body length* este último es el codifica el número de octetos que componen el cuerpo de un paquete, este proceso de encriptación se explica en FIGURA 2 *Proceso de encriptación y desencriptación de openpgp Fuente [11]*, también existen otras maneras de encriptar como lo muestra Dai en [10].

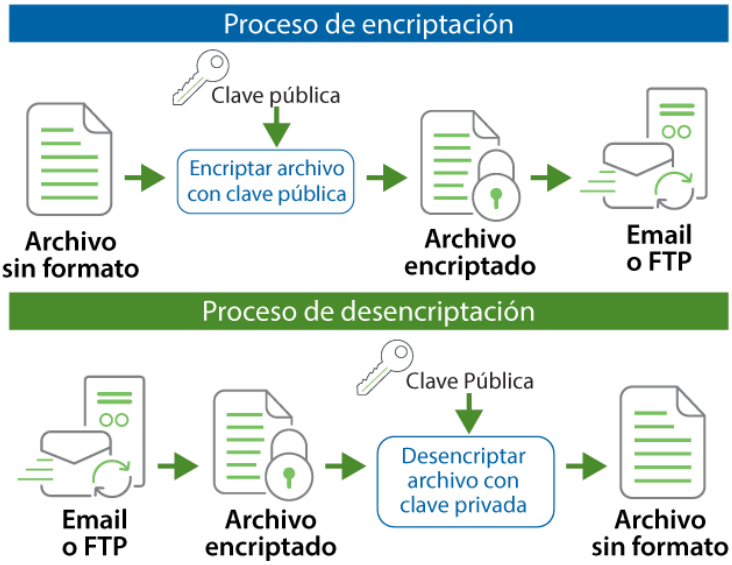


FIGURA 2 Proceso de encriptación y desencriptación de openpgp Fuente [11]

S/MIME

Extensiones multipropósito de correo de Internet (por sus siglas en ingles S/MIME) es un protocolo de correo electrónico; el protocolo original no proporciona esa gran cantidad de características de seguridad. S/MIME es una mejora de seguridad para el estándar de correo electrónico MIME. Esta mejora hace que los servicios de autenticación, integridad y privacidad estén disponibles[11]. Esto es vital ya que

ayuda a mejorar la seguridad del correo electronico brindando integridad y privacidad a la informacion que se comparte en el correo.

A pesar de la seguridad de este protocolo es alta también tiene una alta dependencia a los certificados X509, ya que estos certificados no están implicados en la implementación del protocolo, estos certificados tienen que ser conseguidos de forma externa a la implementación, los usuarios deben tomar medidas que muchas veces no quieren las empresas pueden obligar a sus usuarios a obtener un certificado pero los usuarios normales no lo harán ya que el proceso puede ser confuso para muchas personas [12]. Lo cual implica una confusion mayor a los usuarios, el hecho de tratar cocn certificados web hace que este protocolo sea poco apetecido al ser confuso de manejar.

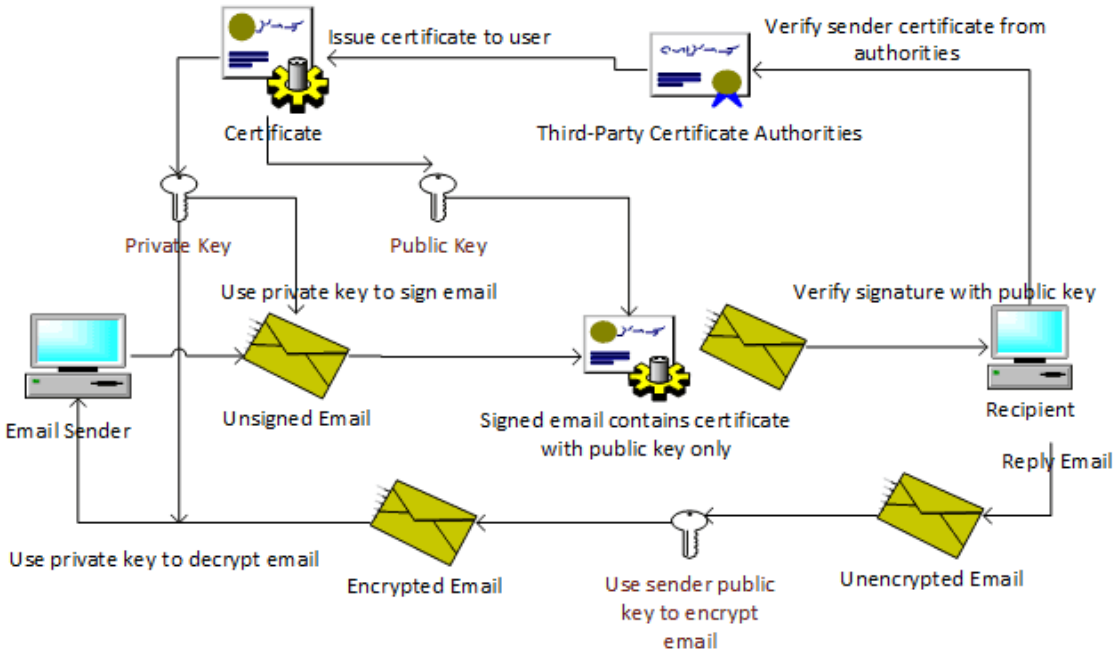


FIGURA 3 Proceso de encriptación de s/mime fuente: [14]

En FIGURA 3 *Proceso de encriptación de s/mime fuente: [14]* se observa el proceso de S/MIME [13] para el envío de mensajes primero se genera una clave aleatoria; esta clave se utiliza para cifrar los datos mediante un algoritmo simétrico. La clave se denomina clave de sesión, es decir, se utiliza en una sesión de correo electrónico. Como segundo paso cifra los datos utilizando el algoritmo simétrico designado como este "DES-CBC" utilizando la clave de sesión y añade su certificado, seguido de esto todos los datos de correo electrónico están cifrados. A continuación, el programa de correo electrónico cifra la clave de sesión utilizando el concepto de criptografía de

clave pública (es decir, utilizando la clave pública del receptor). Luego se genera un paquete que incluye los datos cifrados, la clave de sesión cifrada y el certificado X.509. Al final el programa de correo electrónico del usuario recibe un paquete consta de los datos cifrados y la clave de sesión cifrada. Por lo tanto, el paciente extrae la clave de sesión descifrando la clave de sesión utilizando su clave privada y a continuación, utiliza la clave de sesión para descifrar los datos de correo electrónico utilizando el mismo algoritmo simétrico [11].

BITMESSAGE

Bitmessage es un protocolo p2p, donde a cada par se le asigna una dirección larga de 34 caracteres. Esta dirección contiene un par de claves de criptografía de curva elíptica (ECC) y se utiliza para firmar y cifrar mensajes de usuario. Cuando Alice quiere enviar un mensaje a Bob, ella utiliza el *key* público de Bob, compuesto en su dirección, para cifrar el mensaje. Esta operación preserva la privacidad, sólo Bob es capaz de descifrar el mensaje, ya que es el único que posee la clave privada correspondiente[3].

Este protocolo también usa la criptografía asimétrica este protocolo nos presenta una red peer-to-peer también llamada p2p, la cual es una red de nodos conectados entre sí para luego ser depositados en la bandeja de entrada del destinatario al ser una encriptación asimétrica solo el receptor podrá desencriptar el mensaje. Este protocolo también permite recibir mensajes desde el anonimato con el fin de proteger la identidad del emisor, este protocolo es muy permisivo con el spam y esto hace que muchos usuarios no confíen en este servidor de correo.

El protocolo p2p hace imposible que se pueda rastrear un mensaje ya que para que el mensaje llegue al usuario final este se copia en todos los nodos de la red para así poder llegar a su destino. Para hacerlo aún más difícil las direcciones de usuario utilizadas son aleatorias lo cual hace que sea un reto al menos saber el nombre del emisor[14], lo cual es significativo porque ayuda a que el mensaje no pueda ser rastreado y hace que la tarea de descubrir el emisor sea complicada [15].

Según lo expuesto en los puntos anteriores se tiene los protocolos openpgp y s/mime, estos protocolos son muy parecidos porque ambos implementas la encriptación asimétrica, luego de ver las ventajas de cada uno de estos protocolos hemos visto

también la dificultad que hay para trabajar con s/mime ya que requiere la implementación de certificados esta implementación no ayuda a que la interacción con el usuario sea lo más sencilla posible. No obstante, openpgp no requiere implementación de certificados, pero si necesita que el usuario maneje las llaves públicas de sus contactos lo cual también puede ocasionar problemas con el manejo para sus usuarios. Observando estas dos situaciones la mejor Opción para implementar es openpgp.

DOCKER

Este proyecto de código abierto el cual usa contenedores de software, los cuales permiten la virtualización de aplicaciones en múltiples sistemas operativos.

En otras palabras, docker es una herramienta que puede empaquetar una aplicación y sus dependencias en un contenedor virtual que se puede ejecutar en cualquier servidor Linux. Esto ayuda a permitir la flexibilidad y portabilidad en donde la aplicación se puede ejecutar, ya sea en las instalaciones físicas, la nube pública, nube privada, etc.

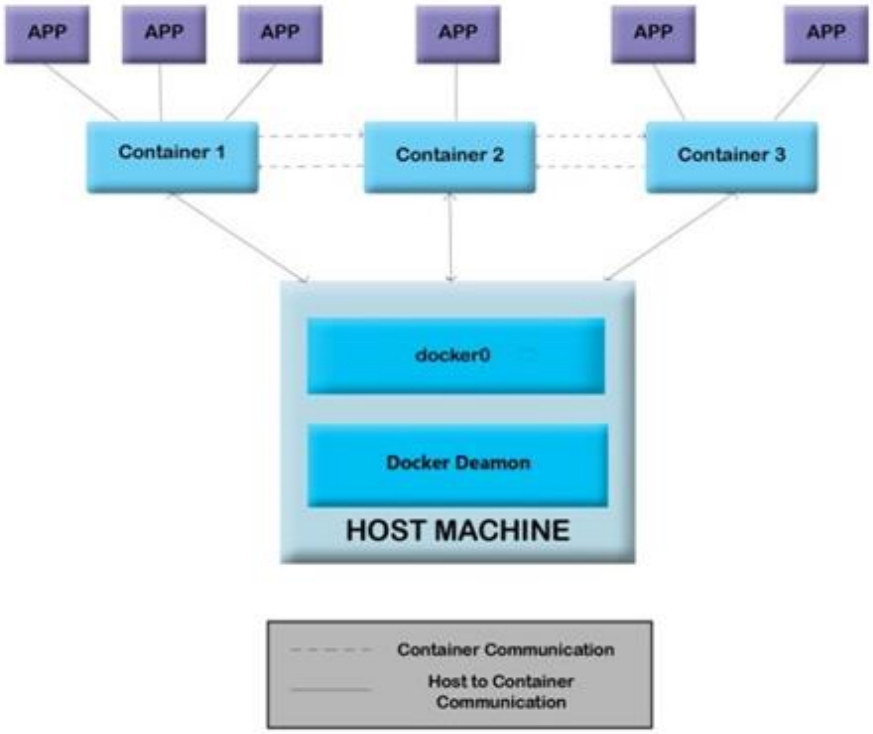


FIGURA 4 Arquitectura de docker [13]

Para su buen funcionamiento Docker consta de su propia arquitectura la cual permite correr varios contenedores con diferentes aplicaciones como se observa en FIGURA 4 *Arquitectura de docker [13]*.

El contenedor de Docker es similar a un directorio. Contiene todo lo necesario para que se ejecute una aplicación. Los contenedores se crean a partir de imágenes de Docker. Un contenedor se puede ejecutar, iniciar, detener, mover y eliminar.

Las imágenes de Docker son plantillas de solo lectura que se usan para crear contenedores de Docker. Por ejemplo, una imagen puede contener un sistema operativo Ubuntu 12.10 con Apache y otras aplicaciones web instaladas. Docker también permite crear nuevas imágenes y también se pueden usar imágenes ya creadas.

La diferencia de Docker con una máquina virtual es que cuando virtualizas un maquina tienes que guardar un sistema operativo para cada máquina esto consume muchos recursos de la máquina, por otro lado con la utilización de Docker no pasa esto ya que comparte el sistema operativo del host por independizado [16].

2.2. Antecedentes

Para complementar esta investigación se revisaron diferentes estudios, los cuales también se enfocaron en el método de encriptación, así como también el protocolo a implementar, con ello también analizaron el nivel de privacidad y seguridad conseguido al final.

Un primer trabajo corresponde a Italo Dacosta, Andreas Put y Bart De Decker, en su investigación "emailcloak: un enfoque práctico y flexible para mejorar la privacidad del correo electrónico" [8], se diseñó emailcloak un servidor de alias de correo electrónico que implementó openpgp de forma automática, usando como base los requisitos de cifrado extremo a extremo, este servidor le da al usuario más control sobre el almacenamiento de datos en el correo electrónico para poder defenderse de amenazas de nivel inferior pero todavía plausibles, también proporciona un nivel de privacidad bastante fuerte, aún mayor que las que ofrece el cifrado estándar de openpgp. No obstante, emailcloak no podrá proteger a los usuarios de adversarios poderosos (gobiernos), es una tarea difícil y solo los podrá proteger parcialmente de estos enemigos y brinda una seguridad superficial.

