UNIVERSIDAD NACIONAL AUTÓNOMA DE NICARAGUA

UNAN – León

Facultad de Ciencias y Tecnología

Departamento de Computación

Comparativa entre las características y el rendimiento de las Suites de Correo Electrónico Open-Xchange, Zimbra y Kopano, ejecutadas en entornos virtuales

Tesis para optar al título de

INGENIERO EN TELEMÁTICA

Presentado por:

Br. Jason Noel Areas Lanuza.

Br. Axel Smith Woolridge Hernández.

Br. Erwin Antonio Sandoval.

Tutor:

M.Sc. Denis Leopoldo Espinoza Hernández.

León, Agosto 2023.

"A LA LIBERTAD POR LA UNIVERSIDAD"

UNIVERSIDAD NACIONAL AUTÓNOMA DE NICARAGUA

UNAN – León

Facultad de Ciencias y Tecnología

Departamento de Computación

Comparativa entre las características y el rendimiento de las Suites de Correo Electrónico Open-Xchange, Zimbra y Kopano, ejecutadas en entornos virtuales

Tesis para optar al título de

INGENIERO EN TELEMÁTICA

Presentado por:

Br. Jason Noel Areas Lanuza.

Br. Axel Smith Woolridge Hernández.

Br. Erwin Antonio Sandoval.

Tutor:

M.Sc. Denis Leopoldo Espinoza Hernández.

León, Agosto 2023.

"A LA LIBERTAD POR LA UNIVERSIDAD"

Resumen

En la actualidad el correo electrónico es un medio de comunicación cada vez más popular. Al ser extremadamente económico y fácil de usar, es también un medio para el comercio electrónico. Además de ser usado por la mayoría de las empresas alrededor del mundo. Existen diferentes maneras de implementar un servidor de correo electrónico, desafortunadamente no todas las empresas cuentan con recursos para comprar o asesorarse bien sobre que suite de correo es la indicada para resolver sus necesidades.

Hoy en día la implementación de Suite de Correos dependerá mucho de la facilidad en su instalación ya que algunas soluciones son multiplataforma y otras solo funcionan en una sola distribución de SO y los requerimientos mínimos necesarios.

Debido a esto, se propuso la siguiente solución al problema que consta del análisis y rendimiento de 3 Suites de correo con diversas características a fin de demostrar que Suite se adecua más a las necesidades de cada empresa comprendiendo estabilidad, seguridad, manejo de spam, almacenamiento en nube, video llamadas y chats. Para ello implementaremos cada una de las suites en un entorno virtual controlado en el cual podremos realizar diversas pruebas a fin de demostrar sus ventajas y desventajas en cada uno de los aspectos antes descritos.

Dedicatoria

Me gustaría dedicar esta Tesis a Dios quien ha sido mi guía, fortaleza y su mano de fidelidad y amor han estado conmigo hasta el día de hoy. mi Abuela y Tía Abuela: Esmeralda y Briceida Roiz (ambas Q.E.P.D) quienes con su amor, paciencia y esfuerzo me han permitido llegar a cumplir hoy un sueño más, gracias por inculcar en mí el ejemplo de esfuerzo y valentía, de no temer las adversidades porque Dios está conmigo siempre. A toda mi familia porque con sus oraciones, consejos y palabras de aliento hicieron de mí una mejor persona y de una u otra forma me acompañan en todos mis sueños, metas y todo ello con una gran dosis de amor y sin pedir nunca nada a cambio.

Br. Jason Noel Areas Lanuza

Hoy, al alcanzar este logro en mi vida académica, quiero expresar mi más profundo agradecimiento a dos pilares fundamentales que han guiado mi camino. A ti, mamá, por tu amor incondicional, tu apoyo constante y tus sacrificios incansables que han hecho posible cada paso que doy. Tu ejemplo de perseverancia y cariño son mi inspiración para seguir adelante.

A los valiosos profesores de la UNAN León, les agradezco por compartir su conocimiento y experiencia con nosotros. Han sido faros en nuestro viaje educativo, guiándonos con sabiduría y paciencia. Cada lección que nos han brindado ha sido una fuente de crecimiento y enriquecimiento.

Este logro no solo es mío, sino también de quienes han creído en mí y han contribuido a mi desarrollo. A todos ustedes, mi gratitud sincera y mi compromiso de seguir adelante con la educación que he recibido aquí.

Br. Axel Smith Woolridge Hernández

Mi tesis la dedico con todo mi amor y cariño a mi madre, porque me dio la fortaleza necesaria para salir siempre adelante pese a las dificultades, por colocarme en el mejor camino, iluminando cada paso de mi vida, y por darme la salud y la esperanza para terminar este trabajo.

A toda mi familia especialmente a mi hermana Julma Sandoval quien me ha servido de ejemplo en todo mi camino de preparación profesional y ha estado conmigo en todo momento a mis tías y mi abuela que han sido sostén y apoyo en mis esfuerzos de superación profesional y por último a todas las personas que han creído en mí.

Br. Erwin Antonio Sandoval

Agradecimientos

A Dios, por iluminar nuestras vidas, porque nos ama e impulsa a ser cada día mejores personas.

A nuestros Padres por ser los ejemplos vivos de superación y amor incondicional, porque gracias a sus esfuerzos y confianza plena, hoy vemos realizados nuestros sueños.

A nuestros docentes por habernos brindado su entrega incondicional, su tiempo, amistad y por cada gesto de solidaridad, permitiendo nuestro crecimiento como personas y profesionales.

Índice de contenidos

1. Introducción

El correo electrónico ha demostrado ser el medio de comunicación más rápido y confiable de nuestro tiempo. Desde empresas hasta particulares, todos confiamos en los correos electrónicos debido a la conveniencia que ofrecen. Si alguna vez se preguntó cómo las computadoras envían estos mensajes aparentemente simples a través de la red.

Hay principalmente dos componentes de software en el corazón de la comunicación por correo electrónico, a saber, el servidor de correo y el cliente de correo. El servidor de correo es responsable de transmitir correos electrónicos de un nodo a otro en una red, normalmente Internet. Y el cliente permite a los usuarios recuperar estos correos electrónicos.

La comunicación interna y externa de una institución es de suma importancia, debido a que es la forma en que fluye la información en las diferentes áreas del organigrama, así mismo es el medio por el cual se dan a conocer estrategias, directrices o normas que se utilizan para alcanzar objetivos que lleven a la organización a lograr sus metas y rentabilidad deseada. Esta investigación se enfoca en analizar el uso de 3 herramientas en las que podría fluir la comunicación interna de una empresa.

Si se combina un dominio, suite correo profesional y una imagen atrayente en un portal de Internet es muy posible lograr una buena identidad en medio del universo del ciberespacio. Es perfecto para las PYMES, ya que les da mayor prestigio, sensación en ser emprendedores y es una motivación para que la compañía crezca.

Los correos de este tipo están mucho más libres de spam, por lo que su espacio de almacenamiento queda mucho más liberado para usos prácticos. Es perfecto para llevar a cabo el llamado marketing social, el cual es de gran utilidad para que los profesionales puedan darse a conocer en el mercado de recursos humanos.

El correo corporativo no se topará con todo el tráfico del correo gratuito, y por lo tanto es más rápido de entregarse a clientes y proveedores. En los correos de este tipo se pueden crear “alias” y grupos de trabajo, tal como sucede en redes sociales al estilo WhatsApp. Son más seguros y fáciles de proteger contra ataques de hackers. Por eso, son el modo predilecto de comunicación en instituciones estatales o de seguridad.

Todo lo antes dicho es apenas una muestra de las ventajas de una suite de correo profesional. Se trata de un modo de comunicación con mejor imagen, más seguridad y velocidad de envío.

1.1. Antecedentes

Róger Antonio Arteaga Sandoval (2012) en su tesis para optar al título de Ingeniero en Telemática titulada **"Instalación y Configuración de un Servidor de Correo Electrónico con Open-Xchange Server y sus protocolos con seguridad"** realiza la instalación del sistema operativo Univention Corporate server ya que este facilita el manejo e implementación de Open Xchange como la herramienta de almacenamiento y administración del correo electrónico además de las herramientas de seguridad como el protocolo TLS y la implementación de una autoridad certificadora.

