UNIVERSIDAD DE CHILE
FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS
DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

Sistema Comunitario de Prevención, Detección y Seguimiento de Filtraciones de Correos Electrónicos Mediante un Proxy de Correos Temporales

MEMORIA PARA OPTAR AL TÍTULO DE
INGENIERO CIVIL EN COMPUTACIÓN

Sebastián Andrés Valdivia Reyes

PROFESOR GUÍA:
Eduardo Riveros Roca

MIEMBROS DE LA COMISIÓN:
Camilo Gómez Núñez
Federico Olmedo

SANTIAGO DE CHILE
2023

Resumen

En la presente memoria, se desarrolló un sistema comunitario de proxy de correos temporales, cuyo propósito es la prevención, detección y seguimiento de filtraciones de correos electrónicos. Este sistema, de código abierto, está diseñado para proporcionar una herramienta útil para futuros estudios sobre la privacidad del correo electrónico en Chile.

El trabajo se centró en la investigación y análisis de sistemas de proxy de correos existentes para identificar áreas de mejora y establecer una base sólida para el desarrollo de una solución adaptada a las necesidades locales. Se diseñó e implementó una base de datos preliminar que garantiza la privacidad y la integridad de la información, y se desarrolló un backend para gestionar la lógica de negocio y el procesamiento de datos de manera eficiente y segura.

El frontend del sistema fue construido para proporcionar una experiencia de usuario fluida y accesible, mientras que una extensión de navegador facilita la creación y gestión de correos electrónicos temporales de manera conveniente. Además, se aseguró la comunicación efectiva entre el frontend, el backend y la base de datos, y se dockerizaron los componentes del sistema para simplificar su despliegue y mantenimiento.

Este proyecto demuestra la viabilidad de una solución comunitaria de proxy de correos electrónicos como una medida efectiva para mejorar la seguridad de las comunicaciones en línea. El diseño modular y escalable del sistema permite adaptaciones y mejoras futuras, con miras a fortalecer aún más la privacidad y seguridad de los usuarios de correo electrónico en Chile.

Para mi Padre, Madre y Hermano, que me enseñaron que los sueños se construyen con esfuerzo, amor y paciencia.

Tabla de contenido

1. Introducción

1.1. Contexto

El correo electrónico, en su papel de herramienta esencial en la vida cotidiana de individuos y organizaciones, se ha entrelazado profundamente con las prácticas diarias de comunicación y gestión de información alrededor del mundo. Su uso extendido, impulsado por la globalización digital y la omnipresencia de tecnologías de información, ha transformado la manera en que interactuamos, realizamos negocios y compartimos información. Sin embargo, esta integración sin precedentes del correo electrónico en nuestras vidas ha llevado a desafíos significativos relacionados con la seguridad y la privacidad de los usuarios [24].

En Chile, la dependencia del correo electrónico y otras tecnologías de información y comunicación ha sido cada vez más notable, reflejando un patrón similar a nivel global. Este crecimiento exponencial en el uso de tecnologías digitales ha hecho que la seguridad en Internet y la protección de datos personales cobren una importancia crítica. A pesar de los esfuerzos por establecer un marco legal robusto, los desafíos asociados con la seguridad de la información, especialmente en lo que respecta a las comunicaciones por correo electrónico, siguen siendo un tema de preocupación constante tanto para individuos como para entidades corporativas y gubernamentales en el país [27].

El correo electrónico no solo se ha convertido en un medio crucial para el intercambio de información, sino también en un blanco primordial para diversas actividades ilícitas, incluyendo ataques de *phishing*, estafas y otros tipos de ciberdelitos. Estos ataques, a menudo dirigidos a obtener acceso no autorizado a información personal y confidencial, han resaltado la vulnerabilidad inherente a los sistemas de correo electrónico y la necesidad de fortalecer las medidas de seguridad [17].

Además, los protocolos de autenticación de correo electrónico, como SPF (Sender Policy Framework) [20], DKIM (DomainKeys Identified Mail) [29] y DMARC (Domain-based Message Authentication, Reporting and Conformance) [22], aunque juegan un papel crucial en la prevención de prácticas fraudulentas, no están universalmente implementados, lo que deja brechas significativas en la seguridad general del correo electrónico. Estos protocolos, diseñados para verificar la autenticidad de los correos y prevenir el phishing y el spam, son una pieza clave en la infraestructura de seguridad del correo electrónico, pero su eficacia se ve limitada por su adopción inconsistente.

A pesar de la existencia de soluciones de proxy de correo electrónico, las cuales ofrecen un nivel de protección adicional al actuar como intermediarios entre los usuarios y los servidores de correo, su uso óptimo y eficiente se ve obstaculizado por limitaciones técnicas y de accesibilidad. Estas limitaciones incluyen, entre otras, suscripciones de pago, falta de garantías sólidas de privacidad, interfaces mayormente en inglés, y requerimientos técnicos elevados para su configuración y mantenimiento [23].

Este contexto subraya la necesidad crítica de desarrollar soluciones innovadoras y adaptadas a

las necesidades locales, especialmente en un país como Chile, donde la seguridad de la información y la protección de la privacidad están tomando un papel central en el discurso público y corporativo. La propuesta de este proyecto, un sistema comunitario de prevención, detección y seguimiento de filtraciones de correos electrónicos a través de un proxy de correos temporales, surge como respuesta a esta necesidad emergente y refleja un esfuerzo por abordar los desafíos de seguridad en el correo electrónico de manera localizada y efectiva.

1.2. Problemas y Relevancia

El problema central que aborda esta memoria es la vulnerabilidad inherente de los correos electrónicos frente a diversas amenazas de seguridad. En particular, se concentra en las filtraciones de correos electrónicos, un fenómeno crecientemente preocupante en un mundo donde la información personal se ha convertido en un bien valioso y a menudo vulnerable. Las filtraciones pueden tener múltiples causas, incluyendo ataques de *phishing*, brechas de seguridad en bases de datos y prácticas negligentes de manejo de datos. Estas filtraciones no solo comprometen la privacidad del usuario, sino que también pueden llevar a consecuencias más graves como el robo de identidad y el fraude financiero [17].

La relevancia de este problema se magnifica en el contexto de una sociedad cada vez más digitalizada, donde la cantidad y el valor de la información personal en línea están en constante aumento. En Chile, como en muchos otros países, la dependencia del correo electrónico para la comunicación personal y profesional ha crecido exponencialmente, haciendo que la seguridad de estos sistemas sea de vital importancia. Sin embargo, las medidas de seguridad actuales, incluyendo protocolos como SPF, DKIM y DMARC, aunque son pasos importantes, resultan insuficientes para abordar completamente la problemática.

Además, la naturaleza dinámica de las amenazas cibernéticas significa que las soluciones de seguridad deben ser continuamente revisadas y actualizadas. Los protocolos existentes, aunque efectivos hasta cierto punto, no cubren todos los aspectos de seguridad necesarios y a menudo son ignorados o pueden ser mal implementados por los proveedores de servicios de correo electrónico, dejando vulnerabilidades significativas. La falta de implementación generalizada de estos protocolos deja a los usuarios en riesgo, incluso cuando ellos mismos siguen las mejores prácticas de seguridad [18].

La utilización de un proxy de correo electrónico representa una solución potencialmente eficaz a este problema. Al actuar como intermediario, un proxy de correo puede ofrecer una capa adicional de seguridad, protegiendo la dirección de correo electrónico real del usuario y minimizando el riesgo de filtraciones. Sin embargo, las soluciones existentes presentan limitaciones significativas, incluyendo costos, complejidad técnica, y preocupaciones sobre la privacidad y la gestión de datos. Estas limitaciones subrayan la necesidad de desarrollar una solución más accesible y adaptada a las necesidades específicas de los usuarios en Chile.

La relevancia de este trabajo, por lo tanto, se extiende más allá de la mera implementación técnica; busca abordar una brecha significativa en la seguridad de la información y contribuir a la protección de la privacidad en un contexto en el que los datos personales son cada vez más codiciados y vulnerables a la explotación.

1.3. Objetivo General

Desarrollar y poner en marcha un sistema comunitario de prevención, detección y seguimiento de filtraciones de correos electrónicos mediante un proxy de correos temporales de código abierto y gratuito, para poder realizar a futuro estudios acerca de la privacidad de los correos en Chile.

1.4. Objetivos Específicos

1. Investigar y analizar en profundidad los sistemas de proxy de correos existentes, evaluando sus funcionalidades, ventajas, limitaciones y posibles áreas de mejora, con el fin de obtener una base sólida para el desarrollo del sistema propuesto.
2. Diseñar e implementar una base de datos preliminar para el almacenamiento eficiente y seguro de los datos del sistema, asegurando la privacidad y la integridad de la información.
3. Desarrollar el backend del sistema, para gestionar la lógica de negocio y el procesamiento de datos de forma eficiente y segura.
4. Construir un frontend interactivo y accesible, que ofrezca una experiencia de usuario fluida y sencilla para interactuar con el sistema de correos electrónicos.
5. Desarrollar una extensión de navegador que permita una experiencia cómoda y rápida al momento de crear y poder acceder a los mails.
6. Integrar y asegurar la comunicación efectiva entre el frontend, el backend y la base de datos, garantizando un flujo de datos coherente y seguro.
7. Dockerizar los componentes del sistema para facilitar su despliegue rápido y sencillo, promoviendo así una mayor accesibilidad y mantenibilidad del proyecto.
8. Poner en marcha el sistema y ponerlo a disposición del público, asegurando su accesibilidad y facilidad de uso para la comunidad.

1.5. Descripción General de la Solución

La solución desarrollada en esta memoria se enfoca en una aplicación web que permita crear correos electrónicos temporales, poniendo especial énfasis en la privacidad y la seguridad de los datos. Inicialmente, se realizó una evaluación técnica de soluciones de código abierto existentes, considerando su posible extensión con tecnologías como Python, JavaScript, FastAPI, Next.js y TailwindCSS. No obstante, se decidió proceder con un desarrollo desde cero para tener un control más riguroso sobre el modelo de datos, que datos almacenar y para establecer estándares de seguridad en particular sobre el Mail Transfer Agent para evitar lecturas de información privada, commits y despliegues que faciliten el trabajo y las mejoras futuras.

Una característica clave del sistema es el uso de Postfix como agente de transferencia de correo (MTA), asegurando una transferencia de correos electrónicos eficiente y segura. Se integra PostgreSQL para la gestión de bases de datos, garantizando el almacenamiento seguro de información relevante.

La interfaz de usuario se ha diseñado para ser intuitiva y accesible, mejorando significativamente la interacción de los usuarios con el sistema. La implementación técnica utiliza Docker para la gestión del entorno de desarrollo y un despliegue eficiente de la aplicación, mientras que Caddy actúa como servidor web y proxy inverso, proporcionando HTTPS automático y optimizando el rendimiento del sistema.

Se ha desarrollado también una extensión de navegador para Firefox y Chrome, empleando JavaScript, que permite a los usuarios generar y administrar correos electrónicos temporales de manera eficaz y conveniente.

Además, para demostrar la viabilidad y facilitar el acceso público, el sistema completo está implementado y puede ser accedido en `https://chinchillamail.cl`. El código fuente está disponible en un repositorio público en GitHub `https://github.com/hackerlab-uchile/mail_relay`, lo que permite su revisión y contribuciones por parte de la comunidad.

La seguridad y privacidad de los usuarios son pilares fundamentales en este sistema, implementando medidas de protección de datos como el cifrado de las comunicaciones y minimizando el almacenamiento de información. El diseño del sistema es extensible, permitiendo futuros análisis sobre el uso de correos proxy y la detección de brechas de información.

En cuanto a la implementación de un proxy de correo, estas implicaciones se relacionan directamente con su propósito central: proteger las direcciones de correo electrónico de los usuarios de ser expuestas y filtradas. Al utilizar una dirección de correo electrónico proxy en lugar de la dirección de correo electrónico real del usuario, permite evitar exponer el correo personal de un usuario.

Además, un sistema de proxy de correo puede también implementar mecanismos de detección y seguimiento de filtraciones. Por ejemplo, ya que genera direcciones de correo únicas para cada

servicio usado por el usuario, se puede identificar fácilmente la fuente de una filtración al recibir un correo malicioso o de un remitente distinto al original.

En este sentido, un proxy de correo no sólo puede proteger contra las filtraciones de datos, sino que también puede ayudar a identificarlas cuando ocurren, permitiendo a los usuarios y a las organizaciones tomar medidas para mitigar el daño y prevenir futuras filtraciones.

Así, entender las implicaciones de las filtraciones de datos y cómo se pueden prevenir y gestionar es esencial para el diseño y la implementación de un sistema de proxy de correo eficaz y seguro.

Este enfoque ofrece una solución integral y segura para la gestión de emails temporales, adaptándose eficazmente a las necesidades actuales de privacidad y seguridad de los usuarios.

2. Estado del Arte

2.1. Situacion Actual

Hasta el año 2021, se reportan alrededor de 4200 millones de direcciones de correo [30]. De entre los cuales el 35 % de los casos de robo a grandes empresas, son causados por ataques tanto de phishing como robo de credenciales, causando perdidas millonarias [9].

En Chile, la seguridad en Internet y la protección de datos personales están cobrando cada vez más importancia debido al crecimiento exponencial del uso de tecnologías de la información y comunicación. Actualmente Chile solo tiene la Ley de Protección de Datos Personales (Ley N° 19.628) que establece un marco legal para garantizar la protección de datos personales en el país [25].

Sin embargo, la ley de protección de datos vigente ya está obsoleta. Si bien se promulgó en 1999 y fue una de las primeras de su tipo en Latinoamérica, no estableció sanciones ni mecanismos o instancias especiales ante las cuales recurrir para protegerse ante una infracción. Nadie fiscaliza, regula ni sanciona, que ha provocado una cultura en la cual no hay concientización sobre los riesgos de compartir información privada [26]. Dado este escenario, el uso de un proxy de correo electrónico otorga una mitigación eficiente a estos problemas.

El mercado actual ofrece distintas soluciones internacionales para la prevención y detección de filtraciones, como los servicios de correos temporales gratuitos como GuerrillaMail [12]., servicios relay de correos de pago como Firefox Relay [11] y iCloud Hide My Email [14]. No obstante, estos servicios tienen limitaciones, como la disponibilidad de cantidad de correos temporales y suscripciones mensuales pagas. Además, no hay soluciones locales que aborden eficazmente este problema y se adapten específicamente a las necesidades de los usuarios chilenos.

Existen también soluciones de código abierto en el ámbito de los proxy de correos electrónicos, como AnonAddy [1] y SimpleLogin [6]. Estas alternativas ofrecen mayor flexibilidad y transparencia al permitir a los usuarios examinar y modificar el código fuente según sus necesidades. Sin embargo, estas soluciones pueden presentar dificultades en términos de instalación, configuración y mantenimiento para usuarios sin conocimientos técnicos avanzados, además de no contar con capacidad de facilitar información para estudios.