Por otro lado Alexander Yakubou, Wazen M. Shbair, Radu realizaron un estudio llamado Block pgp: Un marco basado en Blockchain para servidores clave pgp [17] teniendo énfasis esta investigación en un nuevo marco de gestión pgp con la infraestructura de servidor clave, implementado mediante la tecnología Blockchain, donde diseñaron y se desarrollaron un prototipo para la implementación de servidores claves en blockchain Ethereum con permiso develope. La cual tuvo como resultados que blockchain resuelve el riesgo medio para los servidores clave, acelera la sincronización entre servidores clave a varios minutos, proporciona un historial completo de los estados de un servidor clave en función de su funcionalidad integra.

Mientras un estudio de caso hecho en Estados Unido por Kadapia en el año 2017 con el nombre "Un caso (Estudio) para la usabilidad en la comunicación segura por correo electrónico" [18]. Esta investigación se basa en la usabilidad y la relevancia práctica de los mecanismos de seguridad estándar para la comunicación por correo electrónico, el trabajo se centró en las técnicas de criptografía de clave pública disponibles para firmar y cifrar digitalmente el correo electrónico. Se eligió extensiones seguras, multipropósitos de correo, un estándar para firmar y cifrar correos electrónicos populares como Apple Mail, Outlook Express, y Thunderbird de Mozilla, donde se descubrió que la privacidad bastante buena (pgp) y la guardia de privacidad GNU (GPS) eran inutilizables con corresponsales no técnicos porque les exigía instalar software adicional.

Sin embargo en el año de 2017 A. Barenghi en [4]. Clasifican el formato Openpgp como un lenguaje determinista libre de contexto según la jerarquía Chomsky. Luego, se centran en analizar el formato, demostrando que, incluso si existe una gramática determinista libre de contexto capaz de generar el formato, tal gramática tiene una cantidad inmanejable de producciones. Además, identificamos algunos defectos de diseño en la especificación estándar Openpgp del formato, describiendo posibles ataques que pueden explotarlos. Estos ataques se evalúan contra las dos implementaciones principales de Openpgp (es decir, GnuPG y pgp de Symantec), lo que demuestra que ambos resultan no ser vulnerables debido a las opciones conservadoras de los desarrolladores al tratar con los datos de entrada.

Además Moin A. Khorajiya y M.E Schola desarrollaron un estudio en el año 2016 con el título “Arquitectura basada en seguridad que utiliza Kerberos y pgp” [19] donde proponen un modelo de seguridad de datos, que incluye dos metodologías Kerberos y pgp, la cual se implementó un modelo y se consideró los factores tanto para el sistema existente como para el mejorado, teniendo como objetivo analizar los factores y observar que el sistema mejorado es beneficioso sobre el existente en el aspecto de seguridad y autenticación del usuario. Para obtener los resultados se compararon cuatros factores mejorados en el diseño propuesto, el cual se encargó de la seguridad mediante una firma digital, en el cual nadie pueda realizar un ataque y obtener la información , en cuanto a la privacidad del usuario se autorizó enviar una firma para que la información personal no sea adquirida por una persona que no esté autorizada y el usuario pueda ser identificado con Kerbeos, así un usuario válido pueda acceder a los servicios de confianza y por último la autenticación segura se encargará de enviar una firma de manera digital por lo que proporciona una mejor seguridad.

2.3. Bases legales

Dentro de las bases legales que deben tomarse en cuenta para la presente investigación, se estipulan las siguientes leyes inscritas en la constitución de la República del Ecuador: Ley de Propiedad Intelectual [20], Ley de defensa y Protección del Consumidor [21], Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos [21].

La ley de propiedad intelectual en el artículo 322 del código integral penal, menciona qué, Se reconoce la participación intelectual de acuerdo con las circunstancias que señale la ley. Se impide toda forma de apropiación de conocimientos colectivos, en el ámbito de las ciencias, tecnologías y saberes ancestrales. Con el presente proyecto se busca resguardar la información que se maneje dentro de los correos electrónicos ya que en estos correos muchas veces se envía información de proyectos en elaboración la cual necesita ser privada y no divulgada[20].

También se considera importante tomar en cuenta la Ley de defensa y protección del consumidor la cual en el artículo 71, 75 constituye qué, Las empresas, instituciones

y organismos que presten servicios públicos deberán incorporar sistemas de control de satisfacción de los usuarios y consumidoras, y poner en práctica sistemas de vigilancia y reparación. En este proyecto se establecerá un mecanismo para saber qué tan satisfechos están los clientes con el servicio del servidor de correos, con el fin de mejorar constantemente y los clientes estén contentos con el servicio, también para poder prestar una atención oportuna cuando ocurra cualquier incidente que impida el buen funcionamiento del sistema[20].

En la ley de comercio electrónico, firmas electrónicas y mensajes de datos, en su artículo 7 del código integral penal establece qué, - La verificación de la concordancia entre el emisor del mensaje de datos y su firma electrónica se realizará comprobando la vigencia y los datos del certificado de firma electrónica que la respalda. En otros tipos de firmas o métodos de identificación y autenticación, esta comprobación se realizará mediante la confirmación de los registros acordados o requeridos. Uno de los objetivos de esta investigación es que las personas puedan identificar el emisor de los mensajes mediante las firmas electrónica y el sistema interno de correo electrónico el cual permitiría esta doble identificación haciendo el sistema más seguro y confiable [21].

3. Metodología

3.1. Delimitación de la investigación

La investigación “Interoperabilidad de mensajes protegidos con criptografía utilizando el protocolo pgp”, se realizó en la empresa Zamarino S.A. de la ciudad de Esmeraldas. Sin embargo, a pesar de ser aplicada en esta empresa puede ser aplicada en cualquier otra empresa. La propuesta de la investigación está enmarcada desde el año 2015 al 2020, considerando todos los estudios realizados en este periodo para desarrollar la investigación.

Por otro lado, esta investigación se realizó en el segundo semestre del año 2020 debido a que se necesitó tiempo para preparar las herramientas, contratar los proveedores en los cuales se realizó la práctica y todos los requerimientos necesarios para obtener los resultados adecuados que se presentaron en la investigación.

3.2. Tipos de investigación

Por el nivel de profundidad este estudio es de tipo explicativo debido a que busca el porqué de los hechos, estableciendo relaciones causa-efecto de la seguridad de los datos en el servidor de correo electrónico.

Por otro lado, de acuerdo con la naturaleza de los datos y la información, ésta es una investigación cualitativa por cuanto está encaminado al análisis e interpretación de la información obtenida en el proceso de encriptación de los correos electrónicos, así como también en el proceso de desencriptación de los mensajes. También es cuantitativa ya que analizó los datos estadísticos de los mensajes encriptados, tiempos de ejecución, efectividad al momento de desplegar y entre otros aspectos es decir información que se puede medir. Por lo antes expresado se puede decir que es una investigación hibrida.

Por último, de acuerdo con los medios para obtener los datos ésta es una investigación de campo lo que significa que todas las variables e información recolectadas fueron del servidor de correo electrónico para su posterior análisis.

3.3. Métodos

Los métodos usados en esta investigación fueron inductivo y deductivo. Deductivo porque al implementar los protocolos de encriptación siguiendo todos los pasos respectivos, la seguridad del servidor aumente considerablemente. Inductivo porque según los datos obtenidos en el proceso se midió el nivel de seguridad que va adquiriendo el servidor de correo, también se obtuvo el nivel de satisfacción que tienen los usuarios con las nuevas implementaciones.

3.4. Población y Muestra

La Empresa Zamarino S. A tiene una población de 10 trabajadores por lo cual se tomó la totalidad de trabajadores como muestra debido a que la población es muy pequeña, usando de manera activa sus correos electrónicos.

3.5. Variables de la investigación

Para la elaboración de la tabla se tomó en cuenta como entidades a los beneficiarios del sistema que se llamarón (personas), también los servicios que en este caso será el servidor de correo electrónico. Se usaron estas dos entidades porque se consideran que son las más importantes y que toman un papel protagónico en la investigación, se verá cómo están evaluados estas dos entidades en la Tabla 1 **Variable e indicadores sujetos a estudio**.

Tabla 1 Variable e indicadores sujetos a estudio

VARIABLE	INDICADORES	TIPO DE VARIABLE	ENTIDADES
Calidad de información	* Mensajes enviados * Mensajes recibidos * Mensajes Perdidos	Cuantitativa	Personas Servicios
Usabilidad	* Eficiencia * Efectividad * Satisfacción	Cualitativa	Personas Servicios
Rendimiento	* Disponibilidad * Tiempo de respuesta	Cuantitativa	Servicios
Seguridad	* Identificación de los usuarios * Manejo de los mensajes	Cualitativa	Personas Servicios
Comunicación	* Encriptación * Número de incidentes de seguridad * Costo por incidentes de seguridad	Cuantitativas	Servicios Personas

Las variables listadas en la

Tabla 1 **Variable e indicadores sujetos a estudio**, son descritas a continuación al igual que sus respectivos indicadores:

Variable 1 - Calidad de información. Nivel de calidad de los datos manejados en el sistema. Entre el emisor de los mensajes y el receptor. A quien le voy a aplicar esta variable.

- **Mensajes enviados**. Mensajes que envía una persona a un destinatario desde su cuenta de correo.
- **Mensajes recibidos.** Mensajes que recepta una persona en su cuenta de correo
- **Mensajes Perdidos.** Mensajes que no llegan al receptor por diferentes situaciones, como error en la escritura del correo.

Variable 2 - Usabilidad. La facilidad que tiene el usuario para manejar el sistema de correo y encontrar lo que necesita

- **Eficiencia.** Capacidad del sistema de correo para cumplir cada un de las funciones encargadas
- **Efectividad.** Capacidad de concluir cada una de sus funciones.
- **Satisfacción.** Capacidad del sistema de correo para cubrir todas las necesidades del usuario

Variable 3 - Rendimiento. Nivel de utilidad de los servicios que presta el sistema de correo para el usuario.

- **Disponibilidad.** Tiempo que el sistema de correo está apto para el uso de los usuarios.
- **Tiempo de respuesta.** Cantidad de tiempo que el sistema demora en responder las solicitudes del usuario.

Variable 4 - Seguridad. Efectividad que tiene el sistema en la protección de la información guardada en el sistema de correo.

- **Identificación de los usuarios.** Manejo de la identificación del usuario para el ingreso al sistema de correo y el manejo de la firma electrónica personal.

- **Manejo de los mensajes.** Forma en que el sistema procesa los mensajes para que sea entregado al receptor sin atentar con la integridad de la información.

Variable 5 - Comunicación. Nivel de calidad del servicio utilizada para verificar los fallos en los diferentes procesos como la encriptación los mensajes u otros procesos.

- **Costo por incidentes de seguridad.** Que tanto afecta el incidente puede ser perdida de información o diversas situaciones.
- **Encriptación.** Forma que los mensajes son protegidos para el envío.
- **Número de incidentes de seguridad.** Cantidad de incidentes que se presentas en el sistema.

3.6. Técnicas e instrumentos de recolección de datos

Esta investigación fue de tipo experimental porque se va a crear un servidor de correo electrónico para demostrar la efectividad del protocolo de pgp en la encriptación de mensajes con servidor de correos.

Para llevar a cabo el experimento de esta investigación también se implementó un instrumento muy importante. Diseño del experimento, es el diseño de un servidor de correo electrónico mediante el protocolo de encriptación pgp, estuvo acompañado de unas pruebas de vulnerabilidad al servidor, se realizó con el fin de saber que problemas han tenido con el servidor actual. Los resultados de la prueba se pueden observar en ANEXO 6 *resultados de ataque*.

3.7. Técnicas de procesamiento y análisis de datos

Para esta investigación se tomaron en cuenta algunas técnicas para procesar y analizar los datos las cuales se han marcado con un "si" en la Tabla 2 **Técnicas de análisis de datos**que se muestra a continuación.

Tabla 2 Técnicas de análisis de datos

Simulación de Monte Carlos	**No**
Análisis de patentes y literatura científica	No
Experimentos A/B	No

Análisis de escenario	Si
Análisis de correlación	No
Predicción matemática	No
Análisis basado en estadística descriptiva	Si
Visualización de datos	Si

Se toma en cuenta el análisis de escenario porque es necesario saber cómo reaccionaron cada una de las variables al cambio, que pasaría si los usuarios no firman los mensajes de correos electrónicos , así mismo también el análisis basado en estadística descriptiva debido a que esta permite saber cuándo una variable no está funcionando como debería funcionar y obtener opinión de los usuarios, la visualización de datos permitió obtener una gráfica del comportamiento de cada una de las variables para poder llevar un control del funcionamiento de las mismas.

3.8. Normas éticas

Esta investigación se sostuvo en normativas éticas las cuales van de acuerdo con los lineamientos y reglamento de grados de la PUCESE, como se ha indicado en el apartado de normativas legales se respeta el trabajo de cada uno de los autores que se han nombrado en esta investigación, dándole el reconocimiento que se merecen por las ideas y conceptos que se utilizan en esta investigación. Las herramientas que se utilizaron en esta investigación son de acceso libre y se respeta los términos y las condiciones que traen consigo las licencias del software que se usa.

4. Resultados

4.1. Análisis y resultados

Para la creacion del prototipo del servidor de correo electrónico se necesitó un servidor, en este caso se uso de google cloud platform, la cual permitió crear un servidor con isstema operativo ubuntu 18.04. con 2 CPU virtuales y una memoria de 4gb, con un disco duro de 10 gb como se explica en la FIGURA 5 *Características de la máquina virtual fuente: elaboración propia*.