Padilla Cevallos, Henrry Rolando (2012), quien realizó la: "**Propuesta de Investigación, análisis e implementación de un servidor de virtualización dedicado para integrar un servidor de correo Zimbra** virtualizado con un servidor multitarea Zentyal físico como controlador de dominio, Firewall y Proxi utilizando herramientas como tecnologías de Software libre. Esta investigación tuvo como objetivo analizar e implementar servidores Linux a nivel de infraestructura en la empresa Movidatos que ofrezcan beneficios como lo son dominio corporativo el cual tiene la función de registrar todos los respectivos usuarios como sus contraseñas y tener un registros de los equipos en el dominio para una mejor organización, bloqueo de páginas web para tener un control de acceso a nivel de internet y establecer políticas de seguridad e integridad de las funciones internas de la empresa.

Trabajo realizado en el año 2011, a cargo del **MS.c Aldo René Martínez** titulado **Configuración y Administración de Open-Xchange Server bajo la plataforma Linux.** Esta investigación tuvo como objetivo Habilitar un sistema colaborativo en la Facultad de Ciencias que proporcione una plataforma para el trabajo en grupo de docentes y administrativos. Una vez implementado se promoverá entre los docentes del Departamento el trabajar en grupo, explicando las ventajas que este implique.

1.2. Planteamiento del problema

La expansión de Internet como medio de difusión masiva, ha traído grandes ventajas a la vida cotidiana, el acceso a la información ahora es más ágil y transparente, las limitaciones espaciales no son ya un impedimento para compartir información y acceder a los recursos; del mismo modo Internet se ha convertido en una importante fuente de aprendizaje para las personas que lo utilizan como recurso de estudio autodidacta.

En nuestro país, la mayoría de las empresas que existen son pequeñas y medianas, y no cuentan con suficiente presupuesto para recursos informáticos, Así como la escases de personal calificado que realice las debidas asesorías y sugerencias en el área informática de las empresas existentes. Por ello es que se necesita un análisis para determinar cuál suite de correo se adecua a sus necesidades y presupuestos.

Pregunta general:

- ¿Cómo desarrollar una comparativa de rendimiento de Suites de Correo Electrónico Open-Xchange, Zimbra y Kopano, con el fin de brindar la mejor opción para las distintas empresas?

Preguntas específicas:

- ¿Qué procedimientos se deben seguir para la instalación y configuración de las suites de correo electrónico Open-Xchange, Zimbra y Kopano?
- ¿Cómo identificar las ventajas y desventajas de las suites de Correo Open-Xchange, Zimbra y Kopano?
- ¿Cuál de las suite de correo Open-Xchange, Zimbra y Kopano se adecua mejor a las necesidades de las empresas actuales?

1.3. Justificación

Esta idea nace con el fin de minimizar rendimiento y costos de implementación como una solución para el envío de correos electrónicos y comunicación entre los usuarios de una institución.

Usualmente las empresas usan correos de dominios populares como Google, Outlook sin tomar en cuenta que la seguridad de su información es primordial, por ello algunas instituciones implementan sus propios servicios de correo para así obtener mayor seguridad en el envío de su información ya sea porque tengan un mejor manejo de información o incluso costos más económicos que tener una plataforma con funciones limitadas un ejemplo de ellos son los bancos, diseñan sus propios servicios debido a la información tan delicada que manejan de sus clientes y así también la disponibilidad en el sentido que muchas veces grandes servicios de correo sufren filtración de contraseñas o caídas en sus servidores lo que ocasiona retardos en la entrega de información y muchas empresas por su naturaleza necesitan estar conectadas todo el tiempo.

Uno de los principales objetivos es mostrar información relevante sobre como gestionan la seguridad, el anti-spam y almacenamiento de archivos entre las diferentes suites de correo. Además de sus desventajas que puedan presentar con la interacción de múltiples usuarios al mismo tiempo y la escalabilidad de estas.

Seleccionamos la suite Zimbra porque tiene una plataforma personalizable con la finalidad de intercambiar correos, citas, contactos y archivos. Además de poseer aplicación móvil. Open-Xchange ha sido una plataforma de mensajería instantánea y software colaborativo gratuito y de código abierto que ha venido creciendo constantemente desde su fundación en 2008 esta misma nos ofrece diferentes servicios que son utilizados por diferentes compañías de renombre es por ello que es una de las seleccionadas para la elaboración de este documento debido a su alta escalabilidad, constante soporte e integración con otros servicios similares a este y Kopano por ser una suite moderna que brinda mensajería y video llamadas, así mismo posee una interfaz muy amigable para el usuario y no requiere de muchos recursos para su implementación, incluso posee aplicación web y escritorio

.

2. Objetivos

2.1. Objetivo general

- Realizar una comparativa entre las características de las Suites de Correo Electrónico Open-Xchange, Zimbra y Kopano, ejecutadas en entornos virtuales.

2.2. Objetivos específicos

- Describir los pasos para instalar y configurar las suites de correo Open-Xchange, Zimbra y Kopano en un entorno virtualizado.
- Comparar los protocolos y características soportadas en las suites de correo Open-Xchange, Zimbra y Kopano,
- Comprobar los aspectos de seguridad implementados en las suites de correo Open-Xchange, Zimbra y Kopano.

3. Marco Teórico

3.1. Correo Electrónico

El Correo Electrónico, también llamado E-MAIL (Electronic Mail), es una forma de enviar correo, mensajes o cartas electrónicas de un ordenador a otro. Tanto la persona que envía el correo electrónico, como la persona que lo recibe, deben tener una cuenta de correo en INTERNET.

Al enviar un correo electrónico, puede ser cuestión de minutos que llegue a su destino, sea cual sea el lugar del mundo donde se encuentre el destinatario del mensaje. El mensaje electrónico pasa de un servidor a otro. Cada servidor que recibe un mensaje comprueba la dirección y lo envía por la ruta correcta a otro servidor. Este proceso se repite hasta que el mensaje llega al servidor de destino, entonces se almacena en el buzón electrónico correspondiente (espacio de disco destinado a almacenar el correo electrónico de un usuario de dicho servidor). Sin embargo, con el correo tradicional suele ser cuestión de días, semanas e incluso meses.

Las características del E-MAIL que añaden más funcionalidad son:

- Es posible organizar el correo en CARPETAS. Si el volumen de correo recibido es grande, será necesario almacenar ese correo por temas, por usuarios, etc. Sería algo parecido a almacenar ficheros en directorios.
- Es posible la RETRANSMISIÓN DE MENSAJES que nos llega hacia otras direcciones de correo.
- Lo normal en los sistemas actuales de correo, es la posibilidad de dar REPLICA a un mensaje que nos ha llegado.
- Consiste en responder a un mensaje basándonos en el que nos ha llegado, tomando datos de este.

Hay muchas más características que dan mayor funcionalidad a un sistema de correo electrónico, pero estas son las más habituales. Además, dichas posibilidades dependen del software de correo electrónico usado en cada caso.

Aspectos del correo electrónico

El correo electrónico, es una de las funciones de Internet más utilizadas en la actualidad, cualquier persona que tenga acceso a internet le permite enviar y recibir mensajes entre emisor y receptor cuando estos han acordado el intercambio. Es uno de los servicios más utilizados debido a que facilita las comunicaciones en cualquier momento y a cualquier parte. Se basa en el protocolo TCP/IP y su esquema de conexión es asíncrono, es decir, no requiere establecer una conexión entre emisor y receptor para transmitir. Por lo tanto, al enviar un mensaje se requiere que el receptor revise su correo electrónico para leerlo, de lo contrario este permanece almacenado en un servidor de correo hasta que el usuario lo busque. Es un error pensar que en el correo electrónico del receptor conocerá el mensaje inmediatamente después de enviado, para esto se requiere una conexión sincrónica o en línea, donde tanto trasmisor como receptor están listos para iniciar la charla.

Aspectos negativos:

- No garantiza que los mensajes lleguen a su destino
- No asegura que el remitente sea quien dice ser.
- No mantiene el compromiso de avisar de las anomalías en el transcurso del envió del mensaje
- Problema de seguridad si no se usa con los debidos controles, como virus troyanos, etc.
- El envío de mensajes permite adjuntar al mensaje, archivos de texto, de video, de audio, imágenes, etc.