Características	**Firefox Relay**	**GuerrillaMail**	**ProtonMail**
Tipo de servicio	Correo temporal	Correo temporal	Correo seguro
Encriptación	SSL/TLS	SSL/TLS	PGP y SSL/TLS
Cifrado de extremo a extremo para emails	No	No	Sí
Código Abierto	No	Si	No
Capacidad de almacenamiento	Limitada	No aplicable	Limitada (a menos que se actualice a una cuenta de pago)
Envío de archivos adjuntos	No	No	Sí
Integración con clientes de correo electrónico	No	No	Limitada
Caducidad de las cuentas	Sí (varía según el servicio)	Sí (varía según el servicio)	No
Compatibilidad con servicios de terceros	No	No	Limitada
Cantidad de direcciones de correo permitidas en la versión gratuita	5	1	1
Costo	Gratuito Limitado y de pago	Gratuito	Gratuito Limitado y de pago
Idioma	Inglés	Inglés	Inglés

Tabla 1: Comparación de servicios de correo electrónico.

Como podemos ver ninguno de estos servicios ofrece una solución que permita realizar estudios, en español, sea gratuito, fácil de usar y de código abierto. En este contexto, es necesario desarrollar una solución que permita a los usuarios proteger su correo electrónico y mejorar su seguridad en línea. La creación de un sistema comunitario de prevención, detección y seguimiento de filtraciones de correos electrónicos adaptado a las necesidades locales y regulaciones chilenas es esencial para abordar esta problemática.

2.2. Filtraciones de Datos y sus Implicaciones

Las filtraciones de datos son un problema creciente y significativo que puede tener consecuencias graves para la privacidad y seguridad de los individuos y organizaciones. En el contexto de la seguridad del correo electrónico, una filtración de datos puede dar lugar a la exposición de direcciones de correo electrónico y otros datos personales asociados a ellas.

Las consecuencias de estas filtraciones pueden variar desde el spam y el correo no deseado hasta amenazas más graves como el phishing y el robo de identidad. Además, las filtraciones de datos también pueden dañar la reputación de las organizaciones y resultar en pérdidas financieras debido a multas y litigios [10].

2.3. Métodos de Filtración de Correo Electrónico y sus Contramedidas

En el contexto de los correos electrónicos, la filtración se refiere al proceso por el cual las direcciones de correo electrónico de los usuarios se hacen accesibles a personas o entidades no autorizadas. Esta sección discutirá algunos de los métodos más comunes de filtración de correo electrónico y cómo un proxy de correo puede ser utilizado como contramedida.

2.3.1. Fuga de Datos en Sitios Web

Muchas filtraciones de direcciones de correo electrónico ocurren a través de brechas de datos en sitios web donde los usuarios se han registrado con sus direcciones de correo electrónico. Cuando estos sitios web son hackeados o sufren una violación de seguridad, las direcciones de correo electrónico registradas pueden caer en manos equivocadas.

Un proxy de correo puede mitigar este riesgo al proporcionar una dirección de correo electrónico alternativa para utilizar en los registros de los sitios web. De esta manera, incluso si la dirección de correo electrónico proporcionada es comprometida, la dirección de correo electrónico real del usuario se mantiene segura.

2.3.2. Phishing

El phishing [19] es un método popular de obtener direcciones de correo electrónico y otra información confidencial. Los atacantes engañan a los usuarios para que entreguen sus datos a través de correos electrónicos falsificados que parecen legítimos.

Utilizando un proxy de correo, los usuarios pueden manejar sus correos electrónicos entrantes de una manera más segura. Los correos electrónicos sospechosos pueden ser filtrados y aislados, protegiendo al usuario de posibles intentos de phishing.

2.3.3. Rastreo Web y Recolección de Datos

Los rastreadores web o *web crawler* [8], son bots de motor de búsquedas que descargan e indexan contenido por todo el internet, esto incluye recopilar direcciones de correo electrónico de varias fuentes en Internet, incluyendo redes sociales, foros y sitios web de comercio electrónico.

El uso de un proxy de correo puede dificultar el trabajo de los rastreadores. Al usar diferentes direcciones de correo electrónico para diferentes servicios, se hace más difícil para los rastreadores correlacionar la información y formar un perfil completo del usuario.

2.3.4. Venta y Compartición de Datos

Algunas empresas pueden vender o compartir las direcciones de correo electrónico de sus usuarios con terceros para fines de marketing. Aunque esto se considera una mala práctica, sigue ocurriendo.

Un proxy de correo puede proteger a los usuarios de esta forma de filtración al proporcionar direcciones de correo electrónico "desechables" que pueden ser desactivadas si comienzan a recibir spam o correos electrónicos no deseados.

En resumen, los proxies de correo pueden ser una herramienta efectiva para proteger las direcciones de correo electrónico de los usuarios de una variedad de métodos de filtración. Proporcionan una capa adicional de privacidad y seguridad, ayudando a los usuarios a mantener el control de sus datos personales.

2.4. Estándares y Protocolos de Correo Electrónico

Para entender completamente cómo un proxy de correo puede mejorar la seguridad y la privacidad de los usuarios, es esencial familiarizarse con los estándares y protocolos que rigen el funcionamiento de los sistemas de correo electrónico.

2.4.1. SMTP, IMAP y POP

Simple Mail Transfer Protocol [7] (SMTP) es el protocolo estándar para el envío de correos electrónicos a través de la red. Los servidores de correo electrónico utilizan SMTP para enviar y recibir mensajes de correo electrónico. Por otro lado, Internet Message Access Protocol (IMAP) [16] y Post Office Protocol [4] (POP) se utilizan comúnmente para recuperar los mensajes de correo electrónico del servidor, en nuestro caso no planeamos utilizarlos. Aunque estos protocolos son útiles para explicar el funcionamiento general de los sistemas de correo electrónico, es importante aclarar que en nuestra solución de proxy de correo electrónico, un usuario no debería poder leer los correos directamente desde el proxy para garantizar la privacidad y seguridad del usuario.

Un proxy de correo interactúa con estos protocolos al reenviar los correos electrónicos desde el servidor de correo original al servidor de correo del usuario. Asegurar una interacción adecuada y

segura con estos protocolos es fundamental para el correcto funcionamiento de un proxy de correo.

2.4.2. Agentes de Transferencia de Correo (MTA) y Servidores SMTP

Los Agentes de Transferencia de Correo (MTA) son componentes esenciales en la infraestructura de correo electrónico, encargados de transportar correos electrónicos de un servidor a otro hasta llegar a su destino final. Postfix es un ejemplo de un MTA ampliamente utilizado, conocido por su seguridad y eficiencia. Diferenciándolos de los MTAs, los servidores SMTP se especializan en el proceso de envío y recepción inicial de los correos electrónicos desde y hacia los agentes de correo de los usuarios. En esencia, los servidores SMTP actúan como el punto de entrada y salida para los correos que fluyen a través de Internet. Comprender el funcionamiento de los MTAs y los servidores SMTP es vital para el desarrollo de un proxy de correo electrónico que sea tanto seguro como confiable [21].

2.4.3. TLS y SSL

Transport Layer Security (TLS) y su predecesor, Secure Sockets Layer (SSL), son protocolos criptográficos que proporcionan comunicaciones seguras a través de una red. En el contexto del correo electrónico, se utilizan para cifrar los mensajes de correo electrónico durante el tránsito para protegerlos de la interceptación y el espionaje [28].

Un proxy de correo debe implementar estos protocolos para garantizar la seguridad de los correos electrónicos que maneja. Esto es especialmente importante cuando se envían correos electrónicos a través de redes inseguras o cuando se manejan correos electrónicos que contienen información sensible.

2.4.4. SPF, DKIM y DMARC

Sender Policy Framework [20] (SPF), DomainKeys Identified Mail [29] (DKIM) y Domain-based Message Authentication, Reporting and Conformance [22] (DMARC) son protocolos que ayudan a proteger contra el abuso de correo electrónico y la suplantación de identidad.

SPF permite a los servidores de correo verificar que los correos electrónicos entrantes provienen de un dominio que ha sido autorizado por los administradores de ese dominio. DKIM permite al servidor receptor verificar que los correos electrónicos no han sido alterados durante el tránsito. DMARC es un protocolo que utiliza SPF y DKIM para proporcionar una mayor garantía de que el correo electrónico es auténtico.

Cuando se implementa un proxy de correo, es esencial configurar correctamente estos protocolos para asegurar que los correos electrónicos enviados a través del proxy sean aceptados por los servidores de correo de los destinatarios y no sean marcados como spam o phishing. Esto también ayuda a mantener la reputación del dominio del proxy de correo, lo cual es importante para garantizar la entrega de correo electrónico confiable.

En resumen, el conocimiento y la correcta implementación de estos estándares y protocolos son fundamentales para desarrollar un proxy de correo efectivo y seguro. La incorporación de estas prácticas de seguridad y autenticación garantiza la integridad de los correos electrónicos y la confidencialidad de los datos del usuario.

3. Solución

3.1. Visión General de la Solución

El sistema de proxy de correos electrónicos, ChinchillaMail [2], presenta una solución innovadora para mejorar la seguridad y la privacidad en la comunicación por correo electrónico. En su núcleo, el sistema utiliza una arquitectura robusta, diseñada para interceptar, procesar y reenviar correos electrónicos, proporcionando a los usuarios control y anonimato en sus interacciones por correo electrónico.

La solución consta de varios componentes interconectados, trabajando en conjunto para ofrecer una experiencia de usuario fluida y segura. Estos incluyen un frontend intuitivo, un backend potente y eficiente, una base de datos optimizada para el almacenamiento y manejo de datos, y un servicio Postfix configurado para el procesamiento y reenvío de correos electrónicos.

ChinchillaMail se distingue por su capacidad de generar alias de correo electrónico únicos y aleatorios, combinando elementos culturales chilenos con números, para cada usuario. Esto permite a los usuarios mantener su dirección de correo electrónico principal protegida, mientras utilizan estos alias para diversas actividades en línea. Además, el sistema está diseñado para ser accesible y transparente: está disponible en la página web [2] y su código fuente y documentación están alojados en un repositorio público de GitHub [5], promoviendo así un espíritu de colaboración y mejora continua.

En las siguientes subsecciones, se detalla cada aspecto de esta solución, desde la arquitectura y el diseño hasta la implementación y despliegue específicos, proporcionando una comprensión profunda de cómo ChinchillaMail aborda eficazmente los desafíos de seguridad y privacidad en la comunicación por correo electrónico.

3.2. Diseño de la Solución

El diseño de la solución (Figura 1) se basa en una arquitectura compuesta por varios componentes interconectados, cada uno desempeñando un rol esencial para la funcionalidad global del sistema de proxy de correos electrónicos. A continuación, se detallan las conexiones clave representadas en el diagrama:

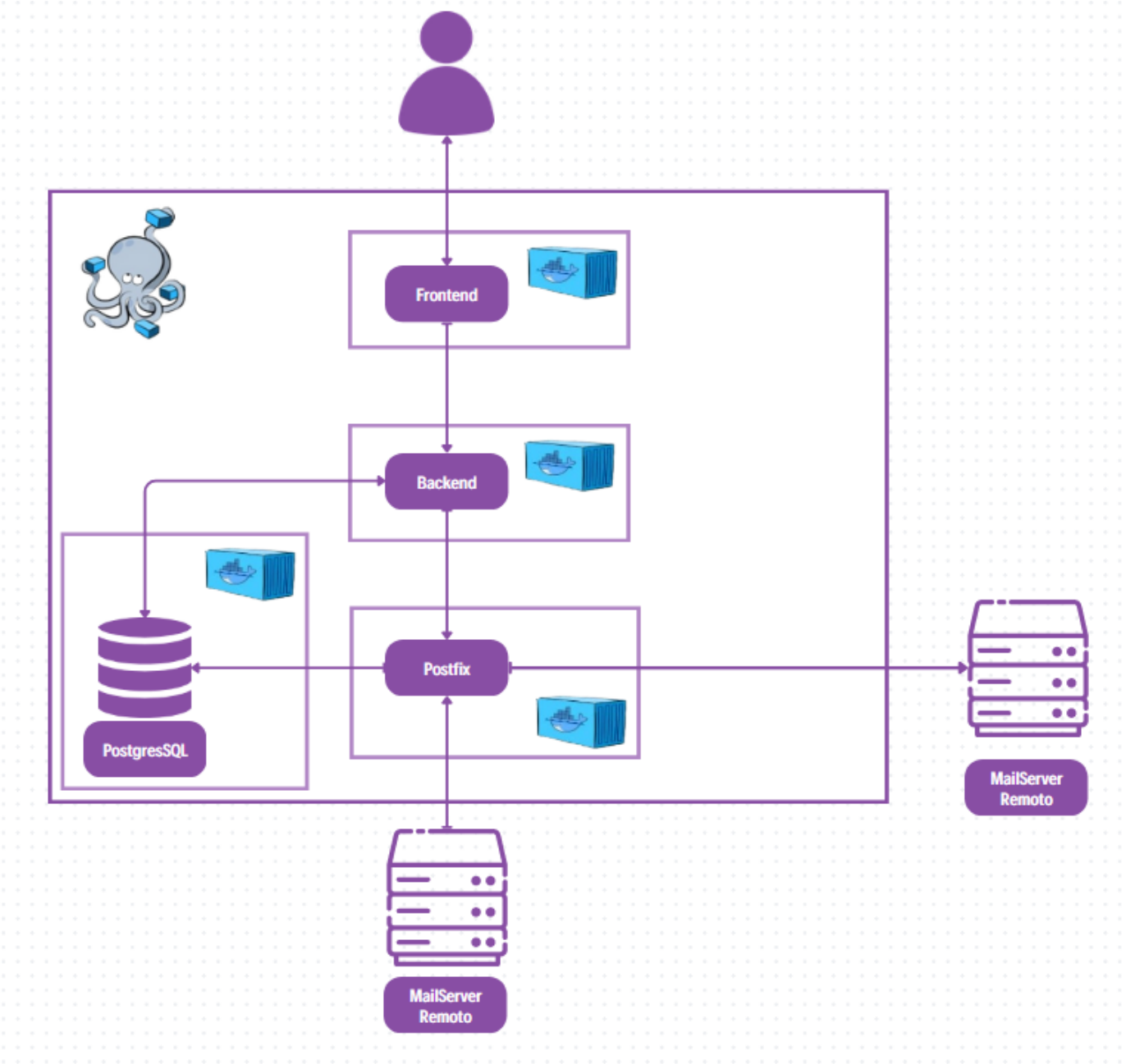

Figura 1: Diseño de la Solución

1. **Usuario:** El punto de partida de la interacción, donde el usuario accede al sistema a través del frontend.
2. **Frontend a Backend:** El frontend comunica las acciones y solicitudes del usuario al backend.
3. **Backend a PostgreSQL:** El backend realiza operaciones de datos, como la gestión de usuarios y alias, mediante consultas a la base de datos PostgreSQL.
4. **PostgreSQL a Backend:** La base de datos devuelve los resultados de las consultas al backend para su procesamiento.
5. **Backend a Postfix:** El backend se conecta con los logs del servidor Postfix para la auditoria de correos enviados.
6. **MailServer Remoto a Postfix:** Otro punto de partida de interaccion con la aplicación, los servidores de correo remotos entregan correos electrónicos al servidor Postfix para ser redirigidos.
7. **Postfix a PostgreSQL:** Postfix se comunica con la Base de Datos para verificar si el mail alias pertenece al sistema.
8. **Postfix a MailServer Remoto:** Postfix interactúa con servidores de correo remotos para enviar correos electrónicos.
9. **Backend a Frontend:** El backend refleja el estado de los correos generados al frontend para que el usuario pueda visualizarlos.