Imagen	Tamaño (GB)	Nombre del dispositivo	Tipo	Encriptación	Modo
ubuntu-1804-bionic-v20201211a	10	tecnobitsfm	Disco persistente estándar	Administrada por Google	Arranque, lectura/escritura

FIGURA 5 Características de la máquina virtual fuente: elaboración propia

Acto seguido se instaló dokcer y dokcer compose para poder correr el contenedor con el servidor de correo electronico usando los siguinetes comandos:

Actualización del sistema:

```
sudo apt update
sudo apt upgrade
```

Instalación de paquetes de requisitos previos para la instalacion de docker:

```
sudo apt-get install  curl apt-transport-https ca-certificates software-properties-common
```

Para entender lo que se instala en el comando anterio la parte. El paquete apt-transport-https: consiente que la guia de paquetes transporte datos por medio de https. El paquete ca-certificates: permite a su navegador web y que el sistema comprueben los certificados de seguridad. La transferencia de datos se hace por medio de l paquete curl. Por otro lado el paquete software-properties-common: agrega scripts para dirigir el software.

Luego de instalar las dependencias se agrega el repositorio de docker el cual será necesario para poder usar el procedimiento de instalacion compatible, primero se añade la clave pgp del repositorio:

```
curl -fsSL https://download.docker.com/linux/ubuntu/gpg | sudo apt-key add -
```

A continuacion se agrega el repositorio:

```
sudo add-apt-repository "deb [arch=amd64] https://download.docker.com/linux/ubuntu $(lsb_release -cs) stable"
```

Se actualiza la máquina para que se actualice el repositorio

```
sudo apt update
```

Para verificar si se está instalando desde el repositorio de docker se escribe el siguiente comando:

```
apt-cache policy docker-ce
```

una salido correcta para este comando seria:

```
docker-ce:
  Installed: (none)
  Candidate: 16.04.1~ce~4-0~ubuntu
  Version table:
     16.04.1~ce~4-0~ubuntu 500
        500
https://download.docker.com/linux/ubuntubionic/stableamd64packages
```

Ahora solo queda instalar docker con el siguiente comando:

```
sudo apt install docker-ce
```

Para comprobar si la instalación se hizo de forma correcta se comprueba con el siguiente comando que va a permitir ver el estado de docker

```
sudo systemctl status docker
```

Acto seguido se descarga la versión estable de docker compose con el siguiente comando:

```
sudo curl -L "https://github.com/docker/compose/releases/download/1.28.2/docker-compose-$(uname -s)-$(uname -m)" -o /usr/local/bin/docker-compose
```

Luego se otorgan permisos al docker compose:

```
sudo chmod +x /usr/local/bin/docker-compose
```

A continuación, se comprueba la correcta instalación de docker compose con el siguiente comando:

```
docker-compose --version
```

una salido correcta para esto seria:

docker-compose version 1.28.2, build 1110ad01

Se ingresa como super usuario con el comando “sudo su”, luego se crea una carpeta en este caso se creó una carpeta llamada “poste” donde se almacenará el archivo “dokcer-compose.yml”. Dentro de este archivo se va a especificar la imagen con la que se va a trabajar, el “restart always” es para que se reinicien los servicios cada vez que se reinicie la imagen, se especifica los puertos que se van a abrir y va a usar el servidor de correos. Se crea también un volumen el cual se va a tener guardado en caso de que se requiera borrar la maquina la información no se pierda y se pueda recuperar se activa el https para poder instalar “Let's encrypt service” a continuación se describe el código

```
sudo su

mkdir poste

apt-get install nano

nano dokcer-compose.yml

dentro de este documento escribimos lo siguiente:

version: "3.4"

services:

  poste:

    image: analogic/poste.io

    restart: always

    network_mode: "host"

    expose:

      - 25

      - 80

      - 443

      - 110

      - 143
```

```
  - 465
  - 587
  - 993
  - 995
  - 4190
volumes:
  - /mnt/mail:/data
environment:
  - HTTPS=ON
  - DISABLE_CLAMAV=TRUE
```

Para correr el archivo creado se debe ingresar a la carpeta creada “poste” y se corre el siguiente comando:

```
docker-compose up -d
```

Este comando reconoce automáticamente el archivo “. yml” y lo correrá, se empezará a descargar la imagen e instalar cada uno de los archivos necesarios.

Luego de la instalación de poste.io se debe configurar en el servidor de dominios en este caso se usó “GoodDaddy” aquí se van a agregar varios registros como se describe en FIGURA 6 *Registros primera parte Fuente: elaboración propia*.

Tipo	Nombre	Valor	TTL	
A	@	34.122.96.239	1 hora	
CNAME	tecnobitsfm.com	@	1 hora	
MX	@	@ (Prioridad: 10)	1 hora	

FIGURA 6 Registros primera parte Fuente: elaboración propia

En el registro tipo A se asigna que cuando se dice @ será igual que decir “34.122.96.239”. El registro CNAME es un registro de nombre canónico es un prototipo de registro de recurso en el sistema de nombres de dominio que permite

hacer esto es que cuando se escriba en el buscador “tecnobitdfm.com” se dirige a la ip asignada en @.

El registro MX es un recurso DNS que detalla cómo debe ser orientado un correo electrónico en internet. Los registros MX registran a los servidores a los cuales envían un correo electrónico.

También se tiene que agregar el registro DKIM como se muestra en FIGURA 7 *Registro DKIM Fuente: elaboración propia* lo cual permite que el servidor receptor sepa que el mensaje recibido es de un dominio ya ha sido autorizado por ese dominio

FIGURA 7 Registro DKIM Fuente: elaboración propia

Este servidor de correo usará un servidor SMTP externo en este caso se usó Mailgun, es un servicio de correo electrónico de terceros que brinda a los usuarios de Compute Engine hasta 10,000 mensajes de correo electrónico gratis por mes. Mailgun además ofrece una API programática, la retención de registros, la personalización del correo electrónico, estadísticas, validación de correo electrónico y otras opciones [23].

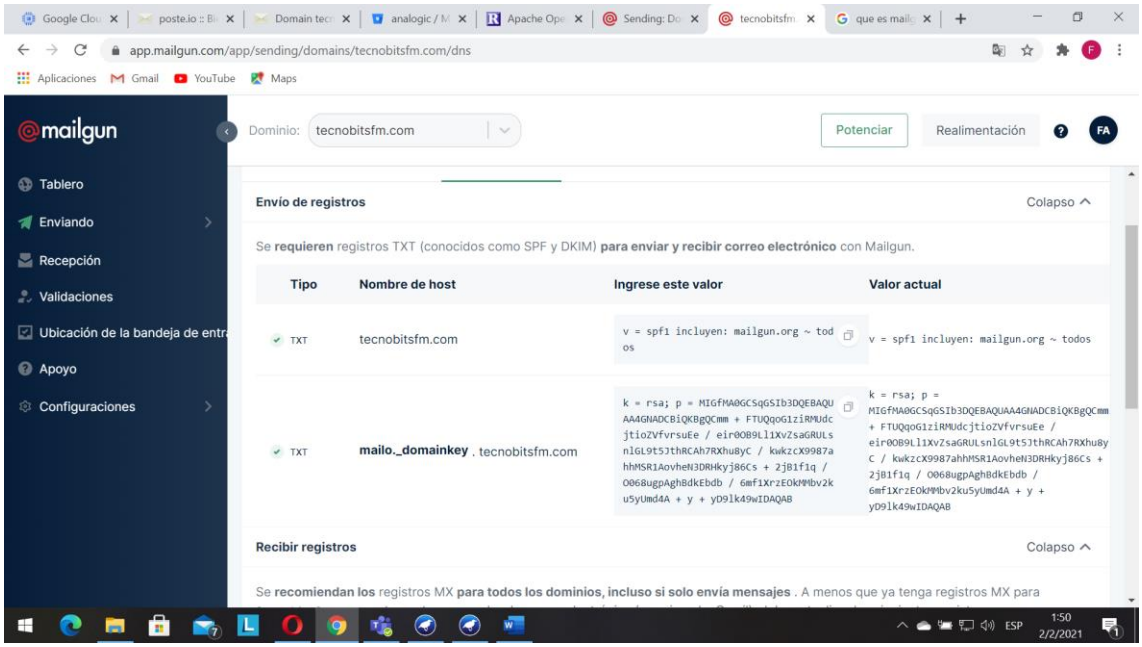


FIGURA 8 Registros de servidor SMTP Fuente: elaboración propia

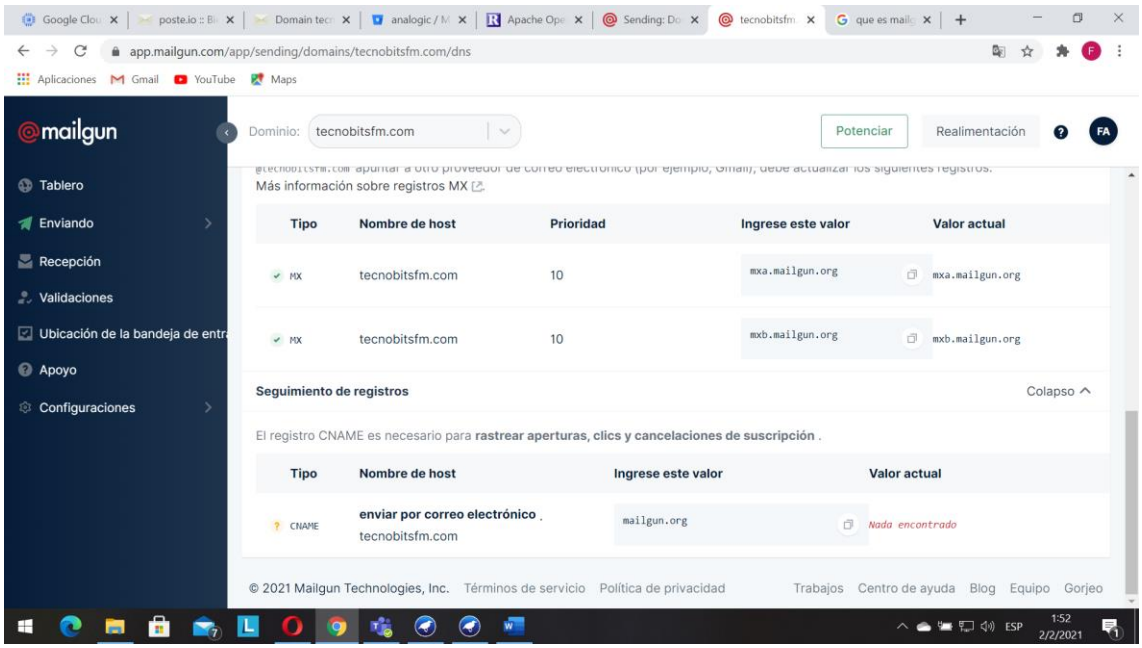


FIGURA 9 Registros SMTP 2 Fuente: elaboración propia

Para vincular el servidor SMTP al dominio se deben agregar algunos registros como lo muestra en FIGURA 8 *Registros de servidor SMTP Fuente: elaboración propia* y en FIGURA 9 *Registros SMTP 2 Fuente: elaboración propia* **¡Error! No se encuentra el origen de la referencia.** estos registros deben ser agregados en el dominio permitirán redirigir el tráfico al servidor SMTP.

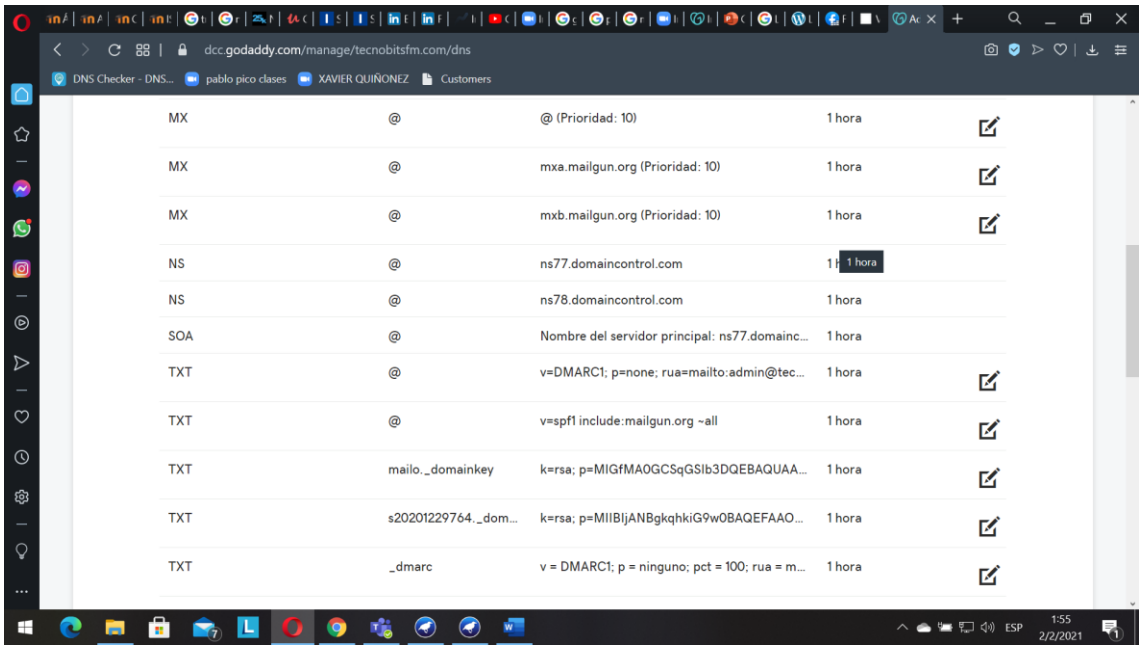


FIGURA 10 Registros agregados Fuente: elaboración propia

Una vez agregados los registros se puede observar que ya funciona el envío de mensajes a otros servidores de correo electrónico como Gmail, Outlook, Hotmail, etc. Ahora el tema principal es como se integran las claves pgp para encriptar los correos electrónicos en este caso se proceden a crear las claves en cada usuario como

en la FIGURA 10 *Registros agregados Fuente: elaboración propia* ese proceso lo hace para cada usuario.