Sigue el modelo cliente/servidor: en el equipo servidor están definidas las cuentas de correo de los usuarios y sus buzones, y los clientes gestionan la descarga de correo, así como su elaboración.

3.2. Agente

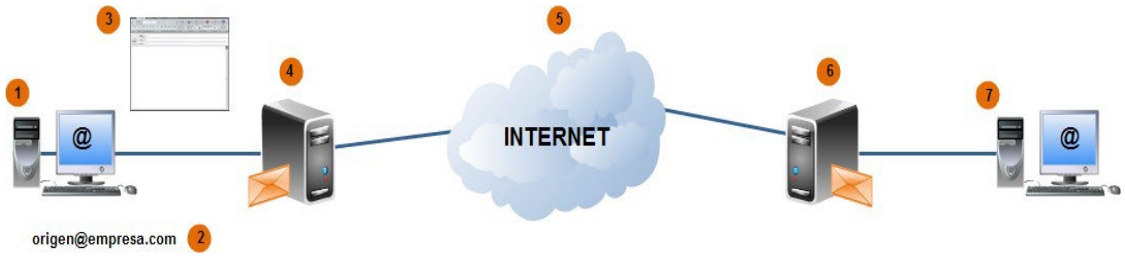

Figura 1. Representación gráfica de envío de correos

1. El software de correo-e del cliente.
2. La cuenta de origen del emisor. Ésta puede ser enmascarada por varios sistemas.
3. El mensaje puede ser alterado, eliminado o puede contener virus.
4. El servidor de correo del emisor y su software, alojado en proveedor de servicios internet (o en la propia empresa caso de disponer de software de correo servidor).
5. El canal: internet, donde los hackers pueden interceptarlo, otros proveedores de telecomunicaciones, los routers servidores DMZ, etc.
6. El servidor de correo del destino y su software (asociado al dominio de la cuenta y al ISP donde esté alojado este dominio).
7. El software del correo del receptor (Outlook, Gmail, Thunderbird, etc.).

Todos estos agentes son potencialmente puntos de riesgo en la seguridad de un envío de correo electrónico.

3.3. Elementos del servicio de correo electrónico

3.3.1. Agente de Acceso al Correo (MAA)

El MAA es usado para recuperar del buzón de mensajes de un servidor de correo electrónico. Ejemplos de MAAs son el protocolo IMAP y POP.

3.3.2. Agente de Transferencia del correo (MTA)

Un programa MTA transfiere los mensajes de correo electrónico entre máquinas que usan el protocolo SMTP. Un mensaje puede pasar por varios MTA hasta llegar al destino final.

La mayoría de los usuarios desconocen la existencia de estos agentes, incluso si cada mensaje se envía a través de como mínimo un MTA.

Aunque el proceso de envío de mensajes entre las máquinas puede parecer bastante directo, todo el proceso de decidir si un agente MTA concreto puede o debe aceptar un mensaje para entregarlo a un host remoto es bastante complicado. Además, debido a los problemas de correo basura, el uso de un MTA concreto normalmente está limitado por la propia configuración del MTA o el acceso a la red del sistema que lo ejecuta.

Muchos de los agentes MUA de mayores dimensiones y complejidad también sirven para enviar correo. Sin embargo, no se debe confundir esta acción con las funciones propias y verdaderas de estos agentes. Para que los usuarios que no ejecutan un agente MTA propio puedan transmitir los mensajes salientes a una máquina remota para su envío, deben utilizar una capacidad en el MUA capaz de transferir el mensaje a un MTA para el que tengan autorización de uso. Sin embargo, el agente MUA no entrega directamente el mensaje al servidor de correo del destinatario final; esta función está reservada al agente MTA.

Funciones.

- Responsable del encaminamiento del correo entre dos sistemas.
- Es el que se conoce como servidor de correo.
- Gestiona la distribución de correo saliente, y está pendiente de la llegada de correo entrante desde Internet.

Ejemplos: Sendmail, Postfix, Qmail, Exim.

3.3.3. Agente de Entrega de Correo (MDA)

Los agentes MTA utilizan programas MDA para entregar el correo electrónico al buzón de un usuario concreto. En muchos casos, el agente MDA es realmente un LDA (Local Delivery Agent, Agente de entrega local), como bin/mail o Procmail. Sin embargo, Sendmail también puede desempeñar la función de un agente

MDA, como cuando acepta un mensaje de un usuario local y lo adjunta a su fichero de spool de correo electrónico.

En general, los MDAs no transportan mensajes entre sistemas tampoco proporcionan una interfaz de usuario; los MDAs distribuyen y clasifican mensajes en la máquina local para que lo acceda una aplicación cliente de correo.

Muchos usuarios no utilizan directamente agentes MDA, porque sólo se necesitan agentes MTA y MUA para enviar y recibir correo. Sin embargo, algunos agentes MDA se pueden utilizar para ordenar los mensajes antes de que los lea el usuario, lo cual es de gran ayuda si recibe una gran cantidad de correo.

Características.

- Su función es copiar los mensajes del MTA al buzón de correo del usuario.
- No transporta mensajes entre sistemas ni es un interfaz de trabajo para el usuario. Ejemplos: Clientes de correo POP e IMAP.

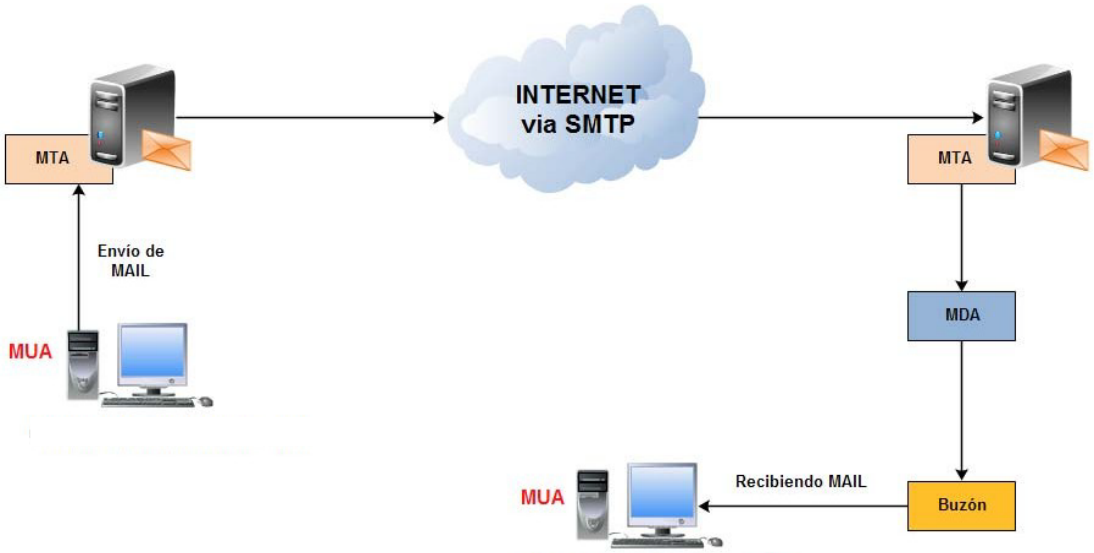

Figura 2. Agente de Envío de correo MDA

3.3.4. Agente de Usuario de Correo (MUA)

Un MUA es un programa que permite a un usuario, como mínimo, leer y escribir mensajes de correo electrónico. A un MUA se le denomina a menudo cliente de correo. Lógicamente, hay muchos programas MUA que ofrecen al usuario muchas más funciones, entre las que se incluyen la recuperación de mensajes mediante los protocolos POP e IMAP, la configuración de buzones de correo para almacenar los mensajes o ayuda para presentar los mensajes nuevos a un programa MTA (Mail Transfer Agent, Agente de transferencia de correo) que los enviará al destino final.

Los programas MUA pueden ser gráficos, como Mozilla Mail, o pueden tener una interfaz basada en texto sencilla, como Mutt o Pine.

Características.

- Constituye el interfaz de usuario que le permite editar, componer, y enviar correo local. Son los llamados clientes de correo.