Estas conexiones aseguran un flujo de información coherente y eficiente a través del sistema, permitiendo que el usuario gestione sus correos electrónicos y alias de manera segura y confiable.

3.3. Backend

El backend de la aplicación web es una pieza central en la arquitectura del sistema de proxy de correos electrónicos. Su diseño y funcionalidad se orientan a cumplir con múltiples responsabilidades clave, garantizando el rendimiento, la seguridad y la escalabilidad del sistema. Las principales áreas de enfoque y funciones del backend se describen a continuación:

3.3.1. Inicialización y Configuración de la Base de Datos

La inicialización y configuración de la base de datos constituyen los primeros y fundamentales pasos en el funcionamiento del backend de la aplicación web. Al arrancar, el backend establece una conexión con PostgreSQL, una base de datos relacional robusta y ampliamente utilizada, conocida por su fiabilidad y su capacidad para manejar grandes volúmenes de datos.

El uso de SQLAlchemy como ORM (Object-Relational Mapper) juega un papel crucial en este proceso. SQLAlchemy no solo facilita la definición de modelos de datos en un formato orientado a objetos, sino que también abstrae y simplifica las interacciones con la base de datos. Esta herramienta permite realizar operaciones de base de datos, como consultas y actualizaciones, de

una manera que es natural para los desarrolladores de Python, manteniendo al mismo tiempo la potencia y flexibilidad de SQL.

Durante la fase de inicialización, el backend se encarga de preparar las tablas de la base de datos. Esto incluye la creación de nuevas tablas según los modelos definidos, así como la configuración de relaciones, índices y restricciones necesarias para el correcto funcionamiento de la aplicación. Este proceso asegura que la estructura de la base de datos esté optimizada y lista para ser utilizada desde el momento en que la aplicación comienza a funcionar.

Una característica importante de este proceso es su capacidad para manejar actualizaciones y cambios en la estructura de la base de datos. Gracias a las herramientas proporcionadas por SQLAlchemy y la flexibilidad del diseño del backend, cualquier modificación en los modelos de datos puede implementarse de manera eficiente y coherente, garantizando así que la base de datos evolucione junto con la aplicación.

3.3.2. Gestión de Alias y Generación Aleatoria

Una característica distintiva del sistema es la generación de alias de correo electrónico. Cada alias se crea utilizando una combinación única de elementos seleccionados aleatoriamente, lo que resulta en direcciones de correo electrónico tanto únicas como memorables. El proceso de generación de alias funciona de la siguiente manera:

- Se mantiene una lista de animales chilenos y otra lista de chilenismos, dos conjuntos de palabras representativos de la cultura y la biodiversidad de Chile.
- Al crear un nuevo alias, el sistema selecciona al azar un elemento de cada lista y lo combina con un número aleatorio entre 0 y 10000.
- Este método produce alias como *condor.pulento.1234@chinchilla.mail* o *puma.picado.6789@chinchilla.*
que no solo son únicos sino también parte de la identidad cultural chilena.
- Cada alias generado se almacena en la base de datos, y Postfix verifica la existencia de estos correos cuando llega un mensaje. Si el alias existe, el correo se procesa; de lo contrario, se rechaza.

Este enfoque para la generación de alias no solo asegura la creación de direcciones de correo electrónico fáciles de recordar y culturalmente relevantes, sino que también añade un toque de personalización y diversión al sistema.

3.3.3. Procesamiento y Registro de Logs de Postfix

Una función notable del backend es su capacidad para procesar y registrar los logs generados por Postfix (MTA). El sistema implementa un cron job que periódicamente lee los logs de Postfix, extrayendo información valiosa sobre los correos electrónicos redirigidos, incluyendo detalles sobre entregas exitosas y fallidas. Esta funcionalidad es vital para monitorear y analizar el flujo de correos electrónicos a través del sistema de proxy.

3.3.4. Exposición de Endpoints para el Frontend

El backend dispone de una serie de endpoints RESTful desarrollados con FastAPI (Figura 2), que permiten al frontend interactuar con el sistema. La implementación de estos endpoints es fundamental para la interactividad y la experiencia de usuario de la aplicación web. Estos endpoints están diseñados siguiendo los principios CRUD (Create, Read, Update, Delete), cubriendo un amplio espectro de funcionalidades:

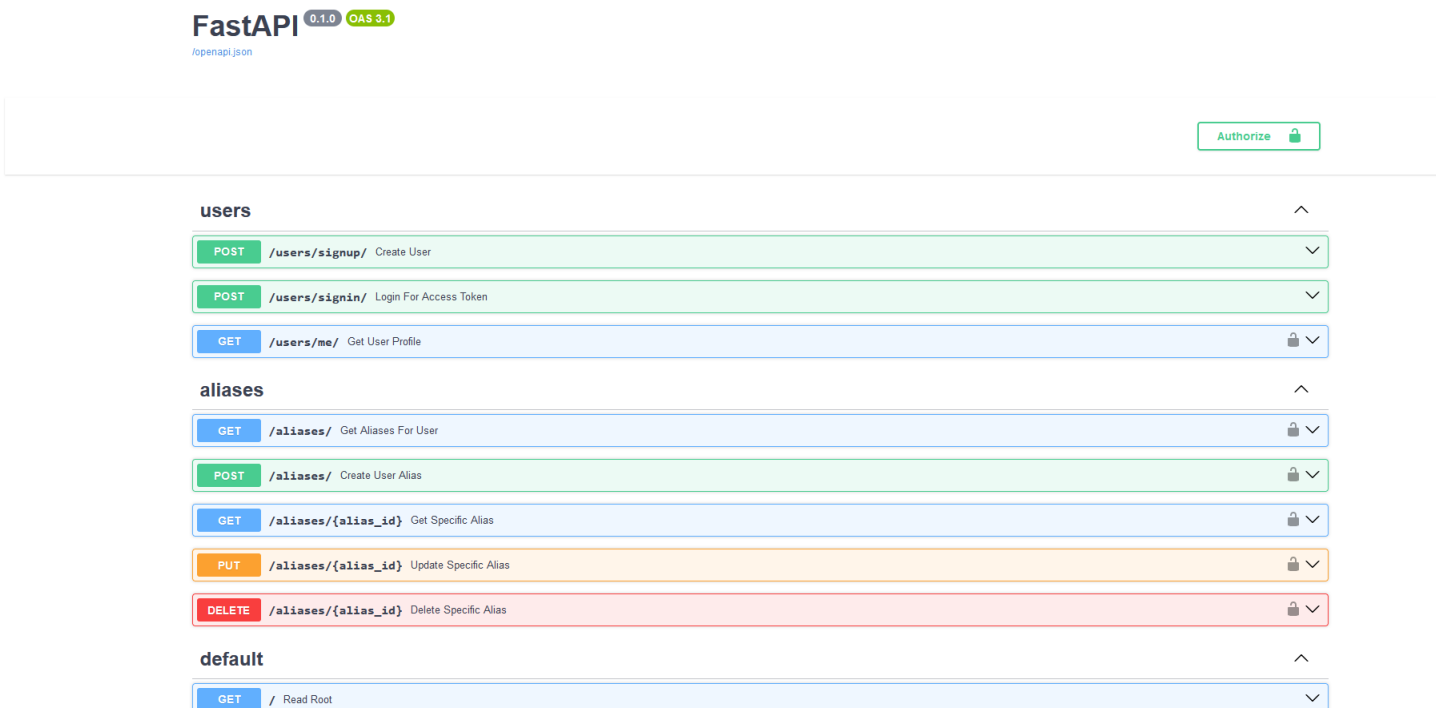

Figura 2: Vista de Backend con FastAPI

- **Endpoints para la Gestión de Usuarios:**
  - *Registro de Usuario (Create):* Habilita la creación de nuevas cuentas de usuario.
  - *Inicio de Sesión (Read):* Autenticación de usuarios y generación de tokens de acceso.
  - *Perfil de Usuario (Read/Update):* Permite a los usuarios acceder y modificar su perfil.
- **Endpoints para la Gestión de Alias:**
  - *Crear Alias (Create):* Permite a los usuarios registrar nuevos alias de correo electrónico aleatorio.
  - *Listar Alias (Read):* Proporciona una lista de todos los alias asociados a un usuario.
  - *Detalles de Alias Específico (Read):* Acceso a la información detallada de un alias particular.
  - *Actualizar Alias (Update):* Permite la modificación de los detalles de un alias existente.
  - *Eliminar Alias (Delete):* Facilita la eliminación de alias no deseados o innecesarios.

Estos endpoints son fundamentales para la funcionalidad de la aplicación, proporcionando las interfaces necesarias para la interacción eficiente entre el backend y el frontend. La implementación de estos endpoints enfoca en la seguridad, la eficiencia y la facilidad de uso, garantizando una experiencia de usuario fluida y segura.

La estructura de estos endpoints refleja un enfoque en la claridad, la mantenibilidad y la eficacia en la comunicación entre el backend y el frontend. Cada endpoint está diseñado para cumplir una función específica dentro del sistema, asegurando así que la aplicación sea modular, escalable y fácil de gestionar.

3.3.5. Seguridad y Autenticación de Usuarios

La seguridad es un aspecto primordial en el backend de la aplicación web, especialmente en lo que respecta a la gestión de sesiones y autenticación de usuarios. Se implementó un conjunto de métodos robustos y modernos para garantizar que solo los usuarios autorizados puedan acceder y modificar sus datos. A continuación, se describen los principales componentes y estrategias utilizadas:

- **Hasheo de Contraseñas:** En el sistema, las contraseñas no se almacenan como texto plano ni como hashes simples, sino que se emplea CryptContext de Passlib con el esquema "bcrypt", que automáticamente maneja un 'salt' para cada contraseña. Este 'salt', o valor aleatorio añadido al hash, protege las contraseñas contra ataques de diccionario y de fuerza bruta, ya que incluso contraseñas idénticas resultarán en hashes diferentes en la base de datos. Esta práctica de seguridad aumenta significativamente la protección de las cuentas de usuario frente a posibles brechas de datos.
- **Tokens JWT para Manejo de Sesiones:** El backend emplea JSON Web Tokens (JWT) para el manejo de sesiones de usuario. Cada token JWT es generado con una firma segura y un tiempo de expiración, lo que proporciona una forma confiable y escalable de mantener sesiones de usuario autenticadas. Los JWT ofrecen ventajas como la facilidad de uso entre diferentes dominios y plataformas, la capacidad de ser autocontenidos con toda la información necesaria y una reducción de la carga en el servidor al no requerir almacenamiento de estado de sesión. Sin embargo, también presentan desafíos como la dificultad de invalidarlos antes de su expiración y el riesgo de seguridad si no se manejan adecuadamente, especialmente en lo que respecta a la protección de la clave secreta utilizada para firmar los tokens y la vulnerabilidad a ataques de robo de tokens si no se implementan prácticas de seguridad robustas.
- **OAuth2PasswordBearer:** Se usa para la implementación del esquema de autenticación OAuth2, donde los tokens JWT son utilizados para autenticar las solicitudes del usuario. Este método asegura que cada solicitud al backend sea validada y autorizada apropiadamente.
- **Verificación y Autenticación de Usuarios:** El proceso de autenticación se realiza a través de la verificación de credenciales y la generación de tokens de acceso. Al iniciar sesión, se

valida la contraseña del usuario y, si es exitosa, se genera un token JWT que será usado para las subsiguientes solicitudes de la sesión.

- **Protección Contra Accesos No Autorizados:** Se implementan medidas de seguridad como la verificación de tokens en cada solicitud al backend y la validación de permisos para prevenir accesos no autorizados o malintencionados a la información del usuario.
- **Verificación de CAPTCHA:** Para el registro de nuevos usuarios, se verifica un token CAPTCHA utilizando la API de Turnstile de Cloudflare. Esto ayuda a proteger la aplicación contra bots y registros automatizados maliciosos.

En resumen, estas medidas aseguran la integridad y privacidad de los datos de los usuarios en el backend. La combinación de hashing de contraseñas, autenticación JWT y OAuth2 proporciona un marco de seguridad robusto y confiable para la aplicación.

3.4. Frontend

El frontend de la aplicación web de correo electrónico está desarrollado utilizando Next.js y React, proporcionando una experiencia de usuario moderna y eficiente. Este desarrollo se centra en tres páginas principales: Index, Login y Signup, cada una diseñada para cumplir una función específica dentro de la aplicación.

3.4.1. Páginas Principales

La aplicación cuenta con tres páginas principales:

1. **Signup**: Ofrece a los nuevos usuarios la posibilidad de registrarse. Necesita pasar por Captcha de Clodflare turnstile además de los campos Usuario, Email y Contraseña para la creación correcta de una cuenta (Figura 3).

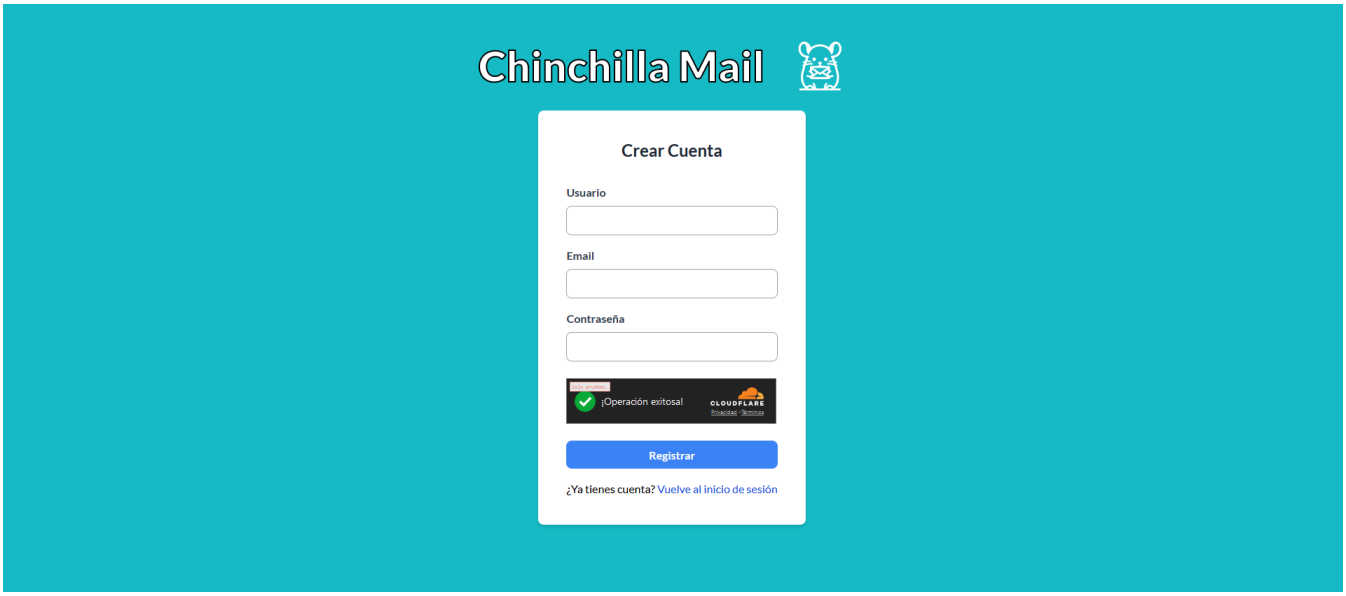

Figura 3: Vista de Registro de Cuenta

2. **Login**: Permite a los usuarios iniciar sesión en la aplicación (Figura 4).
3. **Index**: La página de inicio que presenta la funcionalidad principal de la aplicación (Figura 5).