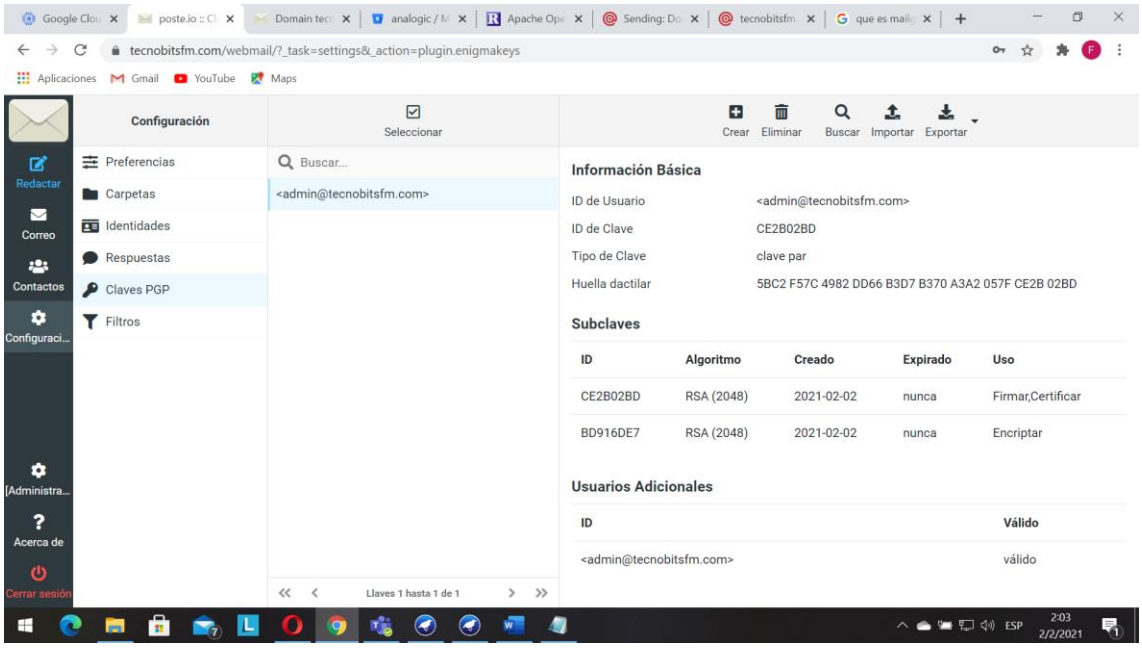


FIGURA 11 Claves pgp Fuente: elaboración propia

Ahora para encriptar un mensaje es super sencillo en la FIGURA 11 *Claves pgp Fuente: elaboración propia*se observa cómo se encripta se adjunta la clave pública para que el receptor pueda guardar esta clave y pueda responder al usuario en un mismo mensaje encriptado, se firma digitalmente el mensaje para que el receptor sepa con seguridad quien es el que está enviando el mensaje como se muestra en la FIGURA 12 *Encriptar mensaje Fuente: elaboración propia*.

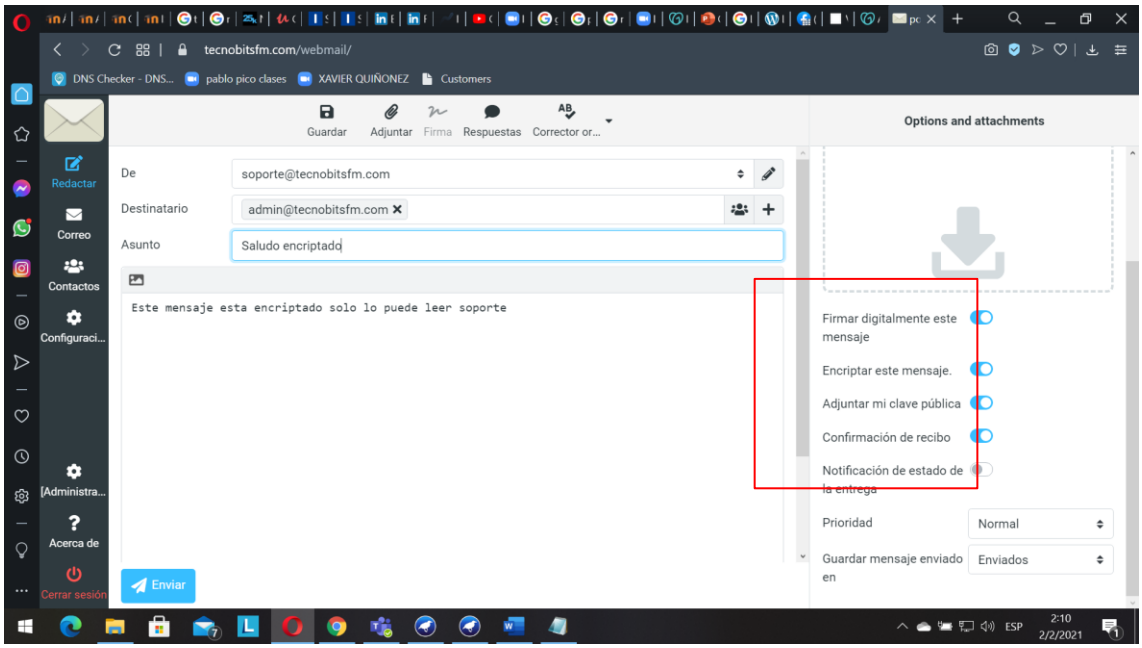


FIGURA 12 Encriptar mensaje Fuente: elaboración propia

También se tiene que importar las claves del receptor para poder enviar el mensaje como se muestra en la FIGURA 12 Encriptar mensaje Fuente: elaboración propia

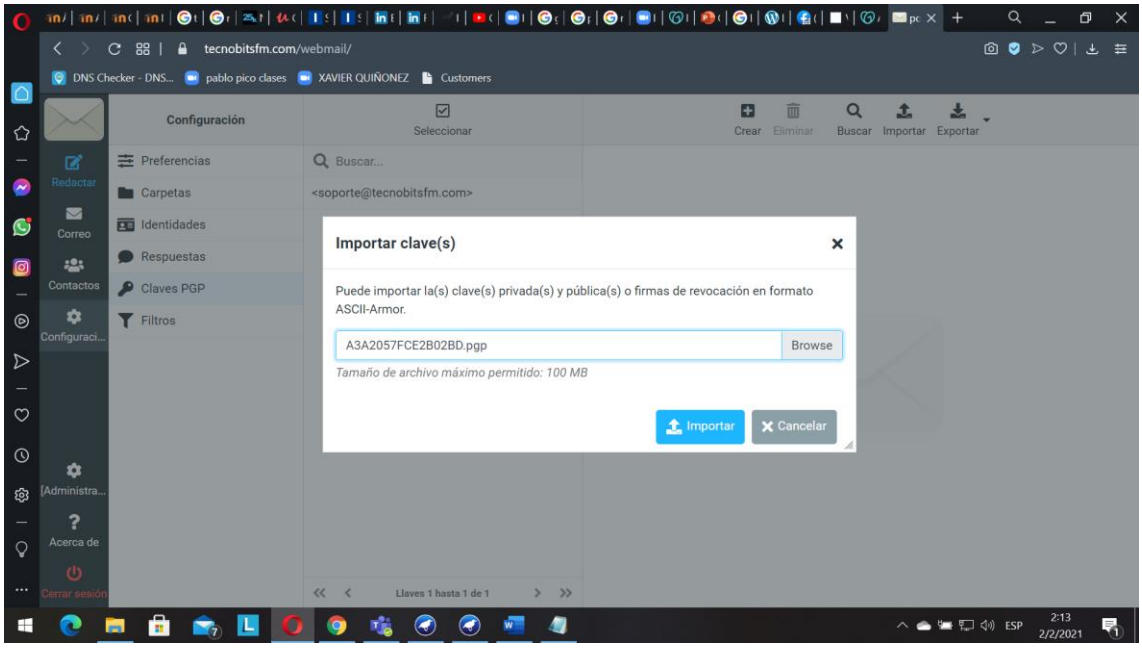


FIGURA 13 Importar claves públicas del receptor fuente: elaboración propia

Cuando se va a enviar el mensaje es necesario anotar la contraseña de la clave pgp como se muestra en FIGURA 14 *Contraseña de mensaje encriptado Fuente: elaboración propia*

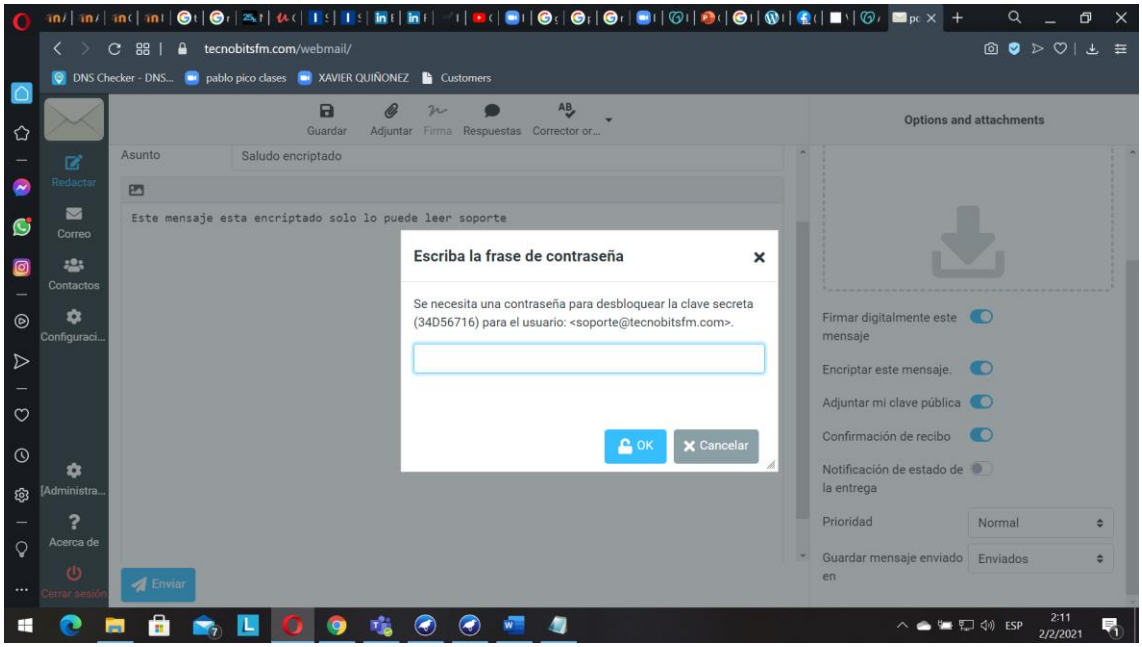


FIGURA 14 Contraseña de mensaje encriptado Fuente: elaboración propia

Cuando el mensaje llega al receptor en este caso admin@tecnobitdsfm.com, va a pedir que escriba la contraseña de su clave pública para poder revelar el mensaje como se muestra en FIGURA 15 *Receptando mensaje encriptado Fuente: elaboración propia*

¡Error! No se encuentra el origen de la referencia.