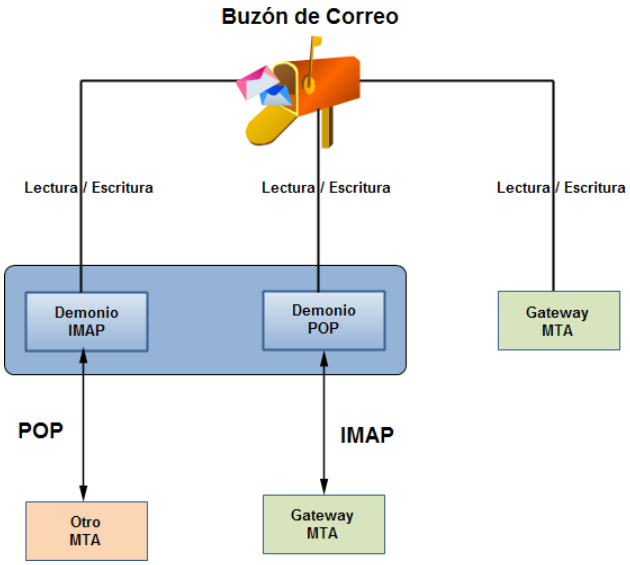

Figura 3. Buzón de Correo Electrónico

3.3.5. Agente de Registro de Correo (MSA)

El MSA o Agente de Registro de Correo es un agente nuevo que divide la carga de trabajo del MTA en servicios con muchos usuarios y mejora el desempeño. La idea es que el agente de servicio se preocupe de las tareas relativas al direccionamiento, tomando cierta parte de la carga de trabajo del MTA primario. Éste simplemente puede confiar la validez de las direcciones cuando recibe un correo de agentes de registros conocidos. El MSA corrige direcciones, y arregla y reescribe encabezados. Procesa el correo de su propia cola y lo envía a un agente de transferencia local.

3.4. Protocolos utilizados en el servidor de correo

El correo electrónico, al igual que otros servicios de red, utiliza diversos protocolos. Estos protocolos permiten que máquinas distintas, que se ejecutan a menudo en sistemas operativos diferentes y que tienen instalados programas de correo electrónico distintos, se comuniquen entre sí y transfieran los correos para que lleguen a los destinatarios adecuados.

Existen dos grupos de protocolos:

Los que van a permitir a un usuario acceder a su buzón de mensajes en un servidor. Los dos protocolos más populares son:

- IMAP (Protocolo de Acceso a Mensajes de Internet)
- POP (Protocolo de Oficina de Correo).

Los que van a permitir enviar mensajes a otros usuarios.

Aquí tenemos el protocolo SMTP (Simple Mail Transfer Protocol, Protocolo Simple de Transferencia de Correo).

3.4.1. Protocolo Simple de Transferencia de Correo (SMTP)

Este protocolo es el estándar de Internet para el intercambio de correo electrónico. SMTP necesita que el sistema de transmisión ponga a su disposición un canal de comunicación fiable y con entrega ordenada de paquetes, con lo cual, el uso del protocolo TCP en la capa de transporte, es lo adecuado. Para que dos sistemas intercambien correo mediante el protocolo SMTP, no es necesario que exista una conexión interactiva, ya que este protocolo usa métodos de almacenamiento y reenvío de mensajes.

Conjunto de reglas que rigen el comportamiento de un servidor SMTP:

- Acepta un mensaje entrante.
- Comprueba las direcciones del mensaje.
- Si son direcciones locales, almacena el mensaje para recuperarlo.
- Si son direcciones remotas, envía el mensaje.
- Si encuentra que el mensaje no se puede enviar (la cuenta ha excedido su cuota o el usuario ya no existe), devuelve un mensaje de error al remitente que explica el problema.

Mientras que los protocolos IMAP y POP permiten que un usuario reciba y lea el correo electrónico, el protocolo SMTP sirve para enviar correo electrónico.

Los mensajes salientes utilizan SMTP para pasar de la máquina del cliente al servidor, lugar desde el que se trasladan hasta el destino final. También dos servidores de correo que intentan transferir entre sí un mensaje utilizan SMTP para comunicarse, incluso si utilizan plataformas totalmente distintas.

Al implementar el SMTP sobre los servicios del TCP se debe establecer una conexión entre un puerto X en el emisor y el puerto 25 del receptor. El protocolo ya tiene asignado este puerto para las conexiones en TCP. De esta manera el SMTP está escuchando el puerto 25 y cuando la conexión está establecida envía la respuesta 220.

SMTP usa el puerto 25 del servidor para comunicarse.

El protocolo SMTP también permite gestionar el reenvío de mensajes entre sistemas si el sistema receptor sabe el destino al que tiene que enviar el mensaje.

A diferencia de los protocolos IMAP y POP, el protocolo SMTP no requiere autenticación en su forma más básica. Esto ha provocado mucho correo basura o spam, ya que un usuario no local puede utilizar el sistema de otro para enviar o transmitir el correo a listas completas de destinatarios con los recursos y ancho de banda del sistema.

En la figura se muestra cómo trabaja el protocolo IMAP en combinación con el SMTP, para la gestión del correo.

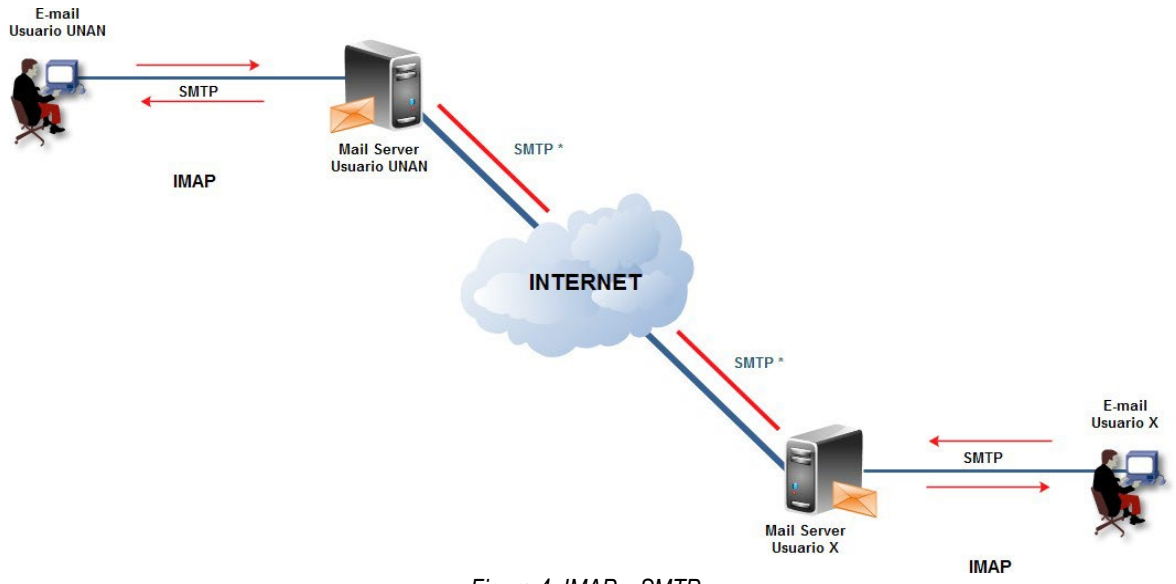

Figura 4. IMAP y SMTP

3.4.2. Protocolo de Oficina de Correo (POP)

Estos protocolos funcionan adecuadamente cuando los destinatarios están permanentemente conectados a INTERNET, unos años después de la publicación de los estándares se hizo más común la INTERNET para usuarios domésticos que desde sus casas se conectaban mediante un MODEM, esporádicamente a la INTERNET. Estos usuarios tienen un contrato con un ISP (Internet Service Provider) que está siempre conectado a la red y al llegar un mensaje de correo para un usuario de ese ISP, el mail- server del ISP debe guardar el mensaje hasta que el usuario se conecte y lo solicite.

Figura 5. Redes ISP

Este ambiente requirió la especificación de otro estándar para estos usuarios, de esta manera apareció en escena el protocolo de oficina postal POP. El protocolo POP permite a los clientes de correo electrónico recuperar los mensajes de los servidores remotos y guardarlos en las máquinas locales. La mayoría de los clientes de correo que utilizan el protocolo POP se configuran automáticamente para eliminar el mensaje del servidor de correo después de transferirlo correctamente al sistema del cliente, aunque esto se puede cambiar.