3.4.2. Componentes Personalizados

Se crearon varios componentes personalizados para mejorar la reutilización y la abstracción (Figura 6):

- **AliasModal y DeleteAliasModal**: Para la creación y gestión de alias de correo electrónico, todo dentro de la misma página principal.
- **Botones y Toggles**: Para facilitar la interacción del usuario con la aplicación.

Figura 4: Vista de Inicio de Sesión

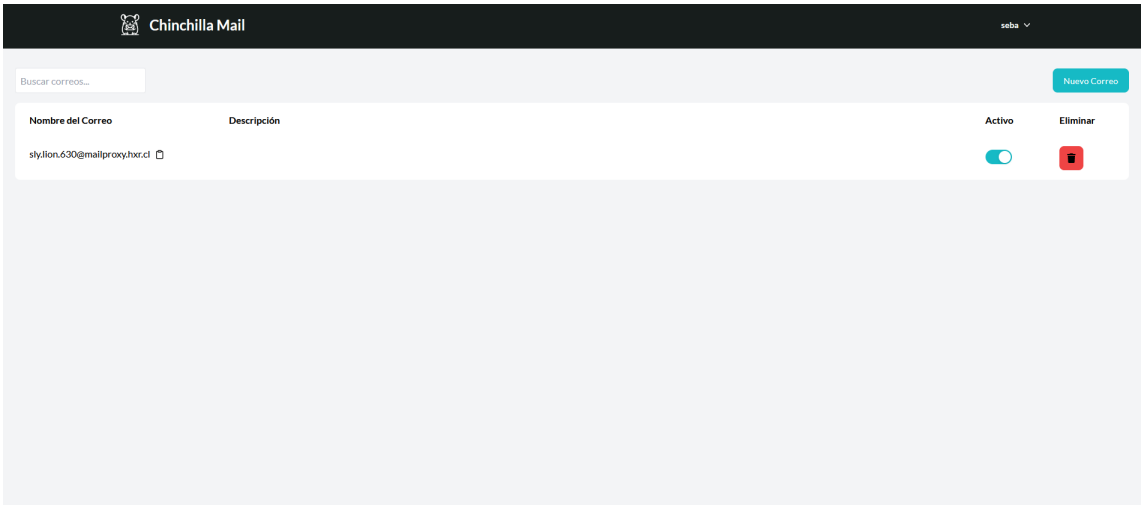

Figura 5: Vista de Inicio de Sesión

- **CustomDialog**: Una abstracción para crear contenido rápidamente y encapsularlo dentro de los modales.
- **Snackbars**: Se utiliza para mostrar notificaciones y mensajes de retroalimentación a los usuarios.

3.4.3. Gestión de Estados y Peticiones API

El manejo de estados y las peticiones API se realizan a través de @tanstack/react-query [15], lo que permite una gestión eficiente del estado del servidor en el lado del cliente. Se emplea Axios para realizar llamadas API, gestionando las operaciones relacionadas con usuarios y alias.

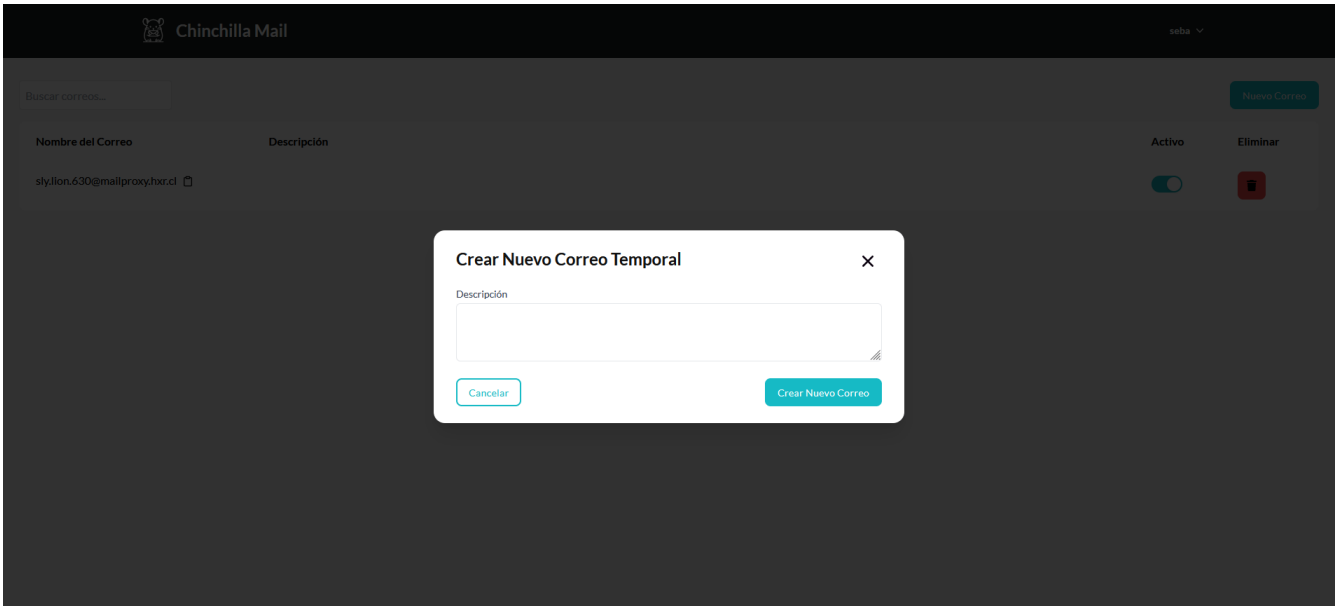

Figura 6: Vista de Modal para Creacion de Correo Temporal

3.4.4. Estilización y Diseño Responsivo

Tailwind CSS se emplea extensivamente para el diseño del frontend, asegurando que la aplicación sea visualmente atractiva y responsiva. La flexibilidad de Tailwind permite ajustar rápidamente los estilos para diferentes dispositivos y tamaños de pantalla.

3.4.5. Seguridad y Autenticación

Para la seguridad, se implementa un sistema robusto de autenticación. Se almacena localmente en el navegador el token JWT (JSON Web Token) obtenido durante el inicio de sesión para gestionar las sesiones de usuario y proteger las rutas y recursos de la aplicación.

3.5. Base de Datos

La base de datos de la aplicación web ha sido diseñada con un enfoque minimalista (Figura 7), buscando almacenar la menor cantidad de información posible, al mismo tiempo que proporcionando la funcionalidad necesaria para el sistema. A continuación, se detallan las tablas principales y sus atributos:

3.5.1. Tabla de Usuarios (users)

Esta tabla es esencial en la gestión de usuarios dentro del sistema y ha sido diseñada para almacenar la información crítica del usuario de manera segura y eficiente. Los campos incluidos en esta tabla son:

- *id:* Este es el identificador único para cada usuario en la base de datos. Se utiliza como clave

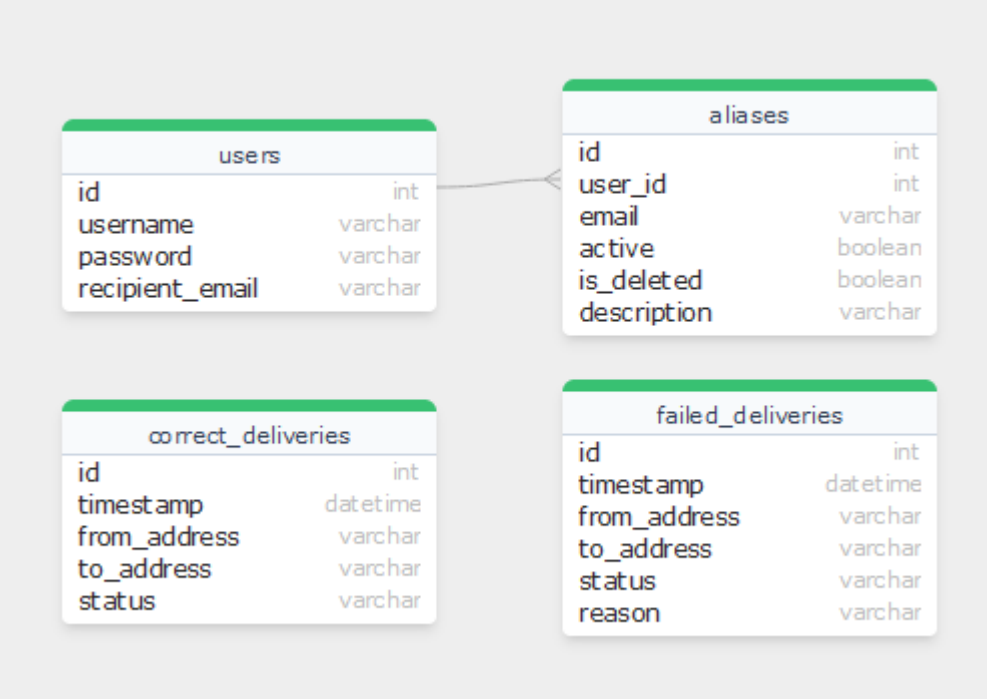

Figura 7: Diagrama de Base de Datos

primaria y es esencial para referenciar de manera única a cada usuario en el sistema.

- *username:* El nombre de usuario seleccionado por el usuario al crear su cuenta. Es una pieza clave en el proceso de autenticación, ya que se utiliza junto con la contraseña para el inicio de sesión. Este campo está indexado y marcado como único para garantizar que cada nombre de usuario sea distinto en el sistema.
- *password:* Almacena el hash de la contraseña del usuario. Para maximizar la seguridad, las contraseñas son hasheadas antes de su almacenamiento, lo cual evita que las contraseñas en texto plano estén expuestas en la base de datos. Esto es crucial para proteger la información de los usuarios en caso de una brecha de seguridad.
- *recipient_email:* Representa la dirección de correo electrónico principal del usuario. Este campo es utilizado para las comunicaciones esenciales con el usuario. Al igual que el nombre de usuario, este campo es único y está indexado, asegurando que cada dirección de correo electrónico esté asociada a un solo usuario en el sistema.

Inicialmente, se contempló la encriptación del campo *recipient_email* para proteger aún más la información del usuario en caso de una filtración de datos. Sin embargo, debido a las limitaciones en la capacidad de desencriptación de la imagen de Postfix seleccionada, esta característica fue descartada. La imagen de Postfix no ofrecía soporte para desencriptar los datos de manera que pudiera realizar el relay de correos de manera efectiva. Esta decisión destaca un área para el desarrollo futuro, donde una versión más personalizada del MTA podría permitir tal funcionalidad, aumentando la seguridad sin comprometer la operatividad del sistema de correo.

El diseño actual, aunque adaptado a las restricciones técnicas, continúa enfocándose en la protección de la privacidad del usuario y la eficiencia operativa, reflejando el compromiso del sistema con la seguridad de los datos del usuario.

3.5.2. Tabla de Alias (aliases)

La tabla de alias es un componente crucial para la gestión de las direcciones de correo electrónico temporales de los usuarios. Esta tabla permite a los usuarios crear y manejar múltiples aliases, mejorando así su privacidad y seguridad en línea. Los campos de esta tabla incluyen:

- *id:* Este campo sirve como identificador único para cada alias en la base de datos. Es la clave primaria de la tabla y permite la identificación y el manejo eficiente de cada alias individual.
- *user_id:* Este campo establece una relación entre cada alias y su usuario correspondiente. Almacena el identificador del usuario al que está asociado el alias. Esta relación es fundamental para garantizar que los alias sean gestionados y accedidos solo por los usuarios autorizados.
- *email:* Contiene la dirección de correo electrónico aleatoria del alias. Cada alias representa una dirección de correo única que los usuarios pueden utilizar en lugar de su dirección principal. Este campo es único para asegurar que no haya duplicados en el sistema.
- *active:* Este campo indica si el alias está actualmente activo. Un alias activo es aquel que puede recibir correos electrónicos, mientras que un alias inactivo no procesará correos entrantes. Este campo permite a los usuarios controlar la actividad de sus alias sin necesidad de eliminarlos.
- *is_deleted:* Marca si el alias ha sido eliminado. Este campo es importante para mantener un historial de los alias que han sido creados y luego eliminados por el usuario. Ayuda en la gestión y auditoría de los alias dentro del sistema.
- *description:* Proporciona una descripción opcional para cada alias. Esto permite a los usuarios asignar una etiqueta o una descripción a sus alias para facilitar su identificación y manejo.

Originalmente, se consideró la encriptación del campo *email* para los alias, con el objetivo de reforzar la privacidad y seguridad. Sin embargo, esta funcionalidad se descartó debido a las restricciones de la imagen de Postfix utilizada. Este detalle pone de manifiesto la importancia de un MTA más personalizable que podría permitir la encriptación y desencriptación al vuelo, una mejora significativa que se explorará en el trabajo futuro.

La tabla de alias, con su diseño actual, proporciona a los usuarios una herramienta poderosa para gestionar su identidad digital de manera efectiva, subrayando el compromiso del sistema con prácticas de privacidad sólidas y operatividad eficiente.

3.5.3. Tabla de Entregas Correctas (correct_deliveries)

La tabla de entregas correctas juega un papel vital en el seguimiento y análisis del flujo de correos electrónicos a través del sistema de relay. Al registrar las entregas exitosas de correos, esta tabla proporciona información valiosa sobre la eficacia del sistema. Los campos de esta tabla incluyen:

- *id:* Este campo actúa como un identificador único para cada registro de entrega correcta. Es la clave primaria de la tabla y facilita la identificación y referencia individual de cada entrega exitosa.
- *timestamp:* Almacena la marca de tiempo exacta en la que se completó la entrega del correo electrónico. Este campo es esencial para rastrear cuándo ocurrieron las entregas exitosas y para analizar el rendimiento del sistema a lo largo del tiempo.
- *from_address:* Contiene la dirección de correo electrónico del remitente del mensaje. Este campo es importante para identificar el origen de los correos electrónicos que pasan a través del sistema de relay.
- *to_address:* Registra la dirección de correo electrónico del destinatario del mensaje. Este campo es crucial para comprender a quiénes se están enviando los correos y para validar el éxito de las entregas a los destinatarios previstos.
- *status:* Indica el estado final de la entrega del correo electrónico. Normalmente este campo reflejará un estado de 'entregado' o similar, confirmando que el correo electrónico alcanzó su destino sin problemas.

La existencia de esta tabla en la base de datos es fundamental para mantener una auditoría precisa y detallada de las comunicaciones de correo electrónico exitosas. Proporciona una vista clara del rendimiento del sistema y ayuda a identificar posibles problemas en el flujo de correo electrónico. Además, el análisis de estos datos puede ser utilizado para mejoras continuas en la eficiencia, la fiabilidad del sistema y posterior análisis sobre el filtrado de emails.