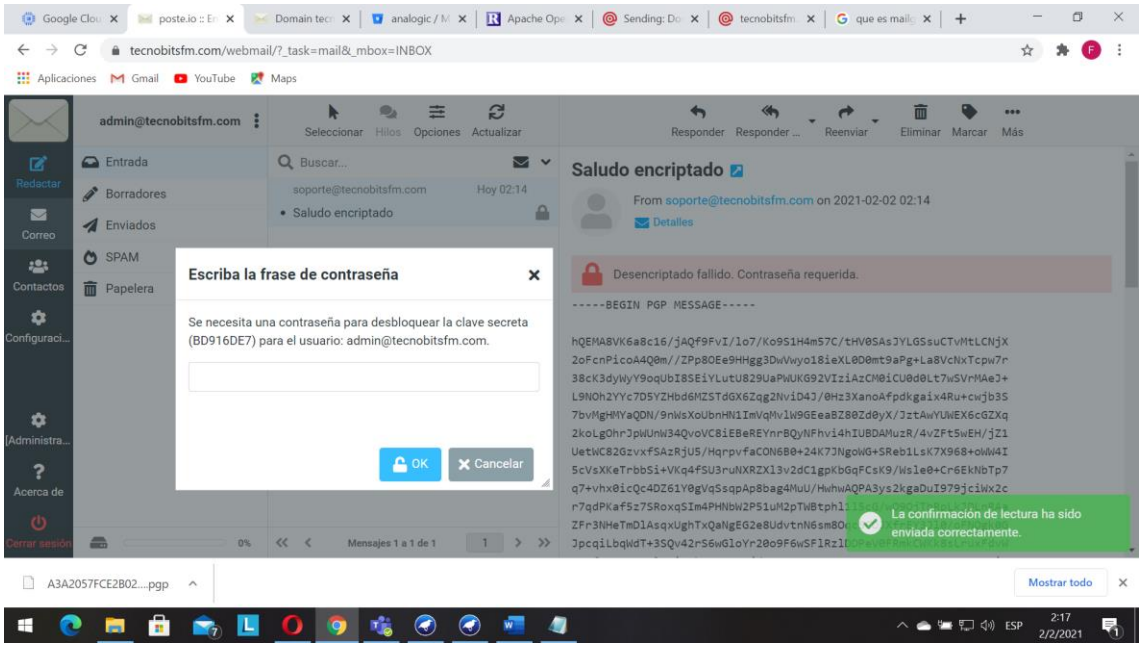


FIGURA 15 Receptando mensaje encriptado Fuente: elaboración propia

Ahora una vez colocada la contraseña de la clave pgp de admin se podrá ver el contenido del mensaje como se muestra en FIGURA 16 *Revelación de contenido Fuente: elaboración propia*

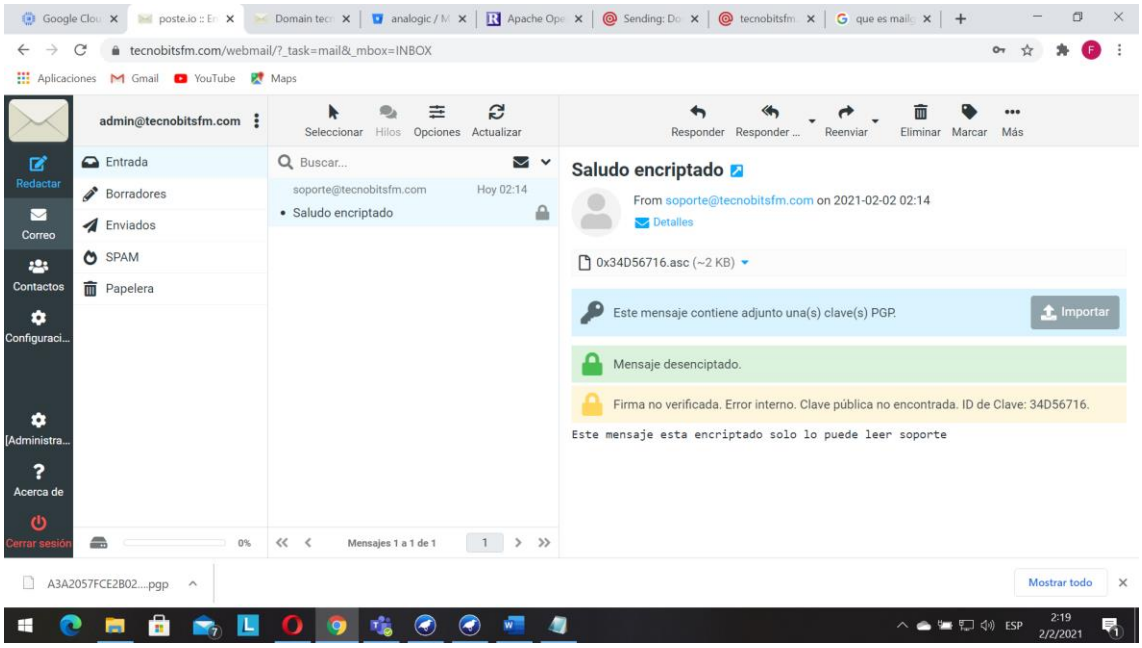


FIGURA 16 Revelación de contenido Fuente: elaboración propia

Recordemos que también pedimos al sistema que nos notifique cuando el mensaje sea leído pues el sistema nos responderá una vez el mensaje sea abierto como se muestra en FIGURA 17 *Confirmación de mensaje Fuente: elaboración propia* **¡Error! No se encuentra el origen de la referencia.**

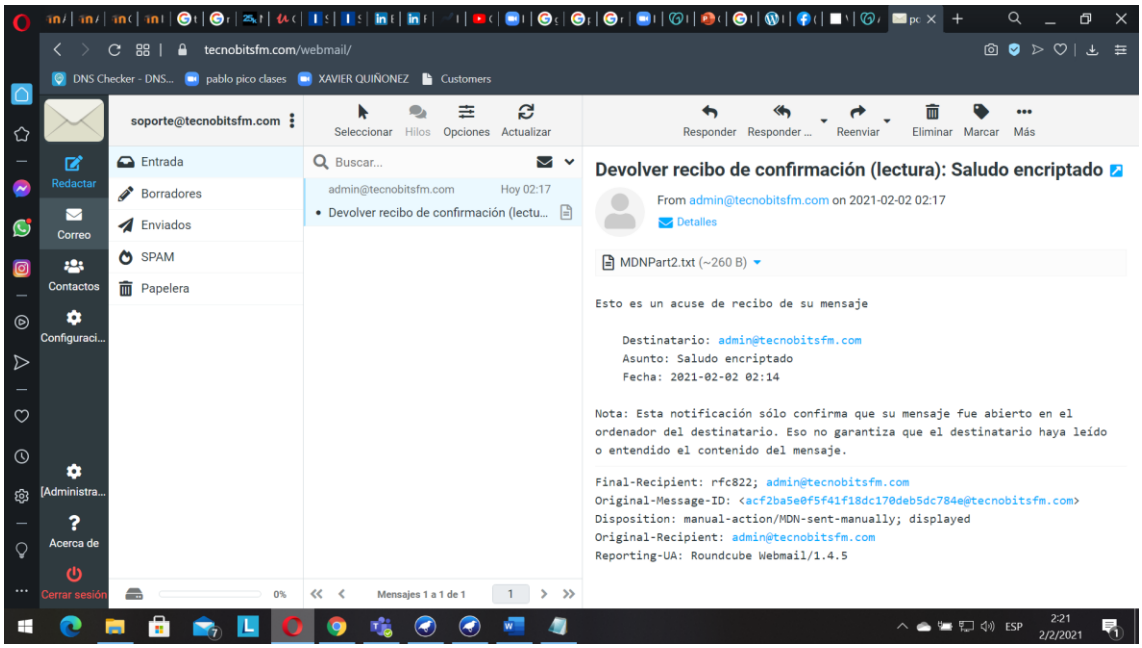


FIGURA 17 Confirmación de mensaje Fuente: elaboración propia

4.2. Nivel de seguridad

Para medir el nivel de seguridad del servidor de correo se usó el plan de seguridad de aplicaciones web abiertas por sus siglas en inglés (*OWASP*), es una institución sin fines de ganancia que trabaja para renovar la seguridad del software. A través de proyectos de software de código abierto liderados por la comunidad, cientos de capítulos locales en todo el mundo, decenas de miles de miembros y conferencias educativas y de capacitaciones de líderes, la Fundación OWASP es la fuente para que los desarrolladores y tecnólogos protejan la web [24].

Owasp presenta sus 10 controles proactivos principales los cuales ayudaran a estar prevenidos en estos tipos de ataques que son los más comunes los cuales son:

Inyección SQL. Esta falla ocurre normalmente cunado se envían datos que son de confianza al interprete como parte de un comando, esto puede ocasionar que el intérprete ejecute acciones no deseadas y perjudiciales para el servidor [25].

Autenticación rota. Los atacantes aprovechan cualquier falla de implementación de las aplicaciones encargadas de gestionar contraseñas, claves o tokens de inicio de sesión, cuando esto ocurre y los atacantes logran hacerse con las sesiones de otros

usuarios el sistema se ve vulnerado ya que pueden tener acceso a información para la que no están autorizados [25].

Exhibición de datos sensibles. Varias aplicaciones web y API no resguardan apropiadamente los datos personales, como los financieros, de salud y PII [25].

Entidades externas XML (XXE). Estas entidades pueden ser objetivo de ataques ya que pueden ser usadas de distintas maneras con el fin de hacer daño a los usuarios entre ellas cosas como divulgación de información mediante el controlador URI de archivos, escaneo de puertos internos, negación de servicio entre otros ataques más que pueden dañar mucho la integridad del servidor [25].

Control de acceso roto. El control de roles dentro de servidor es una parte importante y aplicarla de manera correcta trae muchas ventajas de lo contrario puede ser víctima de un robo de información ya que los usuarios tendrían acceso a información prohibida [25].

Mala conformación de seguridad. En esta parte hace referencia a los servidores que suelen tener configuración de seguridad predeterminada inseguras, el almacenamiento en la nube poco seguro también es un factor que hay que cuidar al igual que los mensajes de error donde se suele mostrar información confidencial que se debe mostrar [25].

Secuencias de comandos entre sitios (XSS). Es deber de los usuarios tomar medidas de seguridad en cuanto al ingreso de información se refiere esto puede ocasionar graves problemas, cuando se ingresa información personal en páginas sin certificación XSS permite a los atacantes ejecutar códigos con los que pueden hasta secuestrar las sesiones d ellos usuarios [25].

Deserialización insegura. La desacralización incierta a menudo lleva a la elaboración remota de código. Incluso si las fallas de deserialización no dan como consecuencia el cumplimiento remoto de código, se pueden usar para realizar ataques, incluidos ataques de reproducción, ataques de inyección y agresiones de escalada de privilegios [25].

Uso de dispositivos con debilidades conocidas. Existen varios componentes en las paginas web que son tomados como puntos débiles para los servidores para ello se pueden socavar defensas de las aplicaciones para así poder resistir estos ataques de impacto [25].

Registro y monitoreo insuficientes. La falta de integración junto con la ineficaz repuestas a los incidentes son vulnerabilidades en las organizaciones que permiten a los atacantes actuar a sus anchas en los servidores, la detección de los ataques debe ser inmediata al igual que el actuar del personal a cargo de la seguridad del sistema [25].

Para conocer el factor de riesgo de cada vulnerabilidad se analizarán los siguientes parámetros que se evaluarán:

- Explotación: Es la violación de la seguridad en los sistemas informáticos.
- Prevalencia: Con qué Frecuencia las vulnerabilidades se manifiestan en los sistemas Informáticos.
- Detección: Con qué facilidad son localizadas las vulnerabilidades en los sistemas informáticos.
- Impacto: Que grado de criticidad tiene cada Vulnerabilidad

Tabla 3 Parámetros de evaluación de explotación

Operaciones de Respuesta de Explotación	Valor
Difícil	1
Media	2
Fácil	3

Tabla 4 Parámetros de evaluación de prevalencia

Operaciones de Respuesta de Prevalencia	Valor
Poco Común	1
Común	2
Difundida	3
Muy Difundida	4

Tabla 5 Parámetros de evaluación de detección

Operaciones de Respuesta de Detección	Valor
Difícil	1
Media	2
Fácil	3

Tabla 6 Parámetros de evaluación de vulnerabilidades

Operaciones de Respuesta de Impacto	Valor

Menor	1
Moderado	2
Grave	3

Se valorará cada una de las vulnerabilidades de acuerdo al resultado obtenido por OWASP, para obtener un promedio final el cual ayudará a dar una valoración final dl servidor.

Tabla 7 valoración de la vulnerabilidad de inyección

Inyección		
Explotación	Fácil	3
Prevalencia	Común	2
Detección	Media	2
Impacto	Grave	3

Tabla 8 valoración de la vulnerabilidad de Autenticación remota

Autenticación remota		
Explotación	Media	2
Prevalencia	Difundida	3
Detección	Media	2
Impacto	Grave	3

Tabla 9 valoración de la vulnerabilidad de Exposición de datos sensibles

Exposición de datos sensibles		
Explotación	Media	2
Prevalencia	Muy Difundida	4
Detección	Fácil	3
Impacto	Moderado	2

Tabla 10 valoración de la vulnerabilidad de entidades externas XML

Entidades externas XML		
Explotación	Fácil	3
Prevalencia	Común	2

Detección	Fácil	3
Impacto	Moderado	2

Tabla 11 valoración de la vulnerabilidad de control de acceso remoto

Control de acceso remoto		
Explotación	Fácil	3
Prevalencia	Común	2
Detección	Fácil	3
Impacto	Moderado	2

Tabla 12 valoración de la vulnerabilidad de mala configuración de seguridad

Configuración de seguridad		
Explotación	Difícil	1
Prevalencia	Poco Común	1
Detección	Media	2
Impacto	Grave	3

Tabla 13 valoración de la vulnerabilidad de secuencia de comandos entre sitios

Secuencia de comandos entre sitios		
Explotación	Fácil	3
Prevalencia	Común	2
Detección	Media	2
Impacto	Moderado	2

Tabla 14 valoración de la vulnerabilidad de deserialización insegura

Deserialización insegura		
Explotación	Media	2
Prevalencia	Común	2
Detección	Fácil	3
Impacto	Moderado	2

Tabla 15 valoración de la vulnerabilidad de uso de componentes con vulnerabilidades conocidas

Utilización de Componentes con Vulnerabilidades Conocidas		
Explotación	Media	2
Prevalencia	Difundida	3
Detección	Difícil	1
Impacto	Moderado	2

Tabla 16 registro y monitoreo insuficiente

Registro y monitoreo insuficiente		
Explotación	Media	2
Prevalencia	Poco Común	1
Detección	Fácil	1
Impacto	Moderado	2