El protocolo de oficina postal fue diseñado para trabajar juntamente con el protocolo TCP, inicialmente el proceso está escuchando el puerto 110, a la espera de una conexión, cuando esta se establece el servidor envía un saludo y luego comienza un diálogo en el que se intercambian comandos y respuestas, hasta que la conexión se libera.

Estados del protocolo POP3.

Actualmente esta es la última versión (3) del protocolo POP. El POP3 va cambiando entre

3 distintos estados a lo largo de su vida, dependiendo de los resultados de algunos comandos especiales, los estados de POP3 son tres autorización, transacción y actualización los que detallaremos a continuación:

- **Autorización:** en el que se entra cuando se establece la conexión TCP y sirve para que los usuarios se identifiquen ante el protocolo.
- **Transacción:** cuando se hace una identificación positiva del usuario que quiere ingresar, aquí los mensajes pasan del servidor al cliente, una vez finalizado esto.
- **Actualización:** donde elimina los mensajes que el usuario recibió, y así finaliza la conexión y se libera.

POP es un protocolo mucho más sencillo que IMAP, porque no se tienen que enviar tantos comandos entre el cliente y el servidor.

POP también es en cierta medida más conocido, aunque la mayoría de los clientes de correo electrónico pueden utilizar cualquiera de estos protocolos.

3.4.3. Protocolo de Acceso a Mensajes de Internet (IMAP)

El protocolo IMAP es un método que utilizan las aplicaciones cliente de correo electrónico para tener acceso a los mensajes almacenados remotamente. Al utilizar el protocolo IMAP, normalmente denominado IMAP4 después de la versión del protocolo en cuestión, los mensajes de correo electrónico se conservan en el servidor de correo remoto, donde el usuario puede leerlos o eliminarlos, además de cambiar el nombre o eliminar los buzones de correo para almacenar correo electrónico.

Además, el protocolo IMAP es totalmente compatible con importantes estándares de mensajes de Internet, como, MIME (Multipurpose Internet Mail Extensions), Extensiones de Correo de Internet Multipropósito), que permiten recibir ficheros adjuntos. Muchos clientes de correo electrónico que utilizan el protocolo IMAP también se pueden configurar para que se almacene temporalmente en caché una copia de los mensajes localmente, de modo que el usuario puede examinar los mensajes que ha leído anteriormente si no está conectado directamente al servidor IMAP.

El protocolo IMAP se puede configurar también actualmente para almacenar los mensajes localmente de modo que se puedan ver los mensajes mientras no se está conectado a la red.

Principales ventajas de IMAP:

1. Puede manipular correos con distintos flags. Definibles por usuario.
2. Puede acceder y manipular múltiples buzones.
3. Puede almacenar correos tan bien como los recoge.
4. Permite actualizaciones concurrentes y acceso a buzones compartidos.
5. Diseñado para optimizar el acceso online, especialmente en accesos de baja velocidad.

IMAP vs. POP3

Al utilizar POP3, los clientes se conectan al servidor de correo brevemente, solamente lo que les tome descargar los nuevos mensajes. Al utilizar IMAP, los clientes permanecen conectados el tiempo que su interfaz permanezca activa y descargan los mensajes bajo demanda. El patrón de IMAP puede dar tiempos de respuesta más rápidos para usuarios que tienen una gran cantidad de mensajes.

Soporte para la conexión de múltiples clientes simultáneos a un mismo destinatario.

El protocolo POP3 asume que el cliente conectado es el único dueño de una caja de correo. En contraste, el protocolo IMAP permite accesos simultáneos a múltiples clientes y proporciona ciertos mecanismos a los clientes para que se detecten los cambios hechos a un mailbox por otro cliente concurrentemente conectado.

Soporte para acceso a partes MIME (Multipurpose Internet Mail Extensions), Extensiones de Correo Internet Multipropósito) de los mensajes y obtención parcial.

Casi todo el email del Internet es transmitido en formato MIME El protocolo IMAP les permite a los clientes obtener separadamente cualquier parte MIME individual, así como, obtener porciones de las partes individuales o los mensajes completos.

Soporte para que la información de estado del mensaje se mantenga en el servidor.

A través de la utilización de banderas definidas en el protocolo IMAP de los clientes, se puede vigilar el estado del mensaje, por ejemplo, si el mensaje ha sido o no leído, respondido o eliminado. Estas banderas se almacenan en el servidor, de manera que varios clientes conectados al mismo correo en diferente tiempo pueden detectar los cambios hechos por otros clientes.

Soporte para acceder a múltiples buzones de correo en el servidor.

Los clientes de IMAP pueden crear, renombrar o eliminar correo (por lo general presentado como carpetas al usuario) del servidor, y mover mensajes entre cuentas de correo. El soporte para múltiples buzones de correo también le permite al servidor proporcionar acceso a los fólderes públicos y compartidos.

Soporte para búsquedas de parte del servidor.

IMAP proporciona un mecanismo para los clientes le pidan al servidor que busque mensajes de acuerdo con una cierta variedad de criterios. Este mecanismo evita que los clientes descarguen todos los mensajes de su buzón de correo con el fin de agilizar las búsquedas.

Soporte para un mecanismo de extensión definido.

Como reflejo de la experiencia en versiones anteriores de los protocolos de Internet, IMAP define un mecanismo explícito mediante el cual puede ser extendido. Se han propuesto muchas extensiones de IMAP y son de uso común. Un ejemplo de extensión es el IMAP IDLE, que sirve para que el servidor avise al cliente cuando ha llegado un nuevo mensaje de correo y éstos se sincronicen. Sin esta extensión, para realizar la misma tarea el cliente debería contactar periódicamente al servidor para ver si hay mensajes nuevos.

IMAP es utilizado frecuentemente en redes grandes; por ejemplo, los sistemas de correo de un campus. IMAP les permite a los usuarios acceder a los nuevos mensajes instantáneamente en sus computadoras, ya que el correo está almacenado en la red. Con POP3 los usuarios tendrían que descargar el email a sus computadoras o acceder vía Web. Ambos métodos toman más tiempo de lo que le tomaría a IMAP, y se tiene que descargar el email nuevo o refrescar la página para ver los nuevos mensajes.

De manera contraria a otros protocolos de Internet, IMAP soporta mecanismos nativos de cifrado. La transmisión de contraseñas en texto plano también es soportada.

3.5. Sistemas seguros de correo electrónico

El correo electrónico es uno de los sistemas telemáticos más vulnerables a los ataques a la seguridad, actualmente el correo electrónico es muy importante a nivel profesional y es la herramienta que se ha desarrollado más rápidamente en internet, pero durante muchos años la parte pendiente ha sido la seguridad con sus cuatro formas: confidencialidad, integridad, autenticación y firmas.

Cuando un usuario envía un mensaje, pierde el control sobre él, es decir, su contenido puede ser leído por cualquiera que lo manipule hasta llegar a su destino. Se define como correo seguro, aquel que garantiza los siguientes aspectos:

- Confidencialidad
- Autenticación
- Integridad

Algunos conceptos importantes relativos al correo seguro son:

- Autoridad de Certificación (CA)
- Certificado Digital
- Certificado raíz

Alternativas para E-Mail seguros

Los servicios de seguridad pueden ser agregados a cada enlace de comunicación a lo largo de una trayectoria dada, o pueden ser integrados alrededor de los datos que están siendo enviados, siendo esto independiente de los mecanismos de comunicación, este enfoque avanzado es frecuentemente llamado seguridad “nodo-a-nodo”. Las dos características de este tipo de seguridad son privacidad (donde el recipiente deseado sólo puede leer el mensaje) y la autentificación (en el otro caso, recipiente puede asegurar la identidad del emisor). La capacidad técnica de estas funciones es bien conocida desde hace tiempo, sin embargo, recientemente ha sido sólo aplicada al correo-e.

Existen dos propuestas principales para ofrecer los servicios de seguridad que hemos mencionado: S/MIME y PGP. Otros protocolos han sido propuestos en el pasado como son PEM y MOSS, no han tenido mayor presencia. Sin embargo, ahora diversos proveedores de servidores de correo-e, incluyen en sus productos a S/MIME, PGP/MIME y OpenPGP que son versiones del protocolo PGP utilizadas para correo.