3.5.4. Tabla de Entregas Fallidas (failed_deliveries)

La tabla de entregas fallidas es un componente esencial para comprender y analizar los problemas en la entrega de correos electrónicos. Al registrar los intentos fallidos, proporciona datos cruciales para identificar y solucionar las causas de estas fallas. Los campos de esta tabla incluyen:

- *id:* Actúa como un identificador único para cada registro de entrega fallida. Este campo es la clave primaria de la tabla y permite la identificación y seguimiento específico de cada incidente.
- *timestamp:* Almacena la marca de tiempo exacta del intento fallido de entrega. Este dato es vital para determinar cuándo ocurrieron los problemas y puede ser utilizado en el análisis de tendencias o en la identificación de problemas recurrentes.
- *from_address:* Registra la dirección de correo electrónico del remitente del mensaje. Este campo ayuda a identificar la fuente del correo electrónico que enfrentó problemas en la entrega.
- *to_address:* Contiene la dirección de correo electrónico del destinatario previsto. Proporciona información esencial sobre el destino final del mensaje y ayuda a entender si los problemas de entrega están relacionados con direcciones de destino específicas.
- *status:* Indica el estado de la entrega fallida, proporcionando una visión general del resultado del intento de entrega. Este campo es crucial para clasificar el tipo de problema que se produjo durante la entrega.
- *reason:* Ofrece una descripción de alto nivel de porque el correo fue rechazado actualmente solo 2 estados, la primera si fue rechazado porque el alias esta deshabilitado/eliminado o porque el correo al cual se trato realizar un relay nunca exisito en el sistema.

La tabla de entregas fallidas no solo ayuda a identificar y corregir problemas específicos relacionados con la entrega de correos, sino que también aporta información valiosa para mejorar continuamente la fiabilidad y eficacia del sistema de correo electrónico. Su diseño está orientado a proporcionar una comprensión completa de los desafíos enfrentados en el proceso de entrega de correos electrónicos, permitiendo así intervenciones más informadas y efectivas.

3.5.5. Justificación para la Doble Tabulación de Entregas

La arquitectura de la base de datos para un sistema de relay de correos electrónicos debe diseñarse con un enfoque en la captura precisa de datos y la facilidad de análisis de los mismos. En este contexto, la decisión de separar las entregas correctas y fallidas en dos tablas distintas se justifica por varias razones estratégicas y técnicas:

- **Claridad y Especificidad:** Separar los registros de entregas correctas y fallidas facilita la identificación y el diagnóstico de problemas específicos. Permite a los administradores del sistema y a los desarrolladores analizar rápidamente las tendencias en las entregas exitosas y las fallas sin necesidad de filtrar una única tabla grande, lo que puede ser ineficiente y

propenso a errores.

- **Optimización del Rendimiento:** Mantener tablas especializadas para diferentes tipos de eventos (entregas correctas y fallidas) permite optimizar las operaciones de la base de datos, como las consultas y los índices. Las tablas más pequeñas y enfocadas pueden ser indexadas y consultadas más rápidamente que una tabla general grande, mejorando el rendimiento del sistema.
- **Seguridad y Privacidad:** Esta separación refleja también una preocupación por la privacidad y la seguridad. Al almacenar las entregas fallidas separadamente, se reduce el riesgo de exposición de datos sensibles en caso de una brecha de seguridad. Las tablas de entregas correctas pueden contener información más sensible que puede requerir mayores medidas de protección.
- **Facilidad de Mantenimiento y Escalabilidad:** Con el crecimiento del sistema y el aumento en el volumen de correos electrónicos procesados, la separación permite una gestión más sencilla de la base de datos. Facilita la implementación de políticas de retención de datos y el escalado de los componentes de almacenamiento de manera independiente según las necesidades de cada tipo de dato.
- **Archivado de Datos Antiguos:** Tener las tablas separadas también abre las puertas a la implementación de políticas de retención de datos y el escalado de los componentes a través de un sistema de archivado para registros históricos para mantener la eficiencia operativa. Esta práctica puede permitir un acceso continuo a datos históricos para análisis y auditorías, mientras asegura que la gestión diaria de datos permanezca eficiente y acorde a las políticas de privacidad y retención de datos.
- **Análisis y Reporte Diferenciado:** Finalmente, esta dualidad en la tabulación permite generar reportes y análisis diferenciados para las partes interesadas, que pueden requerir información sobre la eficacia del sistema o detalles sobre los puntos de fallo y mejora. Proporciona una base de datos estructurada que puede ser utilizada para generar insights accionables y reportes específicos para diferentes necesidades.

En resumen, la utilización de dos tablas separadas para las entregas de correos electrónicos es una decisión de diseño que fortalece la funcionalidad, el rendimiento y la seguridad del sistema. Asegura que el sistema de relay de correos electrónicos sea no solo eficaz en su operación diaria, sino también robusto y preparado para el análisis y la mejora continua.

3.6. Docker

La implementación del sistema de proxy de correos electrónicos se realiza mediante Docker, proporcionando un despliegue simplificado y una gestión eficiente de los diferentes servicios. Se utiliza Docker Compose para orquestar la configuración de múltiples contenedores, cada uno responsable de una parte específica del sistema. A continuación, se detalla la configuración de cada servicio y su papel en la arquitectura general.

3.6.1. Dockerfiles y Configuración:

Los Dockerfiles para el backend, frontend y Postfix definen las imágenes base (Python para el backend, Node para el frontend y Postfix para como Mail Transfer Agent), establecen los directorios de trabajo, instalan las dependencias y exponen los puertos necesarios. Además, se copian los scripts de entrada y se otorgan permisos de ejecución para iniciar correctamente cada servicio.

3.6.2. Caddy Container

El servicio Caddy actúa como un servidor web y un proxy inverso. Utiliza la imagen ‘lucaslorentz/caddy-docker-proxy:ci-alpine‘ y se configura para escuchar en los puertos 80 y 443, manejando así las solicitudes HTTP y HTTPS. Los volúmenes montados aseguran la persistencia de datos y configuraciones. Caddy es fundamental para gestionar las conexiones entrantes y enrutarlas a los servicios apropiados del backend y frontend.

3.6.3. Backend Container

El contenedor del backend se construye desde el directorio ‘./backend‘. Se expone el puerto 8000 y se conecta a las redes internas y de Caddy. Este servicio depende de la base de datos y utiliza un archivo ‘.env‘ para la configuración del entorno. El backend proporciona la lógica de la aplicación y gestiona la interacción con la base de datos.

3.6.4. Frontend Container

El frontend se construye a partir del directorio ‘./frontend‘ y se expone en el puerto 3000. Al igual que el backend, se conecta a las redes internas y de Caddy y depende del backend para funcionar correctamente. Este servicio maneja la interfaz de usuario de la aplicación.

3.6.5. Base de Datos (PostgreSQL) Container

Utilizamos la imagen oficial de PostgreSQL y la configuramos para que se ejecute en la red interna. Se utilizan volúmenes para garantizar la persistencia de los datos. La base de datos es crucial para almacenar y gestionar toda la información del sistema.

3.6.6. Postfix Container

El servicio Postfix se configura para manejar el correo electrónico. Se construye a partir del directorio ‘./postfix‘ y se conecta a la red interna. Este servicio es responsable de procesar y reenviar los correos electrónicos, actuando como el núcleo del sistema de proxy de correos.

3.7. Postfix

El servicio Postfix es un componente integral del sistema de proxy de correos electrónicos, encargado de procesar y reenviar los mensajes. Para la implementación de Postfix, se utiliza la imagen ‘boky/postfix‘ de Docker, que ofrece una base sólida y amigable para las necesidades de la memoria.

3.7.1. Configuración y Personalización

La configuración del servidor Postfix en nuestro sistema se realiza mediante un conjunto de variables de entorno definidas en el archivo ‘.env‘. Estas variables influyen directamente en la configuración del archivo ‘main.cf‘, el cual es el archivo de configuración principal de Postfix. Estas variables permiten ajustar aspectos cruciales del servicio, asegurando tanto su funcionalidad como su seguridad. Detallamos a continuación algunas de las más importantes:

- *POSTFIX_message_size_limit* establece el tamaño máximo de los mensajes en bytes. En este caso, se configura un límite de 30 MB, lo que permite una flexibilidad adecuada para el manejo de correos electrónicos.
- *POSTFIX_myhostname* define el nombre de host del servidor Postfix. Este valor es crucial para la identificación del servidor en la red.
- *POSTFIX_mynetworks* especifica las redes que están autorizadas para enviar correos a través de este servidor. La configuración ‘0.0.0.0/0‘ abre el servidor a todas las redes, lo cual es adecuado para nuestro propósito de reenvío.
- *ALLOWED_SENDER_DOMAINS* limita los dominios que pueden enviar correos a través de este servidor. Esto se utiliza para restringir el uso del servidor a dominios conocidos y de confianza.
- *DKIM_AUTOGENERATE* habilita la generación automática de claves DKIM, lo que mejora la seguridad y autenticidad de los correos enviados desde el servidor.
- *virtual_alias_maps* y *virtual_alias_domains* son utilizados para configurar el mapeo de alias y dominios en Postfix, respectivamente, lo que es esencial para la seguridad del sistema permitiendo verificar que los emails que son procesados por el sistema sean pertenecientes a la base de datos.
- *POSTFIX_smtpd_recipient_restrictions* establece una serie de restricciones para los destinatarios de correo, lo que es crucial para evitar el abuso del servidor y garantizar que solo se entreguen correos a destinatarios autorizados.

Además de estas variables, se realizan otras configuraciones clave en Postfix mediante el script ‘install-pg-client.sh‘ al inicio del contenedor. Este script personaliza el archivo ‘master.cf‘ para deshabilitar las entregas locales y las submissions SMTP, fortaleciendo así la seguridad del servidor. Esto asegura que el servidor se enfoque exclusivamente en el reenvío de correos y previene el uso indebido del servidor por terceros.

En resumen, la configuración cuidadosa y detallada de Postfix a través de estas variables de entorno y scripts personalizados permite que el servidor funcione de manera eficiente y segura, alineado con los objetivos de nuestro sistema de proxy de correos electrónicos.

3.7.2. Script de Inicio Personalizado

El script ‘install-pg-client.sh‘ juega un rol crucial al inicio del contenedor de Postfix. Se ejecuta para instalar el cliente de PostgreSQL y aplicar las configuraciones necesarias en Postfix. Este script asegura que todas las dependencias requeridas estén presentes y facilita la conexión directa con la base de datos. La instalación de bibliotecas específicas permite que Postfix interactúe eficientemente con la base de datos PostgreSQL.

Además, este script tiene la responsabilidad de modificar el archivo *master.cf* de Postfix. Este archivo es esencial para la gestión de los servicios internos que son necesarios para el funcionamiento óptimo de Postfix. Una acción importante realizada por el script es la desactivación de las entregas locales y los servicios de submission SMTP. Este ajuste es fundamental para fortalecer la seguridad del sistema, evitando que terceros puedan enviar correos a los usuarios en caso de que obtengan acceso al contenedor.

En resumen, el script ‘install-pg-client.sh‘ no solo prepara el entorno de Postfix para su operación con la base de datos, sino que también optimiza la configuración de servicios internos para mejorar la seguridad y eficiencia del procesamiento de correos electrónicos.

3.7.3. Integración con PostgreSQL

Una característica clave de nuestra configuración es la integración de Postfix con PostgreSQL. Utilizando los scripts ‘recipients.cf‘ y ‘virtual.cf‘, generados a partir de plantillas y variables de entorno, para vincular Postfix con nuestra base de datos PostgreSQL y asi poder permitir que cada vez que un correo llegue se tenga que verificar si el destinatario existe en la base de datos y ademas verificar que el correo temproal intermediario también exista. Esto nos permite gestionar de manera eficiente las direcciones y alias de correo electrónico, así poder generar y utilizar distintas restricciones y reglas de reenvío.

3.7.4. Extensión de rsyslog

También fue necesario extender la configuración de rsyslog dentro del contenedor de Postfix para capturar y almacenar logs de correo electrónico en archivos *.log*. Estos logs son esenciales para el backend, ya que proporcionan los datos necesarios para analizar y almacenar información sobre las entregas de correos, tanto exitosas como fallidas, en la base de datos.

3.8. Extensión de Navegador

La extensión del sistema de proxy de correos electrónicos es una integración innovadora que mejora significativamente la accesibilidad y la facilidad de uso de la aplicación. En su estado actual, la extensión funciona incorporando la página web de la aplicación en un iframe, lo que permite a los usuarios interactuar con la aplicación directamente desde cualquier pestaña del navegador. Esta implementación aprovecha la responsividad del diseño web de la aplicación, asegurando que la experiencia del usuario sea consistente y fluida tanto en la extensión del navegador como en la web.

3.8.1. Trabajo Actual

El trabajo realizado hasta ahora se ha centrado en incrustar la interfaz web existente dentro de la extensión del navegador (Figura 8). Este enfoque garantiza que los usuarios puedan acceder y gestionar sus correos temporales con la misma funcionalidad que ofrecería el sitio web, pero con la comodidad de no salir de su navegador (Figura 9). El diseño responsivo de la página web asegura que la interfaz sea adaptable y funcional independientemente del tamaño o la resolución de la ventana del navegador.