RESULTADO DE LA VALORACION DEL TOP 10 DE OWASP

										Resultado Final de las Vulnerabilidades										
Criterios	**A1**		**A2**		**A3**		**A4**		**A5**		**A6**		**A7**		**A8**		**A9**		**A10**	
	Resultado	**Valor**	**Resultado**	**Valor**	**Resultado**	**Valor**	**Resultado**	**Valor**	**Resultado**	**Valor**	**Resultado**	**Valor**	**Resultado**	**Valor**	**Resultado**	**Valor**	**Resultado**	**Valor**	**Resultado**	**Valor**
Explotación	Fácil	3	Media	2	Media	2	Fácil	3	Fácil	3	Difícil	1	Fácil	3	Media	2	Media	2	Media	2
Prevalencia	Común	2	Difundida	3	Muy Difundida	4	Común	2	Común	2	Poco Común	1	Común	2	Común	2	Difundida	3	Poco Común	1
Detección	Media	2	Media	2	Fácil	3	Fácil	3	Fácil	3	Media	2	Media	2	Fácil	3	Difícil	1	Fácil	3
Impacto	Grave	3	Grave	3	Moderado	2	Moderado	2	Moderado	2	Grave	3	Moderado	2	Moderado	2	Moderado	2	Moderado	2
		7		7		6		5,33333333		5,333333333		4		4,66666667		4,66666667		4		4

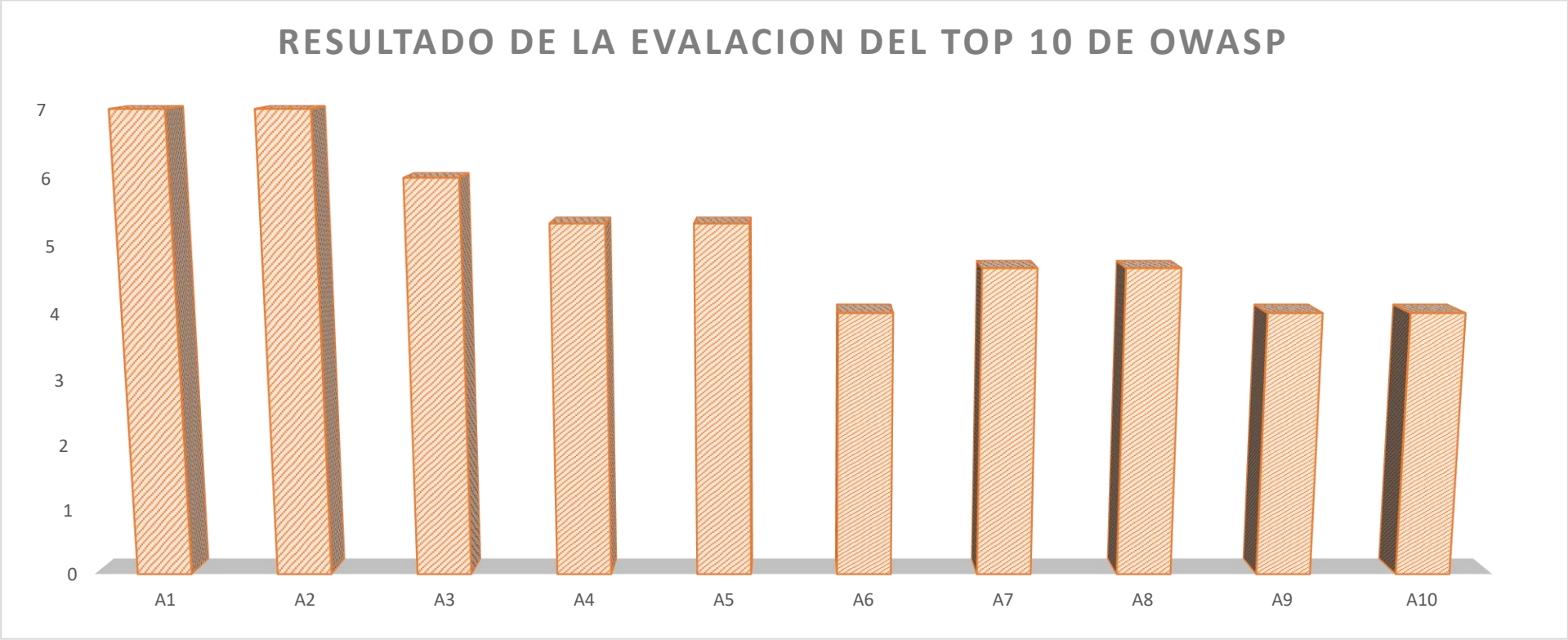


FIGURA 18 Resultado de la evaluación de owasp Fuente: elaboración propia

Según los resultados obtenidos en FIGURA 18 *Resultado de la evaluación de owasp Fuente: elaboración propia* se observa que la inyección sql, autenticación rota, exposición de datos sensibles son las vulnerabilidades más sensibles y de las que se puede esperar un ataque pero esto se puede contrarrestar con la implementación de seguridad en el servidor, para ello en el servidor de han implementado varios métodos que refuerzan esta seguridad como se observa en FIGURA 19 *Inyección de owasp prueba Fuente: elaboración propia* reduciendo a un riesgo bajo la inyección de sql en el servidor.

FIGURA 19 Inyección de owasp prueba Fuente: elaboración propia

De igual manera las otras vulnerabilidades también son contrarrestadas para la seguridad del servidor como se muestra en FIGURA 20 *inicio de sesión roto Fuente: elaboración propia* e FIGURA 21 *exposición de datos sensibles Fuente: elaboración propia*

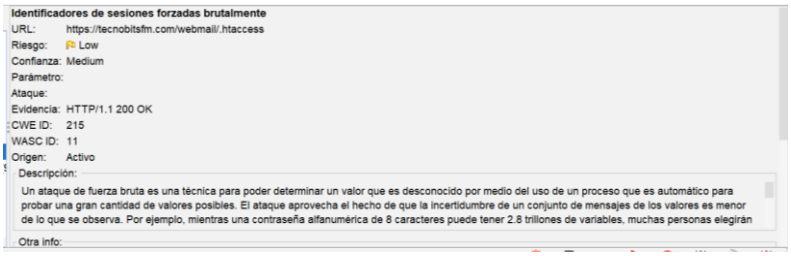


FIGURA 20 inicio de sesión roto Fuente: elaboración propia

FIGURA 21 exposición de datos sensibles Fuente: elaboración propia

Lo antes expuesto deja claro la buena aplicación de la triada CIA [26], la cual pretende mantener confidencialidad, integridad y disponibilidad de los datos. Con estos resultados se puede observar que el servidor cumple con cada una de estas características mantiene la confidencialidad e la información, garantiza la integridad de los datos y estos mismos datos se encuentran disponibles para los usuarios siempre.

7. Discusión

Italo Dacosta en su investigación [8] dice que el cifrado de extremo a extremo que ofrece el protocolo openpgp no brinda una protección máxima para el servidor de correo electrónico, este mismo protege al servidor de ataques pequeños pero si el servidor recibe ataques tales como suplantación de identidad (*spoofing*), tipo pesca (*phishing*). Estos ataques podrían vulnerar la seguridad de estos servidores con openpgp según Dacosta. Pero según la investigación realizada y los resultados obtenidos esta investigación recomienda que los servidores son más seguros si se contratan los servicios desde la nube ya que estos implementan protocolos de seguridad más seguros y ayudan a que la integridad del servidor no sea vulnerada.

Alexander Yakubou y otros en la investigación [17] mencionan que la implementación de blockchain para el manejo de claves públicas y privadas ayuda a que la seguridad del servidor de correo sea más robusta, ya que blockchain asegura la inmutabilidad de la información y elimina la posibilidad de que los usuarios puedan descargar claves corruptas desde el servidor. Pero también la implementación de este servicio puede hacer que el manejo de la información en el servidor sea más pesado debido a su procesamiento por bloques, por otro lado en [27] habla de las implementación de seguridad que ha tenido blockchain nombran dos propuesta muy interesantes una es de IBM y la otra de Oracle ambas explican conceptos en seguridad. IBM proporcionó una visión de la seguridad, incluyendo el negocio, la tecnología, la prestación de servicios y la fusión de dominios tienden a compartir elementos comunes. Oracle propuso una arquitectura de referencia que incluye tres aspectos críticos para lograr la seguridad, a saber, la seguridad de los datos, la prevención del fraude y la habilitación del cumplimiento. Si la implementación de blockchain en la investigación de Yakubou hubiese agregado los aspectos de seguridad y agilidad propuestos por IBM o Oracle, se obtuviera una mejor arquitectura del servidor y permitiría mejores respuestas en menor tiempo.

Por otro lado en [18] hace mención a la importancia de la usabilidad del llavero de claves públicas y privadas, que pasaría si otra persona obtiene su clave privada y puede firmar documentos con mi llave. En la presente investigación se resuelve el problema con la implementación del protocolo openpgp, el cual permite cambiar de llave pública cuando el usuario así lo desee, esto evitará que el usuario reciba spam encriptado con su llave pública y hará que sea más difícil el contacto con el usuario ya que al no tener la llave pública no se podrá encriptar el mensaje. En FIGURA 12 *Encriptar mensaje Fuente: elaboración propia* se observa cómo se encripta el mensaje con la clave pública el usuario, pero en caso de que el receptor cambie de clave publica se hará imposible el envío del mensaje encriptado.

También A. Barenghi aporta una gran investigación en [4] donde explica la importancia de las estructuras al implementar el protocolo openpgp, en este caso se

implementó la arquitectura de Chomsky [28] para clasificar el formato openpgp, como un lenguaje determinista. Este articulo muestra que a pesar de los ataques hechos al servidor ninguno demuestra ser lo suficientemente fuerte como para afectar el funcionamiento del protocolo openpgp, se analizan en dos implementaciones GnuPG y pgp de Symantec, las cuales demostraron tener una seguridad robusta para mitigar estos ataques. En esta investigación se optó por la implementación de Openpgp, gracias a las grandes ventajas que se obtiene al implementarlo. Sobre todo, lo que más se destacó es la mitigación del ataque más común entre los servidores de correo que es *man in the mid*. Este ataque queda obsoleto luego de la implementación de las claves públicas y privadas ya que el mensaje solo puede ser desencriptado por el receptor y también la implementación ayuda a que la información guardada en la nube permanezca encriptada.

8. Conclusiones

1. En esta tesis se desarrolló la interoperabilidad de mensajes de correos electrónicos mediante el uso de criptografía para brindar mayor seguridad y confidencialidad en los datos de los usuarios. Ya qué observando las necesidades del mundo actual se determinó el gran riesgo que tiene la información en los servidores de correo, esta información está siempre en peligro de ser vulnerada y peligra su integridad. Violentando así también la privacidad de los usuarios del correo electrónico.

2. Se analizaron los diferentes protocolos de encriptación como bitmessage, openpgp, S/MIME. Después de este análisis se llegó a la conclusión que, debido a su usabilidad, con referencia al manejo de llaves. En su arquitectura y su robusta seguridad para mitigar ataques el protocolo elegido para este estudio fue el openpgp. Este protocolo también permite que la información almacenada en la nube quede segura ya que se encontraría encriptada y solo el receptor podrá revelar su contenido. La verificación por contraseña ayuda también a que el receptor identifique la verdadera identidad de la persona que está enviando la información, Los ataques realizados en [4] muestra una visión de las ventajas que brinda tener este protocolo en el servidor de correo electrónico

3.También se preparó un prototipo de sistema de correo que implementó el protocolo pgp a través de la herramienta openpgp. La cual permitió encriptar los mensajes brindando así un aumento de seguridad considerable ayudando también a mitigar muchos ataques al servidor de correo. También se descartó la posibilidad del ataque *man in the mid* que generalmente se hacía cuando la información se pasaba del servidor SMTP al receptor. Por otro lado, se pudo valorar el nivel de seguridad del prototipo de correo propuesto. Tomando como referencia el estudio de caso que se implementó en [29][4]. Se implementaron los mismos escenarios para esta

investigación dando como resultado un servidor de correo que mitiga los ataques conservando la integridad de los datos. Las pruebas realizadas por OWASP resaltan la importancia de la seguridad, y lo perjudicial que puede ser para una organización el filtro de la información.