Criptografía

La criptografía comprende toda una familia de tecnologías que incluyen las siguientes:

Cifrado: Transforma la información en una forma no legible asegurando la privacidad.

Descifrar: Es el inverso del cifrado; es decir, transforma la información cifrada a su forma original legible.

Autentificación: Identifica a una entidad como un individuo, una máquina en la red o una organización.

Firmas digitales: La relación de un documento con el dueño de una "llave" particular siendo el equivalente a la firma de un documento.

Verificación de firmas: Es lo contrario de la firma digital; verifica que una firma en particular sea válida.

Llave simétrica o secreta: Utiliza una misma llave para cifrar y descifrar la información enviada a través de la red; pero el problema que se presenta es que tanto quien envía como quien recibe la información deben tener la misma llave asegurándose que nadie más pueda obtenerla porque si intercepta la información pudiera descifrarla y leerla fácilmente.

Llave asimétrica o pública: Fue inventada en 1976 por Whitfield Diffie and Martin Hellman para resolver el problema presentado por la llave simétrica. Es un método de transmisión de información en donde el que recibe la información puede estar seguro de la identidad de quien la envió. La idea básica de este método es el uso de un par de llaves:

- **Llave privada:** Solamente su dueño la conoce y se usa para descifrar la información enviada por otras personas.
- **Llave pública:** Esta se publica y se usa por cualquier persona para cifrar la información antes de enviarla a su destino (dueño).

El par de llaves se genera simultáneamente, usando algoritmos especiales en donde los mensajes que se cifran con la llave pública de una persona puedan ser descifrados solamente con la llave privada de esa misma persona y viceversa. Por lo tanto, para establecer una comunicación segura ya no es necesario compartir primeramente una llave privada. Por ejemplo, si un cliente deseara enviar información segura a un servidor, el servidor daría su llave pública (por correo electrónico) y el cliente haría lo siguiente:

Cifra la información usando la llave pública del servidor y luego se la envía.

El servidor recibiría la información y la descifra usando su llave privada.

Esta transmisión es segura en el sentido de que nadie más que reciba la información podrá leerla porque no sabe el valor de la llave privada. Existe un problema que reside en el hecho de que la llave pública no

puede ser verificada. Cómo sé que la llave pública realmente es suya y no una llave pública generada por algún impostor que desee interceptar sus mensajes. Este problema es más serio cuando es usado para verificar automáticamente la comunicación entre dos “hosts", tales como un cliente (“browser") y un servidor (DNS dinámico). Aquí es donde intervienen los certificados.

Firmas digitales

El paradigma de firmas electrónicas (también llamadas firmas digitales) es un proceso que hace posible garantizar la autenticidad del remitente (función de autenticación) y verificar la integridad del mensaje recibido.

Las firmas electrónicas también poseen una función de reconocimiento de autoría, es decir, hacen posible garantizar que el remitente ha enviado verdaderamente el mensaje.

Función HASH

Una función hash es una función que hace posible obtener un hash (también llamado resumen de mensaje) de un texto, es decir, obtener una serie moderadamente corta de caracteres que representan el texto al cual se le aplica esta función hash. La función hash debe ser tal que asocie únicamente un hash con un texto plano (esto significa que la mínima modificación del documento causará una modificación en el hash). Además, debe ser una función unidireccional para que el mensaje original no pueda ser recuperado a partir del hash. Si existiera una forma de encontrar el texto plano desde el hash, se diría que la función hash presenta una "trapdoor".

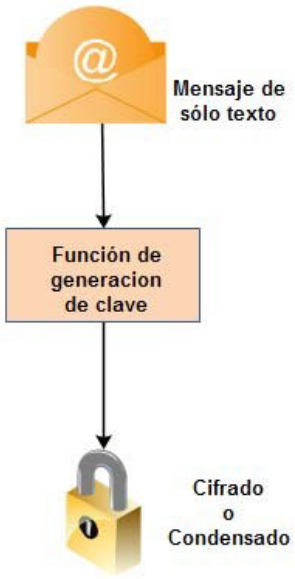

Figura 6. Hash en correo electrónico

Como tal, puede decirse que la función hash representa la huella digital de un documento.

Verificación de la integridad

Al enviar un mensaje junto con su hash, es posible garantizar la integridad de dicho mensaje, es decir, el destinatario puede estar seguro de que el mensaje no ha sido alterado (intencionalmente o por casualidad) durante la comunicación.

Cuando un destinatario recibe un mensaje simplemente debe calcular el hash del mensaje recibido y compararlo con el hash que acompaña el documento. Si se falsificara el mensaje (o el hash) durante la comunicación, las dos huellas digitales no coincidirían.

Sellado de datos

Al utilizar una función hash se puede verificar que la huella digital corresponde al mensaje recibido, pero nada puede probar que el mensaje haya sido enviado por la persona que afirma ser el remitente.

Para garantizar la autenticidad del mensaje, el remitente simplemente debe cifrar (generalmente decimos firmar) el hash utilizando su clave privada (el hash firmado se denomina sello) y enviar el sello al destinatario.

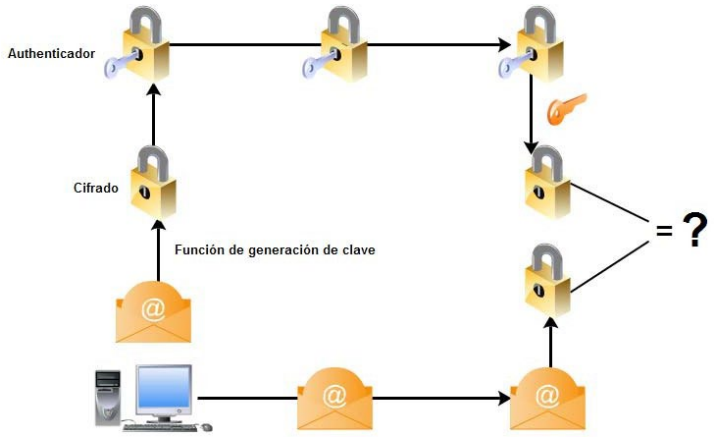

Figura 7. Sellado de Datos.

Al recibir el mensaje, el destinatario deberá descifrar el sello con la clave pública del remitente, luego deberá comparar el hash obtenido con la función hash del hash recibido como adjunto. Esta función de creación de sellos se llama sellado.

Autoridad Certificada (CA)

Una Autoridad Certificadora (AC, en inglés CA) es una entidad confiable que se encarga de garantizar que el poseedor de un certificado digital sea quien dice ser, bridando confianza a ambas partes de una comunicación segura SSL/TLS.

Una Autoridad Certificadora es la encargada de confirmar que el dueño de un certificado es realmente la persona que dice ser. Una Autoridad Certificadora puede definir las políticas especificando cuáles campos del Nombre Distintivo son opcionales y cuáles requeridos. También puede especificar requerimientos en el contenido de los campos.

Existen varias Autoridades Certificadoras, puede que una autoridad certificadora certifique o verifique la identidad de otra Autoridad Certificadora y así sucesivamente; pero habrá un punto en que una Autoridad no tendrá quién la certifique, en este caso, el certificado es firmado por uno mismo, por lo tanto, la Autoridad Certificadora es verificada o confiada por ella misma.

Las Autoridades Certificadoras (o notarios electrónicos) deben ser entes fiables y ampliamente reconocidos que firman las claves públicas de las personas, certificando con su propia firma la identidad del usuario. Por lo tanto, si se desea establecer una Autoridad Certificadora, éstas deben tomar extremadas precauciones para evitar que sus claves caigan en manos de intrusos, lo cual comprometería todo el sistema. Para ello tendrá que utilizar claves largas y dispositivos especiales para su almacenamiento. Además, cuando emiten un certificado, deben estar seguros de que lo hacen a la persona adecuada.

No podemos olvidar que la Autoridad Certificadora es la responsable, en última instancia, de todo el proceso, con una serie de responsabilidades legales y que basa su negocio en la credibilidad que inspire en sus potenciales clientes. Una Autoridad Certificadora con autentificaciones erróneas no tendrá más remedio que cerrar ya que los usuarios no considerarán sus certificados de la suficiente calidad.