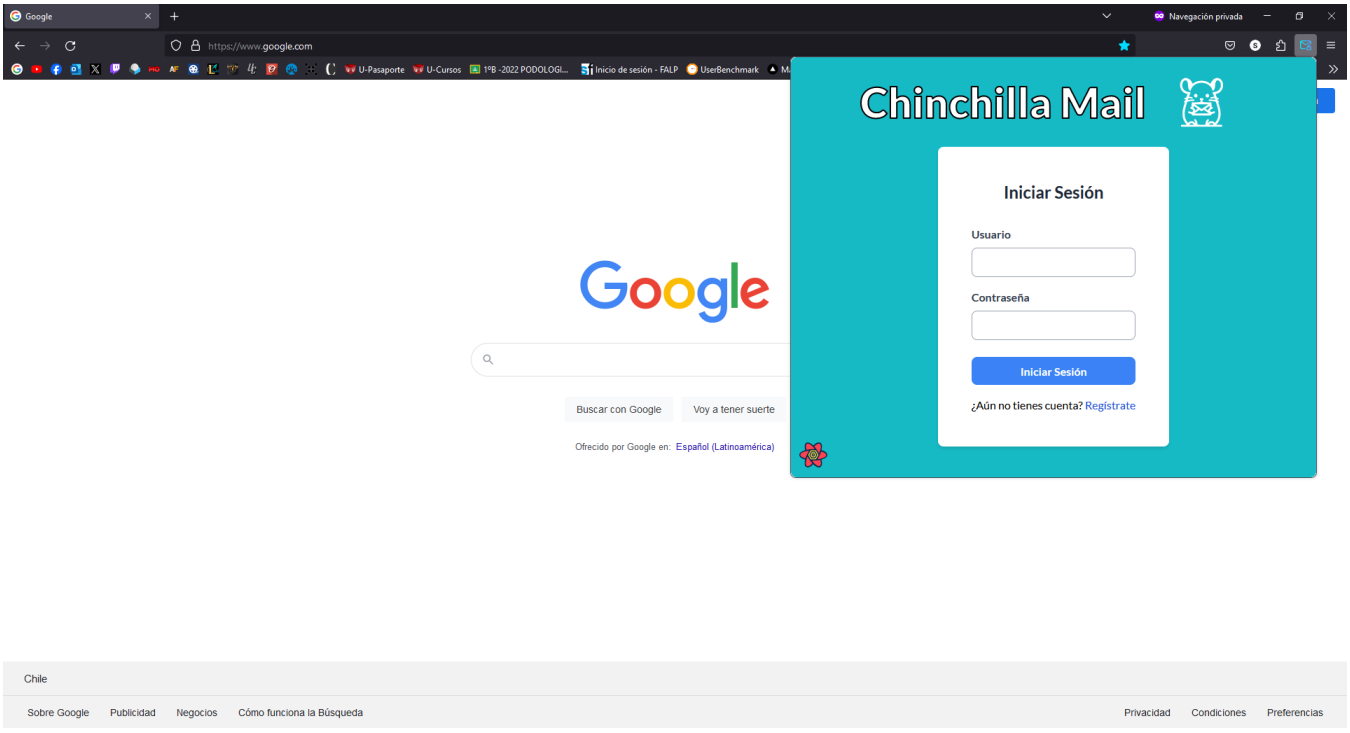

Figura 8: Vista de Login en Extensión

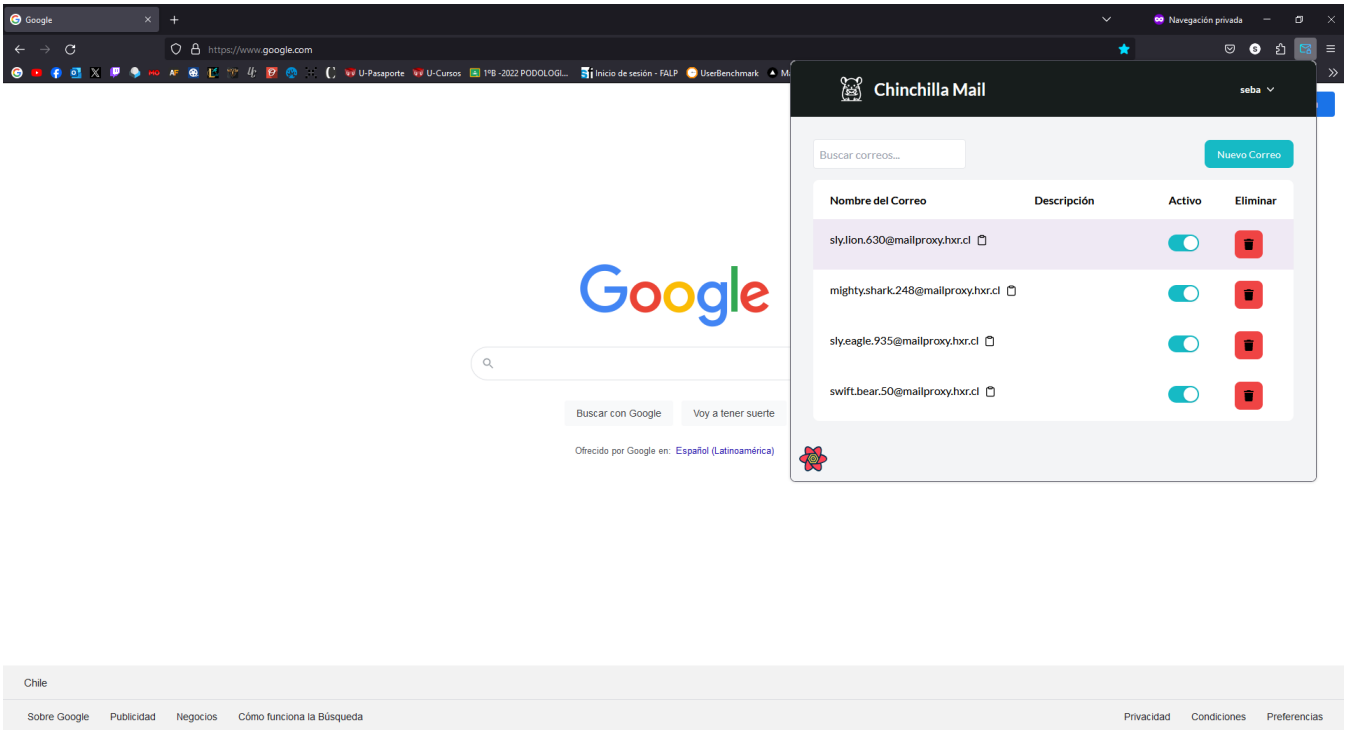

Figura 9: Vista de Index en Extensión

3.8.2. Trabajo Futuro

Mirando hacia el futuro, se espera poder tener una versión más dedicada de la extensión del navegador. Este desarrollo futuro debería centrarse en una interfaz específica para la extensión, que se conectará directamente con el backend del servicio. El objetivo es proporcionar una experiencia de usuario más rápida y cómoda, centrada principalmente en el manejo eficiente de los correos temporales.

Esta versión futura de la extensión permitirá a los usuarios realizar acciones clave, como la creación, gestión y eliminación de alias de correo electrónico, de manera más rápida y directa. La interfaz será optimizada para minimizar la carga y maximizar la eficiencia, eliminando elementos no esenciales y concentrándose en la funcionalidad central relacionada con los correos temporales. Además, esta extensión ligera permitirá una mayor integración con las funcionalidades del navegador, como menús contextuales y notificaciones, mejorando así la interacción del usuario con el sistema.

3.9. Despliegue, Configuración de Redes y Seguridad

En el sistema de proxy de correos electrónicos, la configuración de redes y las medidas de seguridad son aspectos críticos para garantizar tanto la funcionalidad como la protección de la información. A continuación, se detallan las prácticas implementadas en esta memoria.

3.9.1. Integración con Cloudflare

El uso de Cloudflare en el sistema desempeña un papel fundamental en varias áreas, incluyendo la seguridad y la gestión de DNS. Una característica destacada es el uso de Cloudflare Turnstile, un sistema de CAPTCHA que se utiliza para proteger la página de registro de la aplicación. Turnstile ayuda a prevenir el acceso automatizado y malicioso, garantizando que solo los usuarios legítimos puedan crear cuentas.

3.9.2. DNS y Protocolos de Seguridad

Cloudflare también se utiliza para gestionar los registros DNS y configurar los protocolos de seguridad del correo electrónico (Figura 10), como SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail) y DMARC (Domain-based Message Authentication, Reporting and Conformance). Estos protocolos son esenciales para mejorar la seguridad del correo electrónico, asegurando la autenticidad y la integridad de los mensajes enviados y recibidos.

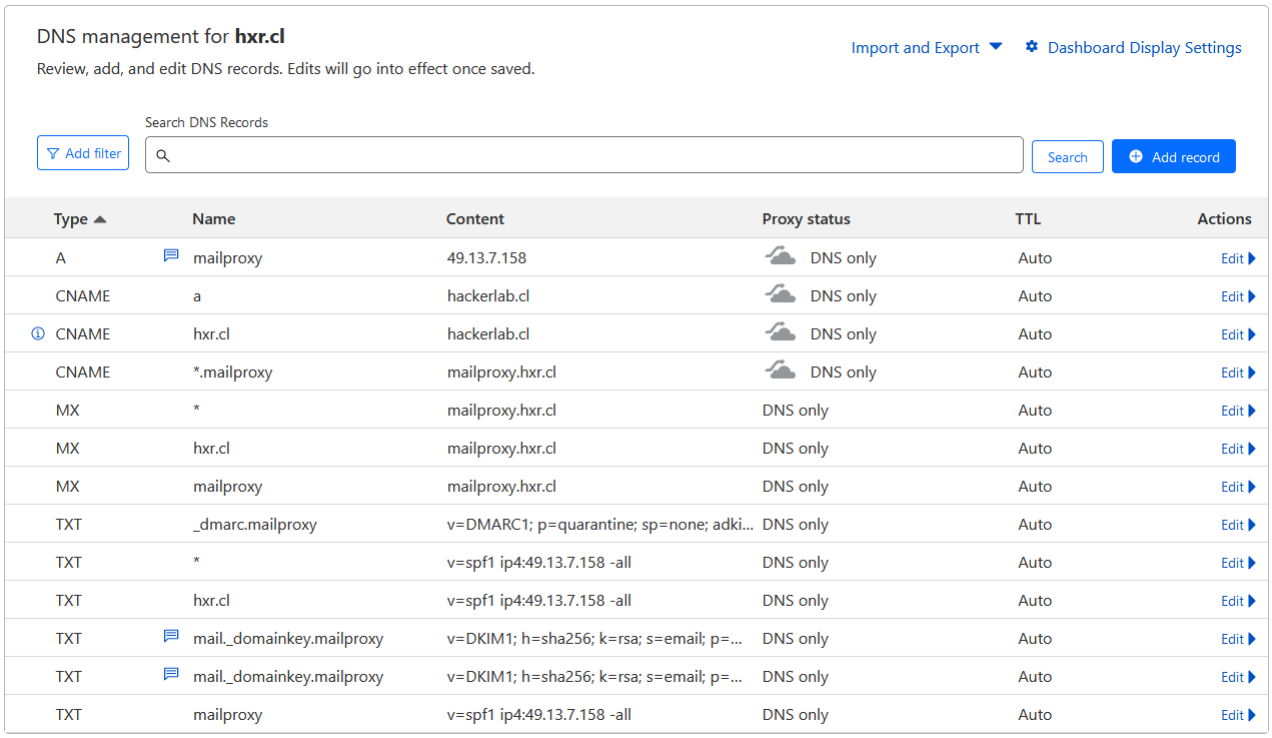

Figura 10: Configuración DNS en Cloudflare

3.9.3. Gestión de Puertos y Firewall

Para el despliegue del sistema en un servidor de Hetzner, se ha llevado a cabo una política estricta de gestión de puertos y firewall. Se han cerrado todos los puertos excepto aquellos esenciales para el funcionamiento del sistema, incluyendo el 22 (SSH), 443 (HTTPS), 80 (HTTP). Esto se hace para minimizar las vulnerabilidades y asegurar que solo se permitan las conexiones necesarias para la operación del sistema.

En particular, los puertos 587 y 465, comúnmente utilizados para conexiones SMTP seguras, han sido cerrados para evitar su uso indebido. Al cerrar estos puertos, se limita la capacidad de los actores maliciosos para enviar correos electrónicos no autorizados a través del sistema, mejorando así la seguridad general del servidor de correos.

La configuración de redes y las medidas de seguridad implementadas en el sistema de proxy de correos electrónicos reflejan un compromiso con la protección de la información y la integridad del sistema. El uso estratégico de Cloudflare para la gestión de DNS y CAPTCHA, junto con una gestión de puertos y firewall cuidadosa, contribuyen a crear un entorno seguro y confiable para la operación del sistema de correo electrónico.

3.10. Despliegue

3.10.1. Hetzner como Proveedor de Servicios en la Nube

Se optó por Hetzner [13] como proveedor de servicios en la nube debido a su equilibrio entre costo, rendimiento y seguridad. Hetzner proporciona una infraestructura robusta, ideal para alojar el servicio del sistema, y asegura una base confiable para su operación.

3.10.2. Configuración del Servidor

El servidor se configuró para satisfacer las necesidades específicas del sistema. Esto incluyó la asignación adecuada de recursos como CPU, memoria y almacenamiento, y la instalación de todas las herramientas y dependencias necesarias.

3.10.3. Uso de Docker para el Despliegue de Servicios

Docker se utilizó para desplegar los componentes del sistema (backend, frontend, Postfix, PostgresSQL) en contenedores separados. Esta estrategia facilita la gestión y escalabilidad de cada servicio y asegura su aislamiento y seguridad. Docker Compose orquesta la configuración de estos contenedores, proporcionando un despliegue coherente y eficiente.

3.10.4. Automatización y Scripts de Despliegue

Como fue mencionado en las subsecciones anteriores se utiliza un set de scripts de automatización para manejar la configuración inicial para cada uno de los contenedores, manejando actualizaciones y para su mantenimiento regular. Estos scripts minimizan los errores humanos y optimizan la operatividad del sistema inicial.

3.10.5. Accesibilidad y Transparencia del Sistema

Para garantizar la accesibilidad y fomentar la transparencia, el sistema completo de proxy de correos electrónicos está disponible públicamente a través de la página web `chinchillamail.cl`. Además, el código fuente y la documentación del proyecto se encuentran en un repositorio público en GitHub, accesible en `https://github.com/hackerlab-uchile/mail_relay`. Esto permite la revisión, el uso y las contribuciones de la comunidad, alineando el proyecto con los principios de código abierto y colaboración comunitaria.

3.10.6. Monitoreo y Mantenimiento Continuo

Durante el desarrollo y despliegue, el sistema se mantuvo bajo vigilancia constante para identificar y solucionar cualquier problema potencial. Esto incluyo monitorear el rendimiento del servidor, la salud de la base de datos y la funcionalidad del sistema de correos. Se buscó y desarrolló estrategias para el desarrollo regular para mantener el sistema actualizado y en óptimas condiciones.

3.10.7. Desafíos con la Lista Negra de Microsoft

Durante el despliegue y operación del sistema de proxy de correos electrónicos, existió un desafío significativo con la lista negra de Microsoft. Los correos electrónicos enviados hacia dominios de Microsoft, como Hotmail y Outlook, eran sistemáticamente rebotados. Este problema se atribuye a la presencia de nuestra infraestructura en la lista negra interna de Microsoft, una situación común para muchos servidores de correo nuevos o desconocidos.

A pesar de los intentos de resolver esta situación, incluyendo la comunicación con Hetzner y Microsoft, no se recibió una solución concreta dentro del marco de tiempo disponible para este proyecto. Esta situación ha limitado la capacidad del sistema para servir a los usuarios con correos electrónicos de Microsoft, una limitación importante dada la prevalencia de estos servicios de correo electrónico.

Este desafío subraya la importancia de considerar las políticas y prácticas de grandes proveedores de correo electrónico en el diseño y operación de sistemas de proxy de correo. También resalta la necesidad de estrategias de mitigación y adaptación en el futuro para asegurar la compatibilidad y funcionalidad completa del sistema.

3.11. Implicaciones de Seguridad ante Diferentes Niveles de Acceso

La seguridad de un sistema informático es un aspecto de constante evaluación, especialmente considerando la variedad de niveles de acceso que pueden tener diferentes actores, incluidos posibles atacantes. En la aplicación desarrollada, se han considerado distintos escenarios para mitigar los riesgos asociados a cada nivel de acceso.

3.11.1. Acceso a Logs de la Aplicación

En el nivel más básico, si un atacante obtiene acceso a los logs de la aplicación, encontrará que la información acerca de los correos electrónicos está hasheada. Esto se ha diseñado intencionalmente para proteger la identidad y los datos de los usuarios. Las tablas *correct_deliveries* y *failed_deliveries* contienen datos hasheados que proporcionan métricas valiosas sobre el tráfico de correos sin comprometer la privacidad de los usuarios.

3.11.2. Acceso a las Tablas de Usuarios y Alias

Un escenario de mayor riesgo es el acceso no autorizado a las tablas *users* y *aliases*. Actualmente, si bien las contraseñas están protegidas a través de hasheo, los correos electrónicos almacenados en la tabla de usuarios y las direcciones de alias no están encriptados. Esto significa que un atacante con acceso a estas tablas podría obtener las direcciones de correo electrónico reales de los usuarios y sus asociaciones con sus recpectivos aliases.

3.11.3. Encriptación y MTA

Una solución a futuro para este punto crítico de seguridad podría ser la implementación de la encriptación de direcciones de correo electrónico. Sin embargo, esto presenta un desafío técnico significativo ya que el MTA actual, imagen docker Boky/Postfix, no admite la desencriptación para el reenvío de correos. Es necesario desarrollar o adaptar un MTA que pueda manejar la encriptación y desencriptación sin perder su funcionalidad principal como relay. Este sería un área clave para el desarrollo futuro, mejorando sustancialmente la seguridad sin sacrificar la funcionalidad.