9. Recomendaciones

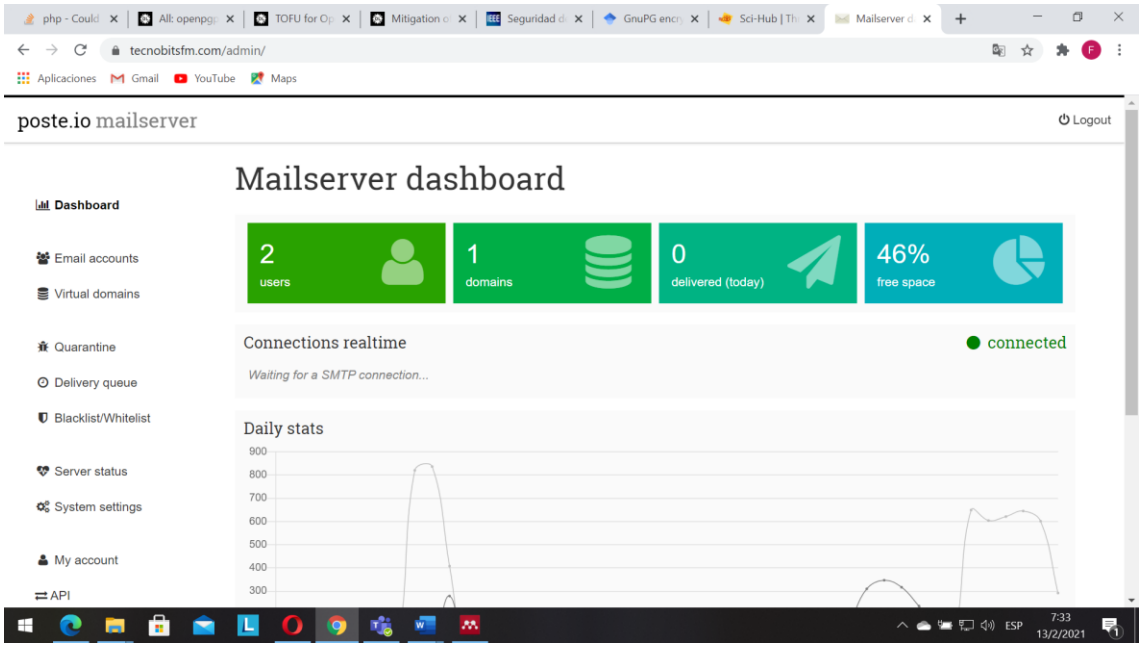
Establecidas las conclusiones de esta tesis se recomienda:

1. Velar por la integridad de la información, implementar de manera continua mejoras al servidor de correo para que la información siempre este protegida y segura en su lugar de almacenamiento, para que los usuarios tengan una mejor experiencia al usar los servidores de correo. Debido a los altos costo de mantenimiento de un servidor se recomienda contratar el servidor de correo como un servicio en una empresa ya constituida, esta a su vez brindará un mejor soporte y dará mejores garantías del servidor de correo.

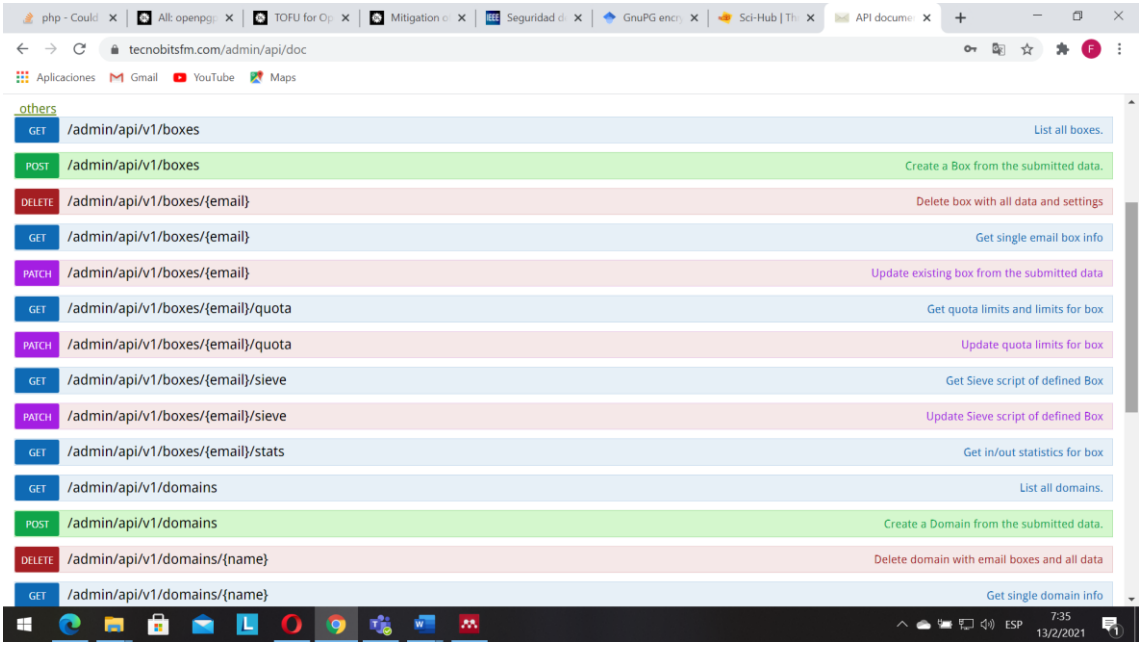
2. Integrar el buen manejo de los protocolos de seguridad ayudará a que la interacción de los usuarios con el servidor sea más cercana. Tener en cuenta que depende de la implementación que se le vaya a dar al protocolo así mismo será su rendimiento ya que estos dependen mucho de su entorno para funcionar bien.

3. Cada día las nuevas tecnologías avanzan, y con ellas también surgen nuevos problemas, nuevos desafíos, nuevas maneras de violentar la seguridad, tratar la información como lo más preciado es el deber de un servidor de correo electrónico y ser seguro para el usuario es lo que hace a estos servidores atractivos. El buen manejo de las nuevas tecnologías ayudará a que la seguridad siempre sea lo principal teniendo en cuenta la implementación constantes pruebas del servidor para así tener controlada las partes que se encuentren vulnerables y cuáles no, para su oportuna corrección.