Las Autoridades Certificadoras no solamente ofrecen certificados, sino también los manejan; es decir, determinan cuánto tiempo van a ser válidos y mantienen listas de certificados que ya no son válidos (Listas de Revocación de Certificados o CRLs).

Por ejemplo, si un empleado posee un certificado para una compañía y el empleado sale de la compañía, no solamente con el certificado se indica que ya no existe, sino que se tiene que registrar por medio del CRL para que dicho certificado que ya había sido utilizado quede invalidado y no pueda ser utilizado posteriormente. Varias compañías se han establecido como Autoridades Certificadoras. Entre las cuales destacan:

- VeriSign, Inc. [http://www.verisign.com]
- Thawte Certification. [http://www.thawte.com]
- Xcert Sentry CA. [http://www.xcert.com]
- Entrust. [http://www.entrust.net]
- CAcert. [http://www.cacert.org]

Estas compañías proveen los servicios de:

- Verificación de solicitud de Certificados.
- Procesamiento de solicitud de Certificados.
- Firma, asignación y manejo de Certificados.

Certificado Digital SSL/TLS

Es un documento digital único que garantiza la vinculación entre una persona o entidad con su llave pública. Contiene información de su propietario como nombre, dirección, correo electrónico, organización a la *que* pertenece y su llave pública, así como información propia del certificado por mencionar: periodo de validez, número de serie único, nombre de la AC que emitió, firma digital de la AC cifrada con su llave privada y otros datos más que indican cómo puede usarse ese certificado.

Contenido de un Certificado

Los certificados pueden adoptar múltiples formas. El formato más difundido está definido por la norma del ITU-T X.509, la cual forma parte del servicio de directorio diseñado por ISO (International Organization for Standardization, Organización Internacional de Estandarización) para el modelo OSI (Open System Interconnection, Interconexión de Sistemas Abiertos).

Un certificado X.509 es típicamente un archivo pequeño que contiene la información mostrada a continuación:

Nombre Distintivo de la entidad: Incluye la información de identificación (el nombre distintivo) y la llave pública.

Nombre Distintivo de la Autoridad Certificadora: Identificación y firma de la Autoridad Certificadora (CA) que firmó el certificado.

Período de Validez: El período de tiempo durante el cual el certificado es válido.

Información adicional: Puede contener información administrativa de la CA como un número de serie o versión.

El Nombre Distintivo de la entidad se usa para proveer una identidad en un contexto específico de acuerdo con las necesidades de la aplicación. Los Nombres Distintivos están definidos en el estándar X.509, así como por las necesidades de la aplicación.

Funcionalidad del Certificado

Los certificados se ofrecen por parte de una Autoridad Certificadora a la solicitud de una persona, entidad u organización que así lo requiera.

Enviar información encriptado usando la verificación de certificados:

- Se envía un mensaje pidiendo su certificado.
- Usted regresa su certificado.
- Se verifica con la Autoridad Certificadora que su certificado sea válido. Especialmente, que dicha Autoridad Certificadora fue quien le dio el certificado y que su llave pública es la misma que la del certificado.
- Se recibe la confirmación de la Autoridad Certificadora que el certificado es válido.
- La información se cifra usando su llave pública y luego es enviada. Usted recibe la información y la descifra usando su llave privada.

Precio en el mercado actual de Certificados Digitales:

La siguiente **tabla 1** contiene información sobre los precios de Certificados Digitales de las Autoridades Certificadoras más reconocidas a nivel mundial. Febrero 2020

AC	Tipo de Certificado	Precio	Periodo de Validez	Nivel de Cifrado
Digicert	Wildcard Plus - Proteger un Domino Completo	$475	3 Año	SHA-2/SHA-1 2048-bit SSL certificates.
		$535	2 Año	
		$595	1 Año	
	Unified Communications - Proteger Dominios Múltiples	$719	3 Año	
		$539	2 Año	
		$299	1 Año	
	SSLPlus-Protegerun Nombre común	$156	3 Año	
		$174	2 Año	
		$195	1 Año	
Symantec	Secure Site Pro con EV	$1500	2 Año	Cifrado de 128 bits como mínimo a 256 bits.
	Secure Site con EV	$1500	2 Año	
	Secure Site Pro	$1250	2 Año	
	Secure Site	$1000	2 Año	
La Domains coopac digital	SSL 123	$120	1 Año	Hasta 256 bits de encriptación
		$240	2 Año	
	Web Server Cert	$179	1 Año	
		$319	2 Año	
	SGC SuperCert	$495	1 Año	
		$749	2 Año	
	WildCard Server Cert	$699	1 Año	
		$1199	2 Año	
	SSL123 Certificates	$149	1 Año	

Thawte	SSL Web Server Certificates	$249	1 Año	128-bit a 256-bit
	SSL Web Server Certificates with EV	$599	1 Año	
	SGC SuperCerts	$1199	2 Año	
Entrust	Standard SSL Certificates	$155	1 Año	Soporta llaves de 2048-bity128-o256- bitde cifradoSSL
	Advantage SSL Certificates	$186	1 Año	
	UC Multi-Domain SSL Certificates	$249	1 Año	
	EV Multi-Domain SSL Certificates	$373	1 Año	

Tab. 1 Precios de Certificados de Autoridades Certificadoras con mayor reconocimiento mundial

Certificados Digitales de entidades Nacionales:

Entidad	AC	Periodo de Validez	Precio
UNAN - León	Autoridad Certificadora Autofirmada	11 Años	Gratis
	VeriSing Class 3 EV	2 Años	$1000/$1500
UNI	Autoridad Certificadora Autofirmada	10 Años	Gratis
UCA	Zimbra Collaboration Suite	1 Años	Gratis
UNAN - Managua	Go.Daddy	2 Años	$69.99/$89.99
Banco Central de Nicaragua	Trustwave Organization Validation CA	3 Años	$149/$1199
Asamblea Nacional	Zimbra Collaboration Suite	10 Años	Gratis

Tab. 2 Certificados Digitales utilizados por entidades Nacionales

3.6. POSTFIX

Postfix es un servidor de correo, un daemon, que gestiona la entrada y la salida de correos de Internet a la intranet o de la intranet a Internet o sin salir de la propia intranet. Postfix fue diseñado por Wietse Venema como alternativa a sendmail. Postfix rige el estándar del protocolo smtp (Simple Mail Transfer Protocol o Protocolo Simple de Transferencia de Correo Electrónico).

3.6.1. ¿Porque Utilizar Postfix?

Las razones para usar Postfix fueron básicamente su sencillez, potencia y versatilidad a respuesta a todas las interrogantes, porque es tan potente como Sendmail, fácil de configurar y, además, hasta es entretenido.

- Diseño modular (no es un único programa monolítico).
- La seguridad ha sido un condicionante desde el comienzo de su diseño.
- Lo mismo cabe decir del rendimiento (seguramente Sendmail no se diseñó pensando que algún día

habría sitios necesitaran procesar cientos de miles o millones de mensajes al día).

- Soporte para las tecnologías más usadas hoy día: LDAP, Bases de datos (MySQL), autentificación mediante SASL Simple Authentication and Security Layer (capa de seguridad y autenticación simple), LMTP (Local Mail Transfer Protocol o Protocolo de la Transferencia del Correo Local), es un derivado del SMTP, el Simple Mail Transfer Protocol, etc.
- Estricto cumplimiento de los estándares de correo-e.
- Facilidad de configuración.
- Abundante documentación y de calidad.
- Fácil integración con antivirus.
- Uso sencillo de listas negras.
- Tiene múltiples formas de obtener información de lo que está pasando para resolver problemas o simplemente, para aprender.
- Se pueden lanzar varias instancias de Postfix en la misma máquina con distintas configuraciones, usando cada una distinta direcciones IP, distintos puertos, etc.
- Filtrado de cabeceras y cuerpos de mensajes por expresiones regulares.
- Utilidades para varias cosas, como gestionar las colas de mensajes.

Por último, pero no menos importante, hay que decir que el código fuente de Postfix (por supuesto de dominio público) es un ejemplo de diseño, claridad y documentación, lo cual facilita su mantenimiento, así como la incorporación de nuevas capacidades, corrección de errores, etc.