3.11.4. Ventajas de la Configuración Actual de Postfix

Es importante destacar que la imagen actual de Postfix empleada en la solución está configurada exclusivamente para funcionar como relay. Esto implica que, incluso si un tercero o un administrador obtiene acceso completo al servicio de Postfix, no serían capaces de acceder al contenido de los correos electrónicos. Este diseño de relay cerrado ofrece una capa adicional de seguridad, ya que el contenido del correo permanece inaccesible y se preserva la confidencialidad de la comunicación de los usuarios. Sin embargo, es importante tener en cuenta que un administrador con acceso completo al sistema podría, en teoría, modificar la configuración de Postfix para registrar o interceptar correos electrónicos. Por ejemplo, podrían alterar la configuración para que los correos se almacenen temporalmente o se reenvíen a otro destino, lo que podría permitir el acceso al

contenido.

3.11.5. Rol del Administrador del Sistema

El administrador del sistema tiene un amplio acceso y control sobre la aplicación, lo que incluye la capacidad de acceder a logs, bases de datos y configuraciones de sistema. Es crucial que los administradores sigan las mejores prácticas de seguridad y el monitoreo constante de la actividad del sistema para prevenir y detectar cualquier acceso no autorizado o malintencionado.

3.11.6. Conclusión

La protección de los datos de los usuarios es una prioridad en el diseño y funcionamiento de la aplicación de proxy de correos. A pesar de que las medidas actuales proporcionan una defensa sólida en varios niveles, el desarrollo futuro debe centrarse en mejorar aún más la seguridad de los datos, especialmente en lo que respecta a la encriptación de correos electrónicos y la funcionalidad del MTA. Con la implementación de estas mejoras, el sistema no solo mantendrá su integridad operativa, sino que también fortalecerá la confianza de los usuarios en el servicio proporcionado.

4. Evaluación

La evaluación del sistema de proxy de correos electrónicos es esencial para determinar su eficacia en cumplir con los objetivos propuestos, centrados en la funcionalidad, usabilidad y capacidad de redirigir correos electrónicos eficientemente. La evaluación de usabilidad se realizó mediante encuesta en forma de guía sobre el uso de la aplicación web a 17 personas, no relacionadas con el área de la computación.

Para la realización de la evaluación de usuarios se les solicito a los usuarios realizar las siguientes tareas guiadas mediante un formulario de Google[3] durante un periodo libre de tiempo.

Tareas Guiadas:

1. *Paso 1: Inicio de Sesión y Registro en Chinchilla Mail*
2. *Paso 2: Creación de un Alias de Correo*
3. *Paso 3: Uso del Alias en Servicios Externos*
4. *Paso 4: Administración de Alias*
5. *Paso 5 (OPCIONAL): Verificación de Correos Recibidos*

4.1. Evaluación de Funcionalidad y Eficacia

Descripción: La evaluación se enfocó en la capacidad del sistema para redirigir correos electrónicos a servicios como Gmail, asegurando que estos no sean marcados como spam o rebotados. *Métodos de Evaluación:*

- Monitoreo del índice de correos electrónicos exitosamente redirigidos versus correos marcados como spam o rebotados.
- Análisis de registros y reportes del sistema para identificar patrones en la entrega y recepción de correos.

Resultados Obtenidos:

- De los correos procesados, 27 fueron exitosamente redirigidos a los destinatarios finales.
- Se registraron 49 correos rebotados o fallidos. De estos, 47 casos fueron debido a direcciones de correo que no existen (la mayoría aparentemente generados por bots) y 2 casos debido a que los aliases ya habían sido deshabilitados.
- Los patrones identificados en los registros del sistema mostraron que la mayoría de los problemas de entrega se relacionaban con direcciones de correo incorrectas o dominios no reconocidos.
- La tasa de éxito en la redirección de correos, excluyendo los dominios mencionados, fue aproximadamente del 93 % (27 exitosos de un total de 29 correos procesados).

Conclusiones: La alta tasa de éxito en la redirección de correos electrónicos demuestra la funcionalidad y eficacia del sistema. Esto sugiere que la eficacia del sistema es considerablemente alta cuando se filtran posibles ataques de bots o correos de prueba. Los pocos casos de correos marcados como spam o rebotados proporcionan una oportunidad de mejora, especialmente en la gestión de autenticación y en la verificación de la exactitud de las direcciones de correo.

4.2. Pruebas de Usabilidad

Descripción: Evaluación de la usabilidad del sistema por medio de pruebas con usuarios reales.
Métodos de Evaluación:

- Implementación de pruebas de usabilidad con un grupo de control que utilizará el sistema durante un período de dos semanas.
- Distribución de cuestionarios post-uso para recopilar comentarios y opiniones de los usuarios sobre la experiencia del sistema.

Resultados Obtenidos (Figura 11):

- Los usuarios reportaron una experiencia generalmente positiva en términos de la facilidad de registro e inicio de sesión, con un promedio de 4.2 sobre 5 en satisfacción.
- La creación y gestión de aliases de correo fue valorada con una media de 3.7 sobre 5, indicando una experiencia satisfactoria pero con margen de mejora.
- La mayoría de los comentarios resaltaron la simplicidad y la funcionalidad efectiva del sistema, aunque algunos usuarios sugirieron la necesidad de una interfaz más intuitiva y guías de usuario detalladas.

Conclusiones: Los resultados de las pruebas de usabilidad muestran una recepción positiva del sistema en términos de facilidad de uso y eficiencia. Las sugerencias y comentarios de los usuarios proporcionan valiosas perspectivas para futuras mejoras, especialmente en la necesidad de agregar una página dedicada a explicar los beneficios y el uso de correos temporales.

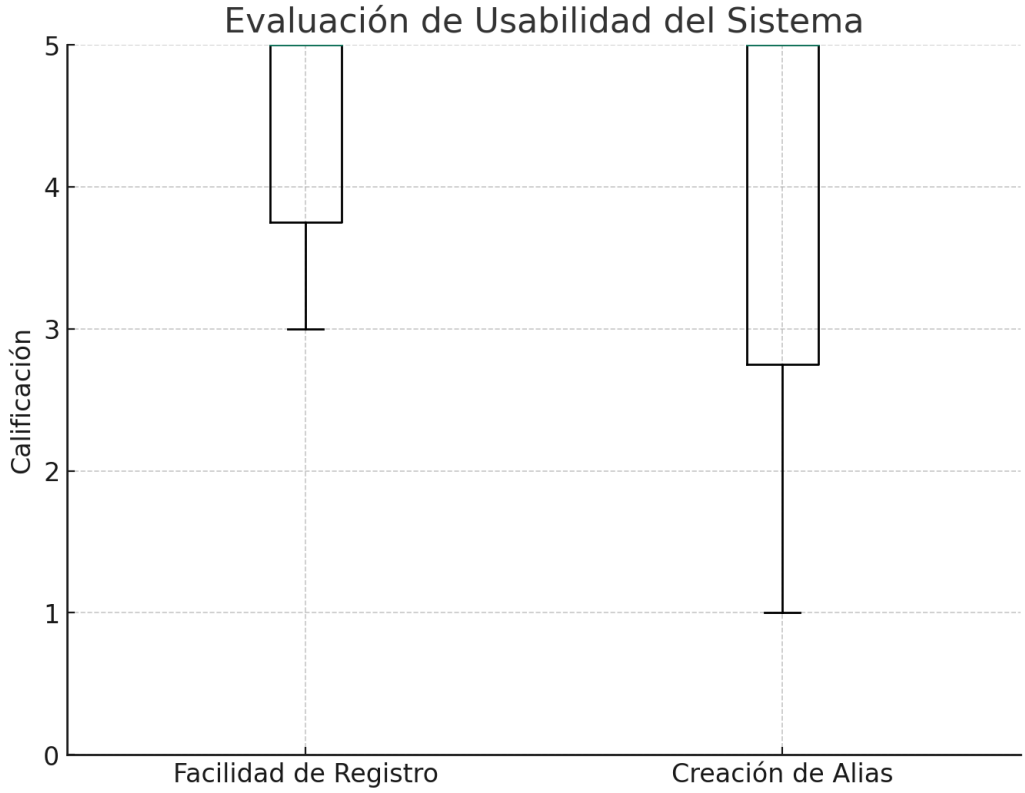

Figura 11: Evaluación de Usabilidad del Sistema

4.3. Análisis de Adopción y Satisfacción

Descripción: Este análisis busca comprender el grado de adopción del sistema de proxy de correos electrónicos por parte de los usuarios y su satisfacción general con el sistema. *Métodos de Evaluación:*

- Análisis de las tasas de adopción y uso continuo del sistema por parte de los usuarios, basado en su intención de uso futuro.
- Evaluación de la satisfacción de los usuarios a través de los resultados del cuestionario, enfocándose en su experiencia general con el sistema.

Resultados Obtenidos (Figura 12):

- **Tasa de Adopción:** La tasa promedio de adopción, basada en la intención de uso futuro del sistema, fue de 3.58 sobre 5. Esto indica una aceptación moderada, con algunos usuarios mostrando un fuerte interés en continuar utilizando el sistema.
- **Satisfacción del Usuario:** La satisfacción general de los usuarios con el sistema fue valorada en promedio con 4.0 sobre 5. Este resultado sugiere una recepción positiva, destacando la efectividad y la utilidad percibida del sistema.

Conclusiones: Los resultados demuestran una adopción y satisfacción general positivas entre los

usuarios. Sin embargo, también indican áreas de oportunidad para mejorar la claridad y la facilidad de uso, lo cual podría incrementar aún más la tasa de adopción. Estos hallazgos son cruciales para las futuras mejoras y estrategias de implementación del sistema.

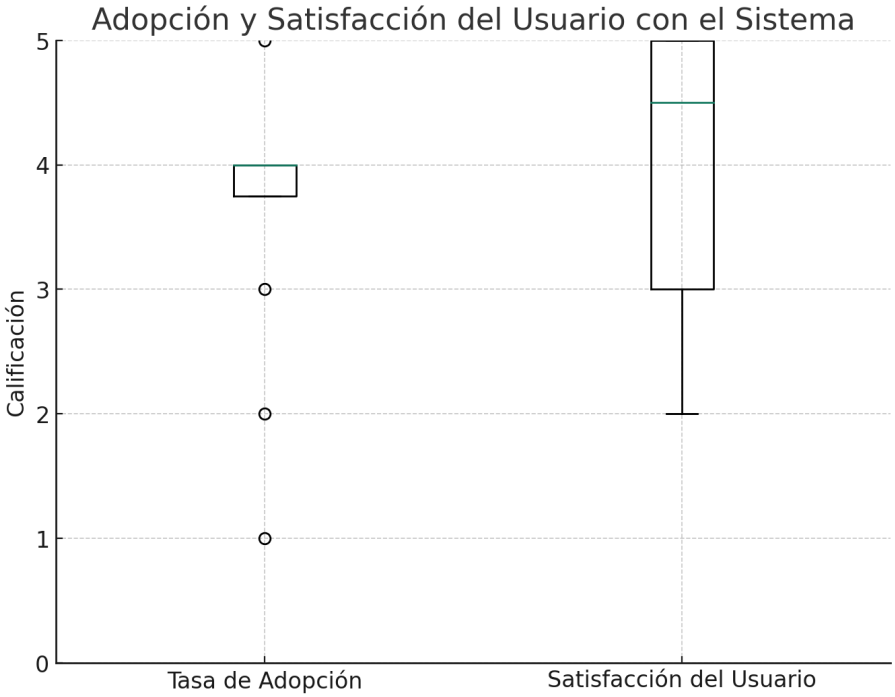

Figura 12: Evaluación de Adopción y Satisfacción del Sistema

5. Conclusiones

5.1. Resumen del Trabajo Realizado

Este proyecto ha desarrollado un sistema de proxy de correos electrónicos que ofrece una solución de fácil despliegue, abriendo estudios sobre filtraciones sin exponer información sensible y extensible para el manejo de la comunicación por correo electrónico. La aplicación se centra en la privacidad y seguridad del usuario, permitiendo la creación y gestión de correos temporales. A lo largo de este trabajo se abordaron varios aspectos clave:

- *Diseño y Desarrollo del Backend:* El backend de la aplicación, desarrollado con tecnologías como FastAPI y SQLAlchemy, se encarga de la inicialización de la base de datos, el procesamiento de logs de Postfix, y la exposición de endpoints RESTful para la interacción con el frontend.
- *Implementación del Frontend:* Utilizando Next.js y React, se creó una interfaz de usuario que es moderna, eficiente y responsiva, con páginas principales como Index, Login y Signup.
- *Base de Datos:* Se optó por un diseño minimalista, enfocado en almacenar la menor cantidad de información privada posible, con tablas como usuarios, alias y registros de entregas de correos.
- *Uso de Docker:* El despliegue del sistema se realizó utilizando Docker, lo que permite un despliegue simplificado y eficiente.
- *Configuración de Postfix:* Se configuró Postfix para el manejo eficiente y seguro de los correos electrónicos, incluyendo la personalización de su script de inicio y la integración con PostgreSQL.
- *Extensión de Navegador:* Se implementó una extensión de navegador, que actualmente incrusta la página web en un iframe, mejorando la accesibilidad y usabilidad.
- *Configuración de Redes y Seguridad:* Se integró el sistema con Cloudflare para la gestión de DNS y la implementación de protocolos de seguridad.
- *Despliegue en Servidor de Hetzner:* Se eligió Hetzner como proveedor de servicios en la nube, configurando el servidor para satisfacer las necesidades del sistema, incluyendo la gestión de puertos y el firewall.

Este trabajo representa un avance significativo no solo en poder realizar estudios acerca la detección de filtraciones de emails. Si no también en la gestión de la comunicación por correo electrónico, ofreciendo una solución que combina la eficiencia, la seguridad y la privacidad. La aplicación desarrollada puede ser una herramienta valiosa para el estudio futuro, la gestión de correos temporales y la protección de la privacidad del usuarios chilenos.

5.2. Recuento de Objetivos Alcanzados y No Alcanzados

Al realizar un recuento de los objetivos establecidos para el desarrollo del sistema de proxy de correos electrónicos, podemos destacar los logros alcanzados y reconocer las áreas que requieren más trabajo o que no se cumplieron según lo planeado.

5.2.1. Objetivo General

El objetivo general de desarrollar y poner en marcha un sistema comunitario para la prevención, detección y seguimiento de filtraciones de correos electrónicos se ha alcanzado de manera satisfactoria. El sistema proporciona un proxy de correos temporales y se encuentra operativo, aunque aún está en proceso de evaluación para futuros estudios sobre la privacidad de los correos en Chile.