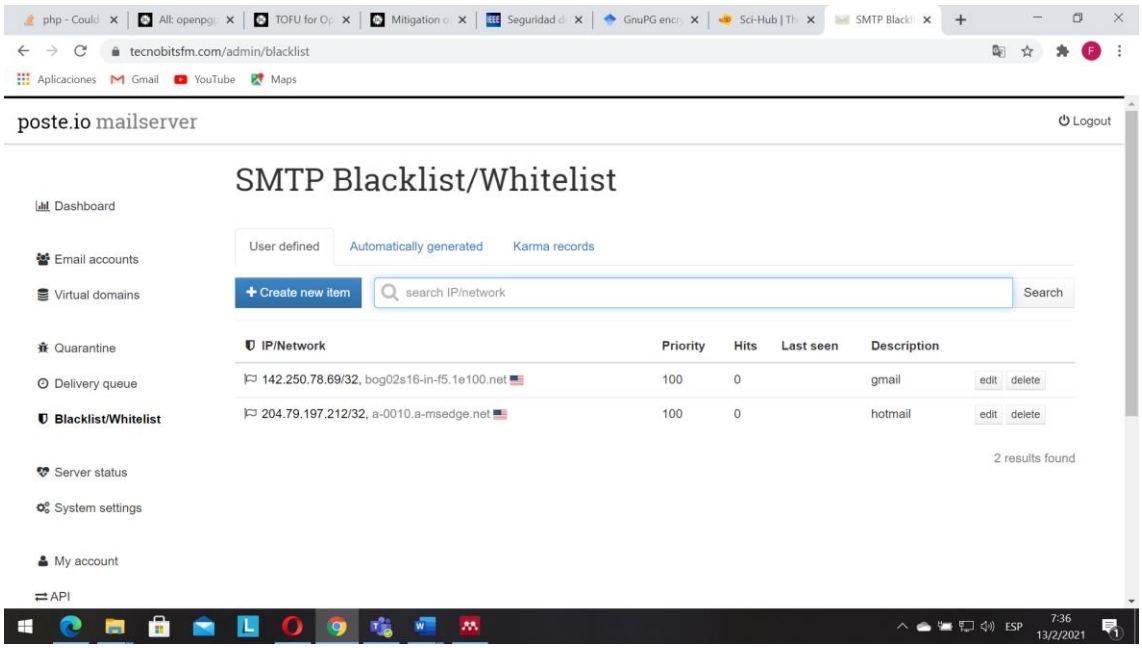
10. Anexos



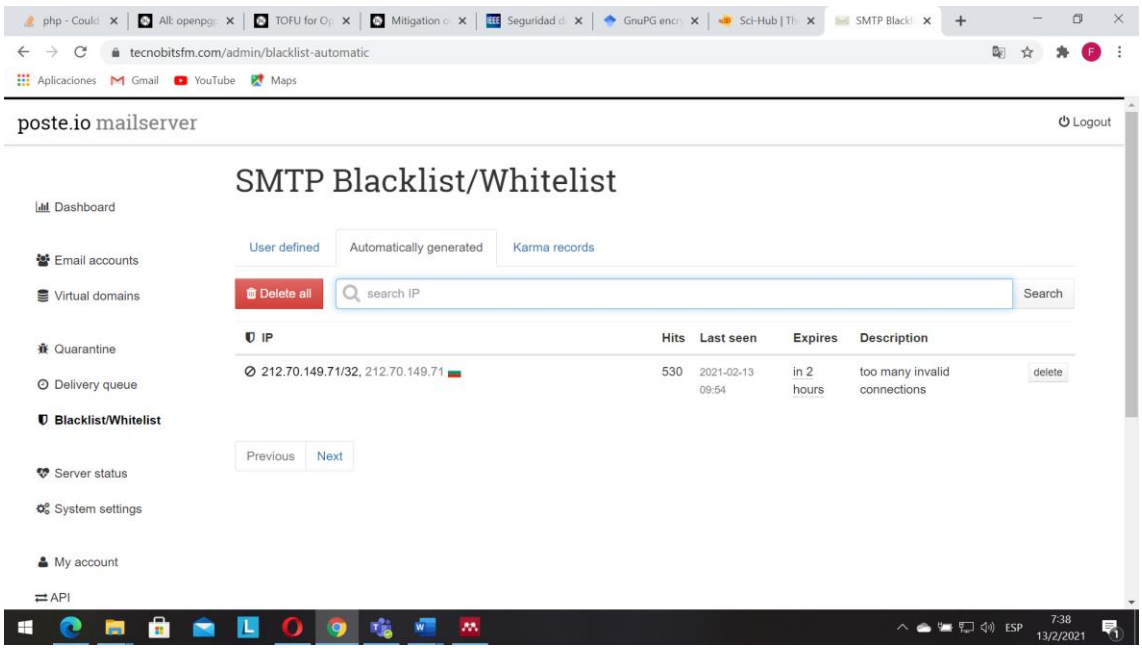
ANEXO 1 Panel de administrador



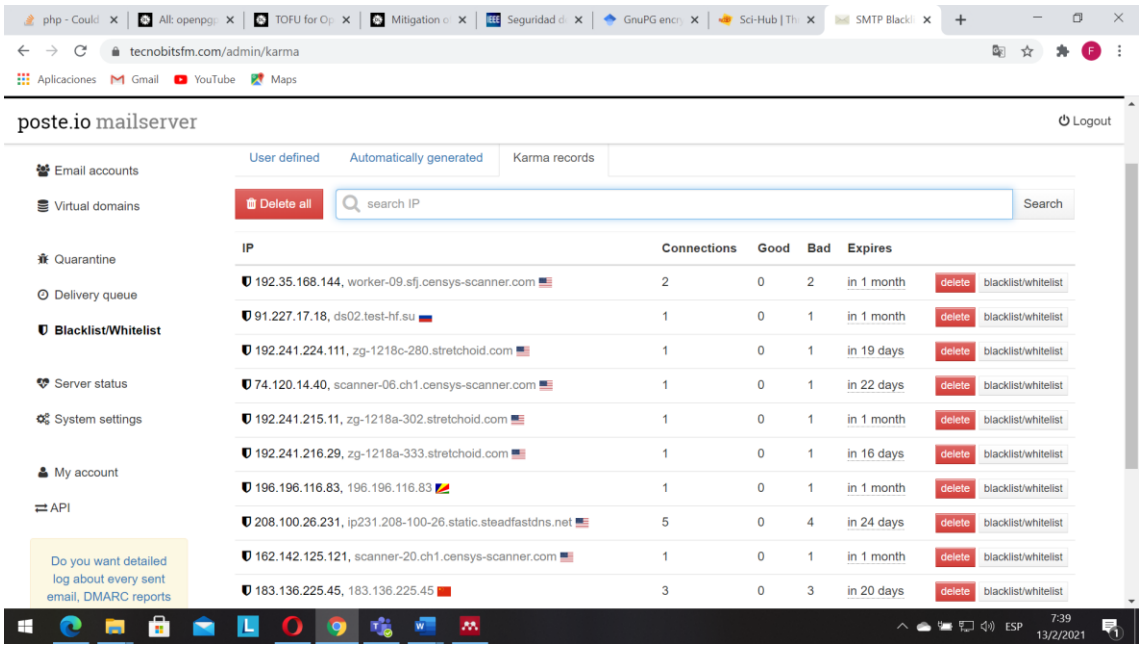
ANEXO 2 Panel de api´s



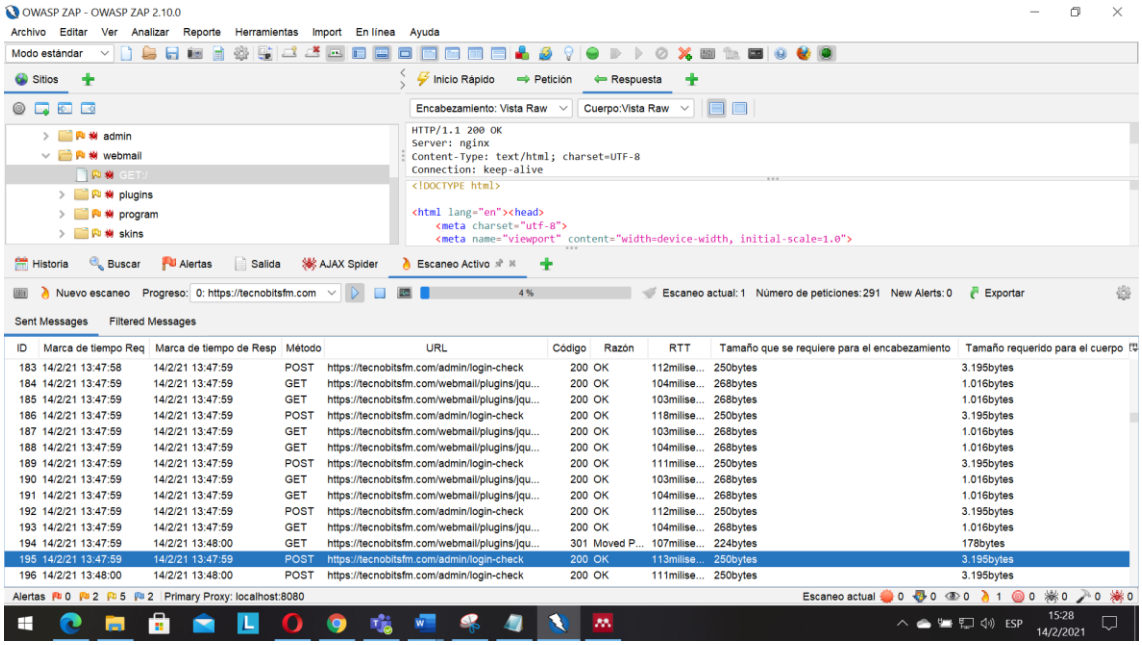
ANEXO 3 Black list/white list



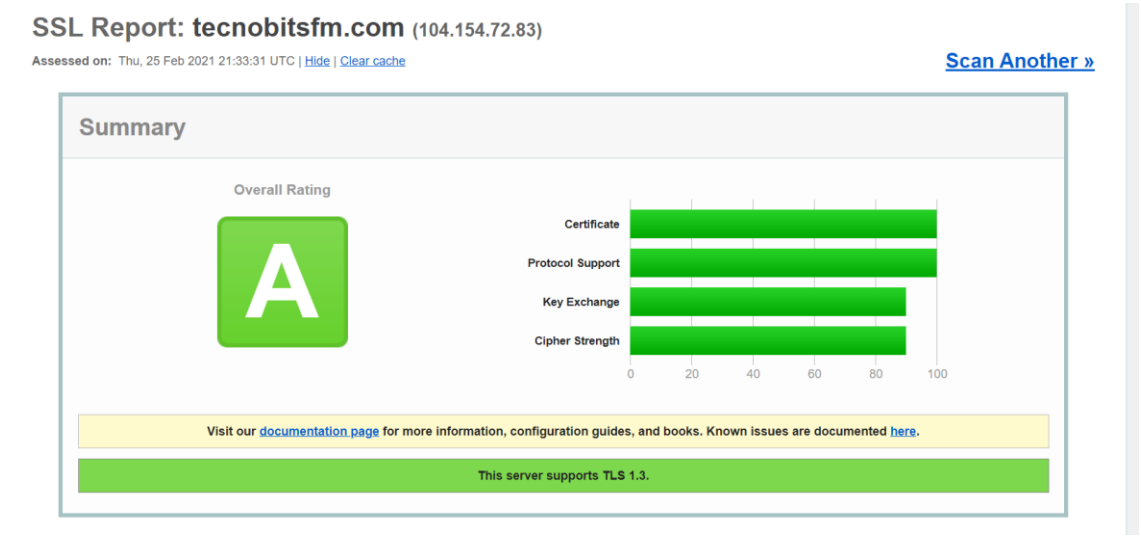
ANEXO 4 Black list automática



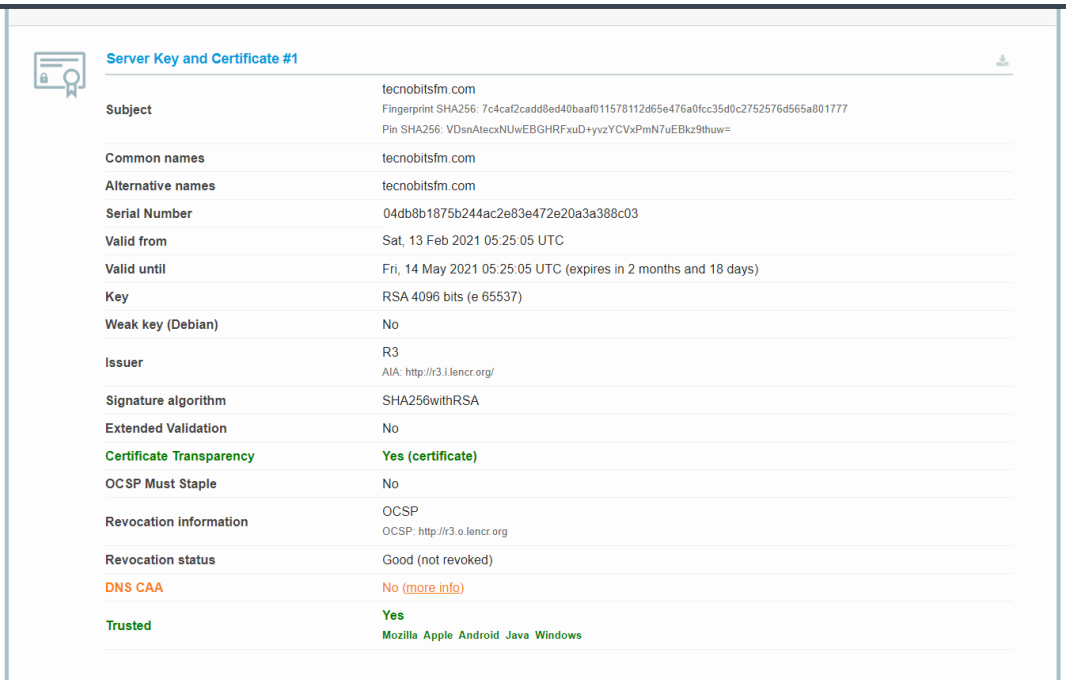
ANEXO 5 Karma list



ANEXO 6 resultados de ataque



ANEXO 7 Reporte de calificación ssl server



ANEXO 8 Reporte de calificación SSL

11. Referencia

[1] R. Roque Hernández, "Concientización y capacitación para incrementar la seguridad informática en estudiantes universitarios," *PAAKAT Rev. Tecnol. y Soc.*, vol. 8, no. 14, p. 5, 2018, doi: 10.18381/pk.a8n14.318.

[2] BBC, "Cómo fue el 'hackeo' de piratas informáticos de Rusia durante las elecciones de Estados Unidos," 2016. https://www.bbc.com/mundo/noticias-internacional-38350244.

[3] A. Kovacs, I. Karakatsanis, and D. Svetinovic, “Argumentation-based security requirements analysis: Bitmessage case study,” *Proc. - 2014 IEEE Int. Conf. Internet Things, iThings 2014, 2014 IEEE Int. Conf. Green Comput. Commun. GreenCom 2014 2014 IEEE Int. Conf. Cyber-Physical-Social Comput. CPS 20*, no. iThings, pp. 408–414, 2014, doi: 10.1109/iThings.2014.74.

[4] A. Barenghi, N. Mainardi, and G. Pelosi, “A security audit of the openPGP format,” *Proc. - 14th Int. Symp. Pervasive Syst. Algorithms Networks, I-SPAN 2017, 11th Int. Conf. Front. Comput. Sci. Technol. FCST 2017 3rd Int. Symp. Creat. Comput. ISCC 2017*, vol. 2017-Novem, pp. 336–343, 2017, doi: 10.1109/ISPAN-FCST-ISCC.2017.35.

[5] M. T. Banday and S. A. Sheikh, “S/MIME with multiple e-mail address certificates: A usability study,” *Proc. 2014 Int. Conf. Contemp. Comput. Informatics, IC3I 2014*, pp. 707–712, 2014, doi: 10.1109/IC3I.2014.7019789.

[6] L. Gómez Dueñas, “Interoperabilidad en los Sistemas de Información Documental (SID): la información debe fluir1,” *Códices*, vol. 3, no. 1, pp. 23–39, 2007.

[7] L. Sosa and P. Prefecta, “Plan Estrategico Informatico,” 2014.

[8] I. Dacosta, A. Put, and B. De Decker, “EmailCloak: A practical and flexible approach to improve email privacy,” *Proc. - 9th Int. Conf. Availability, Reliab. Secur. ARES 2014*, pp. 242–250, 2014, doi: 10.1109/ARES.2014.39.

[9] A. Anugurala and A. Chopra, “Securing and preventing man in middle attack in grid using open pretty good privacy (PGP),” *2016 4th Int. Conf. Parallel, Distrib. Grid Comput. PDGC 2016*, pp. 517–521, 2016, doi: 10.1109/PDGC.2016.7913249.

[10] K. Dai, “PGP e-mail protocol security analysis and improvement program,” *Proc. - 2011 Int. Conf. Intell. Sci. Inf. Eng. ISIE 2011*, pp. 45–48, 2011, doi: 10.1109/ISIE.2011.144.

[11] M. S. Nabi, M. L. M. Kiah, A. A. Zaidan, and B. B. Zaidan, “Messages Protocol to Secure Electronic Medical Records,” *Second Int. Conf. Futur. Gener. Commun. Technol. (FGCT 2013)*, pp. 93–97, 2013, doi: 10.1109/FGCT.2013.6767179.

[12] S. Turner, “Secure/multipurpose internet mail extensions,” *IEEE Internet Comput.*, vol. 14, no. 5, pp. 82–86, 2010, doi: 10.1109/MIC.2010.121.

[13] S. L. Garfinkel, D. Margrave, J. I. Schiller, E. Nordlander, and R. C. Miller, “How to make secure email easier to use,” *CHI 2005 Technol. Safety, Community Conf. Proc. - Conf. Hum. Factors Comput. Syst.*, pp. 701–710, 2005, doi: 10.1145/1054972.1055069.

[14] A. Schaub and D. Rossi, “Design and analysis of an improved bitmessage anti-spam mechanism,” *2015 IEEE Int. Conf. Peer-to-Peer Comput. P2P 2015*, 2015, doi: 10.1109/P2P.2015.7328523.

[15] F. Platzer, M. Schäfer, and M. Steinebach, “Critical traffic analysis on the tor network,” *ACM Int.*

Conf. Proceeding Ser., 2020, doi: 10.1145/3407023.3409180.

[16] E. N. Preeth, J. P. Mulerickal, B. Paul, and Y. Sastri, "Evaluation of Docker containers based on hardware utilization," *2015 Int. Conf. Control. Commun. Comput. India, ICCC 2015*, no. November, pp. 697–700, 2016, doi: 10.1109/ICCC.2015.7432984.

[17] A. Yakubov, W. Shbair, and R. State, "BlockPGP: A blockchain-based framework for PGP key servers," *Proc. - 2018 6th Int. Symp. Comput. Netw. Work. CANDARW 2018*, pp. 316–322, 2018, doi: 10.1109/CANDARW.2018.00065.

[18] A. Kapadia, "A case (study) for usability in secure email communication," *IEEE Secur. Priv.*, vol. 5, no. 2, pp. 80–84, 2007, doi: 10.1109/MSP.2007.25.

[19] M. A. Khorajiya and G. N. Kumar, "A security based architecture using kerberos and PGP," *ACM Int. Conf. Proceeding Ser.*, vol. 12-13-Augu, 2016, doi: 10.1145/2979779.2979821.

[20] E. Constitutivos and D. E. L. Estado, *Constitución de la República del Ecuador*. 1998, pp. 1–222.

[21] A. Mu, *Reglamento a la Ley de comercio electrónico, firmas electrónicas y mensajes de datos*, vol. 53, no. 9. 2019, pp. 1689–1699.

[22] S. Aguilar, "Fórmulas para el cálculo de la muestra en investigaciones," *Salud en Tabasco*, vol. 11, pp. 2–7, 2005, [Online]. Available: https://www.redalyc.org/pdf/487/48711206.pdf.

[23] Mailgun, "Mailgun." https://www.mailgun.com/company/.

[24] OWASP, "OWASP Difinicion," [Online]. Available: https://owasp.org/.

[25] owasp, "OWASP TOP 10," [Online]. Available: https://owasp.org/www-project-top-ten/.

[26] F. De *et al.*, "Ciberseguridad," pp. 73–99, 2016.

[27] J. Leng, M. Zhou, L. J. Zhao, Y. Huang, and Y. Bian, "Blockchain Security: A Survey of Techniques and Research Directions," *IEEE Trans. Serv. Comput.*, vol. 1374, no. c, 2020, doi: 10.1109/TSC.2020.3038641.

[28] A. Çelik *et al.*, "Three models for the description of language," *J. Mater. Process. Technol.*, vol. 1, no. 1, pp. 1–8, 2018, [Online]. Available: http://dx.doi.org/10.1016/j.cirp.2016.06.001%0Ahttp://dx.doi.org/10.1016/j.powtec.2016.12.055%0Ahttps://doi.org/10.1016/j.ijfatigue.2019.02.006%0Ahttps://doi.org/10.1016/j.matlet.2019.04.024%0Ahttps://doi.org/10.1016/j.matlet.2019.127252%0Ahttp://dx.doi.o.

[29] M. V. G. V. Jessica Janneth Valle Padilla, "ANÁLISIS DE VULNERABILIDADES DE SOFTWARE PARA MEJORAR LA SEGURIDAD EN LOS SISTEMAS INFORMÁTICOS.," 2015.