5.2.2. Objetivos Específicos

1. *Investigación de Sistemas Existentes:* Se ha cumplido este objetivo al investigar y analizar diferentes sistemas de proxy de correos, lo que permitió obtener un conocimiento sólido para el desarrollo del sistema propuesto.
2. *Diseño de la Base de Datos:* El diseño e implementación de una base de datos preliminar minimalista se ha realizado con éxito, garantizando la eficiencia, seguridad y privacidad de los datos, aunque falta poder tener mas datos para poder analizar si efectivamente el sistema puede determinar y proveer información valiosa para el estudio de filtraciones de emails.
3. *Desarrollo del Backend:* Se ha logrado desarrollar un backend robusto y seguro que gestiona eficientemente la lógica de negocio y el procesamiento de datos.
4. *Construcción del Frontend:* El frontend del sistema ha sido construido y ofrece una experiencia de usuario interactiva y accesible, aunque hay espacio para mejoras en términos de usabilidad y diseño.
5. *Extensión de Navegador:* Se ha desarrollado una extensión de navegador, aunque actualmente es una versión preliminar y aun no se tiene acceso desde las tiendas de los navegadores, se puede acceder a el por medio del repositorio público y se espera como trabajo a futuro tener una interfaz más específica y dedicada, ademas de poder publicarlo oficialmente tanto para chrome y firefox.
6. *Integración de Componentes:* La comunicación entre el frontend, backend y base de datos ha sido integrada y asegurada exitosamente.
7. *Dockerización del Sistema:* Todos los componentes del sistema han sido dockerizados, facilitando su despliegue y promoviendo la accesibilidad y mantenibilidad.
8. *Puesta en Marcha y Disponibilidad Pública:* El sistema ha sido lanzado y está disponible para el público, cumpliendo con el objetivo de accesibilidad y facilidad de uso.

Conclusión del Recuento de Objetivos: El recuento de los objetivos muestra un éxito considerable en la mayoría de las áreas, con algunos aspectos, como la extensión del navegador y el diseño

del frontend, que aún pueden ser mejorados. El sistema cumple con su propósito principal y sienta las bases para futuros estudios y desarrollos relacionados con la privacidad del correo electrónico en Chile. Las lecciones aprendidas durante este proyecto ofrecen valiosas perspectivas para la mejora continua y la innovación en el campo de la seguridad del correo electrónico.

5.3. Lecciones Aprendidas

El desarrollo del sistema de proxy de correos electrónicos ha sido un proceso lleno de aprendizajes valiosos, tanto en términos técnicos como en la gestión y planificación del proyecto. A continuación, se resumen algunas de las lecciones más importantes aprendidas a lo largo de este trabajo:

5.3.1. Importancia de la Planificación y Diseño Preliminar

Una de las lecciones cruciales fue la importancia de una planificación y diseño preliminares exhaustivos. La estructura y funcionalidad del sistema se beneficiaron enormemente de un enfoque detallado en las etapas iniciales, que ayudó a anticipar y mitigar problemas potenciales y a establecer una base sólida para el desarrollo.

5.3.2. Valor de la Investigación y Análisis de Sistemas Existentes

La investigación y análisis de los sistemas de proxy de correos existentes proporcionaron insights valiosos para el diseño y desarrollo del sistema. Este enfoque permitió identificar las mejores prácticas, así como las limitaciones de los sistemas existentes, lo que influyó de manera significativa en las decisiones de diseño y funcionalidad.

5.3.3. Desafíos de la Integración de Tecnologías

El proyecto implicó la integración de varias tecnologías y herramientas, como FastAPI, Docker, SQLAlchemy y React. Navegar por los desafíos de esta integración fue una experiencia de aprendizaje importante, resaltando la necesidad de una comprensión profunda de cómo diferentes tecnologías pueden trabajar juntas de manera eficiente.

5.3.4. Trabajar con Postfix y sus Limitaciones

Uno de los mayores desafíos fue trabajar con Postfix, especialmente al utilizar una imagen existente de este MTA. Aqui aparecen limitaciones en la personalización de este mismo debido al tiempo y a las restricciones inherentes a la imagen seleccionada. Esta experiencia subrayó la importancia de considerar soluciones personalizadas frente a soluciones preexistentes, especialmente en un área tan crítica como el manejo de correos electrónicos.

5.3.5. Importancia de la Seguridad y Privacidad desde el Inicio

El proyecto reforzó la importancia de considerar la seguridad y la privacidad desde las primeras etapas de desarrollo. Las decisiones tomadas en cuanto a la gestión de datos y la arquitectura del sistema tuvieron un impacto significativo en la seguridad y la privacidad general del sistema.

5.3.6. Gestión y Resolución de Problemas

A lo largo del proyecto, nos encontramos con varios desafíos y problemas técnicos. Aprender a gestionar y resolver estos problemas de manera efectiva fue una parte esencial del proceso, mejorando nuestras habilidades de resolución de problemas y toma de decisiones.

5.4. Trabajo a Futuro

El desarrollo del sistema de proxy de correos electrónicos ha sentado las bases para una serie de mejoras y extensiones en el futuro. Estas mejoras no solo aumentarán la funcionalidad y eficiencia del sistema, sino que también fortalecerán su seguridad y usabilidad.

5.4.1. Mejoras en el Frontend

El frontend actual, a pesar de ser funcional y eficiente, presenta oportunidades de mejora en varios aspectos críticos para realzar la usabilidad y el diseño. Estas mejoras no solo buscan enriquecer la interacción del usuario con el sistema, sino también fortalecer la seguridad y la accesibilidad del mismo.

- *Interfaz de Usuario y Experiencia del Usuario (UX):* La prioridad será mejorar la interfaz de usuario para hacerla más intuitiva y atractiva. Esto incluye el rediseño de elementos de la interfaz, la implementación de una navegación más fluida y la adaptación del diseño para garantizar una mayor responsividad y accesibilidad. Además de incluir una página principal cuyo objetivo sea informar sobre los beneficios de los correos temporales y su uso.
- *Vista de Opciones para el Usuario:* Una actualización clave será la incorporación de una vista de opciones dedicada para los usuarios. Esta vista permitirá a los usuarios administrar sus cuentas de manera más eficiente, incluyendo funcionalidades como la eliminación de cuentas, la modificación de ajustes de privacidad y la personalización de preferencias de correo.
- *Integración de Sign-In sin Contraseña (Passwordless Sign-In):* Un trabajo que quedo pendiente durante el desarrollo fue implementar un sistema de sign-in sin contraseña, lo que aumentaría la seguridad y la comodidad para los usuarios. Esta tecnología permitirá a los usuarios acceder a sus cuentas sin la necesidad de recordar contraseñas, utilizando métodos alternativos como códigos de acceso únicos enviados a sus correos electrónicos o dispositivos móviles.
- *Recuperación de Contraseña:* Un aspecto crucial para mejorar la experiencia del usuario es la implementación de un sistema de recuperación de contraseñas. Esta funcionalidad a diferencia del Sign-In sin Contraseña, permitirá a los usuarios recuperar y cambiar las contraseñas del acceso a sus cuentas de manera eficiente en caso de olvido o pérdida de sus credenciales.
- *Desarrollo de Características Adicionales:* También se podria explorar la adición de nuevas características que enriquezcan la experiencia del usuario, como la personalización avanzada de la interfaz, opciones de filtrado de correos y alertas de seguridad mejoradas.

5.4.2. Desarrollo Avanzado de la Extensión de Navegador

La extensión de navegador actual, que actualmente utiliza un iframe para incrustar la página web, por lo que seria mucho mejor tener una extensión dedicada a reemplazar la aplicación web. El objetivo es crear una versión más ligera y dedicada que permita la gestión rápida y cómoda

de correos temporales, conectándose directamente con el backend del servicio. Esta nueva versión ofrecería una experiencia de usuario más optimizada y centrada en la gestión eficiente de los correos.

5.4.3. Trabajo en un MTA más Personalizable

El desarrollo o la extensión de un Agente de Transferencia de Correo (MTA) personalizable representa un desafío significativo pero esencial para el avance del sistema de proxy de correos electrónicos. Este esfuerzo permitirá abordar las necesidades específicas del sistema y proporcionará un control más completo sobre el manejo y procesamiento de los correos electrónicos.

- *Flexibilidad y Control Mejorado:* Un MTA personalizado permitirá una mayor flexibilidad en términos de configuración y opciones de manejo de correos. Esto incluye la capacidad de definir reglas específicas para el enrutamiento y procesamiento de correos, adaptándose a las necesidades cambiantes de los usuarios y del entorno de correo electrónico.
- *Encriptación de Correos Electrónicos:* Un aspecto crucial del desarrollo será la capacidad de almacenar correos electrónicos de forma segura utilizando encriptación. Esto asegurará que los correos almacenados en el sistema sean inaccesibles para terceros no autorizados, aumentando la privacidad y seguridad de los usuarios.
- *Desencriptación al Recibir Correos:* Junto con la encriptación, el MTA personalizado deberá ser capaz de desencriptar los correos electrónicos al momento de la recepción. Esto permitirá que el sistema mantenga su funcionalidad de relay, redirigiendo correos de manera segura y eficiente mientras protege la información confidencial.
- *Optimización para Funcionar como Relay:* El MTA deberá estar optimizado para funcionar eficientemente como un sistema de relay, manejando una gran cantidad de correos electrónicos redirigidos sin comprometer el rendimiento ni la seguridad.
- *Desarrollo Continuo y Adaptabilidad:* El MTA personalizable deberá ser diseñado con un enfoque en el desarrollo continuo y la adaptabilidad, permitiendo la incorporación de nuevas tecnologías y estándares de seguridad conforme evolucionen las necesidades y desafíos del entorno de correo electrónico.
- *Integración con la Infraestructura Existente:* Finalmente, cualquier desarrollo o extensión del MTA deberá ser integrado de forma coherente con la infraestructura existente del sistema de proxy de correos electrónicos, asegurando una transición suave y una operatividad consistente.

5.4.4. Encriptación y Seguridad de Datos Mejorada

En línea con el objetivo anterior, una prioridad será mejorar la encriptación y la seguridad de los datos almacenados. Esto incluiría el desarrollo de métodos para encriptar los correos electrónicos almacenados de manera que, incluso si un tercero no autorizado obtuviera acceso a la base de datos, no pudiera obtener información útil. La encriptación robusta y la gestión segura de claves

serán esenciales para esta mejora.

5.4.5. Expansión y Escalabilidad del Sistema

Finalmente, se buscará expandir y escalar el sistema para soportar un mayor número de usuarios y una gama más amplia de funcionalidades. Esto podría incluir la integración con más servicios de correo electrónico, la mejora de las capacidades de análisis y seguimiento de correos, y la optimización del rendimiento general del sistema.

Bibliografía

[1] *AnonAddy*. Sitio web. Recuperado el 27 de abril de 2023, de https://anonaddy.com/.

[2] *ChinchillaMail*. Sitio web. Recuperado el 22 de enero de 2024, de https://github.com/hackerlab-uchile/mail_relay.

[3] *Encuesta de usabilidad Chinchilla Mail*. Sitio web. Recuperado el 22 de enero de 2024, de https://docs.google.com/forms/d/e/1FAIpQLScsSURgwL_O0YJ4vWQiinO9JJ9JmvJlHF7OMOaXLnHrQvbNXg/viewform.

[4] *POP Protocol*. Sitio web. Recuperado el 28 de junio de 2023, de https://www.javatpoint.com/pop-protocol.

[5] *Repositorio Github ChinchillaMail*. Sitio web. Recuperado el 22 de enero de 2024, de https://anonaddy.com/.

[6] *SimpleLogin*. Sitio web. Recuperado el 27 de abril de 2023, de https://simplelogin.io/.

[7] *What is the Simple Mail Transfer Protocol (SMTP)?* Sitio web. Recuperado el 28 de junio de 2023, de https://www.cloudflare.com/learning/email-security/what-is-smtp/.

[8] *¿Qué es un bot de rastreador web?* Sitio web. Recuperado el 28 de junio de 2023, de https://www.cloudflare.com/es-es/learning/bots/what-is-a-web-crawler/.

[9] *Cost of a data breach 2022*. Sitio web. Recuperado el 26 de abril de 2023, de https://www.ibm.com/reports/data-breach, 2022.

[10] *Estafas a empresas por e-mail mediante suplantación de identidad*. Sitio web. Recuperado el 08 de julio de 2023, de https://www.interpol.int/es/Delitos/Delincuencia-financiera/Estafas-a-empresas-por-e-mail-mediante-suplantacion-de-identidad-BEC-
s.f.

[11] *Firefox Relay*. Sitio web. Recuperado el 25 de abril de 2023, de https://relay.firefox.com/, s.f.

[12] *Guerrilla Mail*. Sitio web. Recuperado el 25 de abril de 2023, de https://www.guerrillamail.com/, s.f.

[13] *Hetzner Cloud Server*. Sitio web. Recuperado el 14 de diciembre de 2023, de https://www.hetzner.com/cloud, s.f.

[14] *iCloud Hide My Email*. Sitio web. Recuperado el 25 de abril de 2023, de https://support.apple.com/es-es/guide/icloud/mme38e1602db/1.0/icloud/1.0, s.f.

[15] *TanStack Query*. Sitio web. Recuperado el 14 de diciembre de 2023, de https://tanstack.com/query/latest, s.f.

[16] A. Melnikov, Ed. y Ed. B. Leiba: *Internet Message Access Protocol (IMAP) - Version 4rev2*.

[17] Chile, CNN: *BancoEstado confirma filtración de cuentas y contraseñas de 1.400 clientes*. 2019. https://www.cnnchile.com/tecnologias/bancoestado-filtracion-datos-cuentas-contrasenas-claves_20190404/.

[18] Hu, Hang, Peng Peng y Gang Wang: *Understanding the Security Management of Global Third-Party Android Marketplaces*. arXiv preprint arXiv:1711.06654, 2017. https://arxiv.org/abs/1711.06654.

[19] Jansson, K. y R. von Solms: *Phishing for phishing awareness*.

[20] Kitterman, S.: *Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1*.

[21] Klensin, J.: *Simple Mail Transfer Protocol*. (5321), 2008. https://www.rfc-editor.org/rfc/rfc5321.html, RFC 5321.

[22] M. Kucherawy, Ed. y Ed. E. Zwicky: *Domain-based Message Authentication, Reporting, and Conformance (DMARC)*.

[23] Mailmeteor: *What is a proxy email address?* Sitio web. Recuperado el 25 de abril de 2023, de https://mailmeteor.com/glossary/proxy-email.

[24] Market Research, Worldwide Independent Network of: *Privacidad de la Información digital*. 2021. https://chile.activasite.com/estudios/estudio-mundial-3/.

[25] presidencia, Ministerio Secretaria general de la: *Ley 19628 Sobre Protección de la Vida Privada*. Biblioteca del Congreso Nacional, 1999. https://www.bcn.cl/leychile/navegar?idNorma=141599&idVersion=2020-08-26.

[26] presidencia, Ministerio Secretaria general de la: *Qué se hace con los datos privados de los chilenos*. La Tercera, 2019. https://www.latercera.com/reportajes/noticia/

se-los-datos-privados-los-chilenos/669843/.

[27] Rebollo, Clara: *Los ciberataques para secuestrar datos se duplicaron en los seis últimos meses*. D. El Pais, 2022. https://elpais.com/tecnologia/2022-08-18/los-ciberataques-para-secuestrar-datos-se-duplicaron-en-los-seis-ulti
html.

[28] Sheffer, Y., R. Holz y P. Saint-Andre: *Updated Transport Layer Security (TLS) Server Identity Check Procedure for Email-Related Protocols*. RFC 7817, RFC Editor, 2016. https://www.rfc-editor.org/rfc/rfc7817, RFC 7817.

[29] T. Hansen, D. Crocker y P. Hallam-Baker: *DomainKeys Identified Mail (DKIM) Service Overview*.

[30] The Radicati Group, INC.: *Email Statistics Report, 2021-2025*. https://www.oberlo.com/statistics/how-many-people-use-email.