3.6.2. Ventajas de Utilizar Postfix.

- Servidor de correo que funciona sobre sistemas de tipo Unix.
- Su intención fue la de sustituir a Sendmail. Compatible para el resto de las aplicaciones.
- Arquitectura y diseño muy modular.
- Fácil de administrar y configurar.
- Repartir correo de forma local puede repartir a almacén de correo o pasarlo a un MDA (Mail Delivery Agent o Agente de Entrega de Correo).
- Muy rápido. Fue diseñado pensando en el rendimiento. Evita saturar otros sistemas.

3.6.3. Característica de seguridad de Postfix

- Arquitectura modular: Cada proceso se ejecuta con privilegios mínimos para su tarea.
- Proceso que no se necesita se deshabilita: No se puede explotar.
- Los procesos se aíslan unos de otros. Muy poca comunicación entre procesos.
- Evita utilizar buffers de tamaño fijo, evitando que tengan éxito ataques buffer overflow.

- Puede ejecutarse en modo chroot.
- Preparado para ataques DoS (Deny of Service, Denegación de Servicio). Cantidad de memoria controlada.

3.6.4. Arquitectura.

Al contrario de Sendmail, que es un gestor de correo monolítico, en el diseño de Postfix se han disgregado los diversos tratamientos que se realizan sobre un mensaje a su paso por un Mail Transfer Agent (MTA), adjudicando cada tratamiento o grupo de tratamientos a un proceso independiente. El conjunto de todos estos procesos es Postfix.

Los procesos que conforman Postfix se comunican a través de sockets que se crean, por razones de seguridad, en un directorio de acceso restringido. La información que intercambian los diversos procesos es la mínima posible, limitándose en la mayoría de los casos a la referencia de la entrada en una cola y la relación de destinatarios, o a un simple identificador de estado.

3.6.5. Colas de correo

Postfix basa su funcionamiento en cuatro colas: maildrop, incoming, active y deferred.

Maildrop queue: El correo que es generado y/o entregado localmente en el sistema es procesado por la cola Maildrop.

Incoming queue o cola entrante: Esta cola recibe correo de otros hosts, clientes o de la cola maildrop. Si llegan correos y Postfix no puede atenderlos se quedan esperando en esta cola.

Active queue o cola activa: En esta cola están los mensajes en la fase de encaminamiento.

Deferred queue o cola diferida: En esta cola se almacena los mensajes que no se han podido encaminar o están pendientes de reintentar su encaminamiento.

3.6.6. Procesos

Postfix gestiona las colas mediante procesos independientes.

Pickup o recolección: Recoge los correos que provienen de las colas maildrop y los pasa a cleanup.

Smptd: Este proceso atiende, mediante el protocolo SMTP los correos de otros sistemas.

Cleanup o limpieza: Analiza las cabeceras de los correos. Si es ok. Los deposita en la cola incoming.

Qmgr: Proceso encargado de tratar los correos que llegan a incoming, depositarlos en active y lanzar el proceso adecuado para su encaminamiento: local, smtp o pipe.

Local: Proceso encargado de depositar el correo en el buzón.

SMTP (Simple Mail Transfer Protocol o Protocolo Simple de Transferencia de Correo Electrónico): Proceso encargado de enviar el correo al host destino mediante protocolo SMTP.

3.6.7. Comandos

Algunos comandos de Postfix más interesantes:

Newaliases: Actualiza la base de datos de los alias (/etc/aliases). Enlace simbólico a Sendmail (compatibilidad).

Postsuper: Se encarga de realizar operaciones de mantenimiento.

Postqueue: Comando que sirve de interfaz para la gestión de las colas.

Postmap: Crea, actualiza o consulta una o más tablas Postfix.

Postconf: Muestra los valores actuales de los parámetros de Postfix.

3.6.8. Tablas

Las tablas, creadas por el administrador sirven a los procesos para saber que tratamiento hay que dar a cada correo. Son 6 tablas, aunque no son obligatorias.

Access: Sistemas a los que se acepta o rechaza los correos. La utiliza el proceso smtpd.

Aliases: Define nombres alternativos a usuarios locales. Consulta el proceso local.

Canonical: Relación entre nombres alternativos y reales, locales o no. Proceso cleanup.

Relocated: Devolver los mensajes que han cambiado de dirección. Proceso qmgr.

Transport: Política de encaminamiento por dominios. Proceso trivial-rewrite.

Virtual: Relación entre usuarios virtuales y reales. Proceso cleanup.

Postfix: soporta muy diversos soportes de backend para las tablas.

CompSendmail: Significa que el MTA Mail Transport Agent (Agente de Transporte de Correos), se comporta como Sendmail en algunos aspectos que harán que sea más transparente cambiarse de Sendmail a un agente alternativo de transporte de correo.

3.7. Transport Layer Security (TLS)

Por defecto, toda comunicación en Internet se hace sin ningún tipo de cifrado y sin una autenticación fiable. Esto significa que cualquiera con acceso físico a la línea de datos por la que viaja un paquete puede

espiar dicha comunicación. Aún peor, es posible redirigir o alterar esa comunicación para que la información que se desea mandar se pierda y nadie se dé cuenta.
De cara a solventar estos problemas de seguridad, Netscape, Inc. introdujo el protocolo SSL (Secure Sockets Layer), que ha ido evolucionando en el protocolo estandarizado TLS (Transportation Layer Security). Ofrece tanto cifrado de la comunicación (frenando las escuchas) como autenticación fuerte (asegurando que ambas partes de una comunicación son correctamente identificadas y que la comunicación no puede ser alterada).
Postfix/TLS no implementa el protocolo TLS por sí mismo, sino que usa el paquete OpenSSL para esta tarea.

En el website de OpenSSL pueden encontrarse enlaces a documentación que profundiza en el protocolo y sus características.

3.7.1. Características TLS

TLS cuenta con una variedad de medidas de seguridad:

- Protección contra una rebaja del protocolo a una anterior (menos seguro) versión o una suite de cifrado más débil.
- Numeración de los registros posteriores de aplicaciones con un número de secuencia y el uso de este número de secuencia en la autenticación de los códigos de mensajes (MAC).
- El uso de un resumen de mensaje mejorado con una clave (por lo que sólo una clave-titular puede comprobar el MAC). El HMAC de construcción utilizados por la mayoría de conjuntos de cifrado TLS se especifica en el RFC 2104 (SSL 3.0 utiliza un diferente basado en MAC hash).
- SSL 3.0 mejorado SSL 2.0 mediante la adición de sistemas de cifrado SHA-1 y un apoyo para la autenticación de certificado.

3.7.2. Protocolo Handshake

El protocolo TLS Handshake Protocol opera sobre el Record Protocol, que es el encargado de ofrecer una transferencia de datos segura. El Handshake Protocol se encarga de establecer y terminar las conexiones TLS. Las aplicaciones (como por ej. un Web browser, un servidor Web, un servidor de e-mail, etc.) usan el Handshake Protocol para abrir y cerrar conexiones seguras, y se requiere que las aplicaciones estén diseñadas para soportar TLS (por ej., pueden usar la biblioteca SSLPlus).

Este protocolo es responsable de la negociación de una sesión, que consiste en los siguientes items:

- **Session Indentifier:** una secuencia de bytes arbitrarios elegidos por el servidor para identificar un estado de sesión activa o reiniciable.
- **Peer Certificate:** Es el certificado X509v3 del par.
- **Compression Method:** un método de compresión (el algoritmo a utilizar antes de cifrar).

- **Cipher Spec:** Especifica el algoritmo de cifrado de datos, (por ejemplo, NULL, DES, etc.) y un algoritmo de MAC (como MD5 o SHA). También define atributos criptográficos como el hash_size.
- **Master Secret:** un secreto compartido de 48 bytes entre el cliente y el servidor.
- **is resumable:** es un flag para indicar si la sesión puede usarse para iniciar nuevas conexiones.

Estos items se usan también para crear parámetros de seguridad que serán utilizados por el Record Layer cuando se protegen los datos de la aplicación. Muchas conexiones pueden instanciarse usando la misma sesión a través de la característica de re-inicialización.

Como ya sabemos, el Handshake Protocol opera sobre el Record Protocol. Para que un cliente y un server puedan empezar a comunicarse, ellos primero se ponen de acuerdo en la versión del protocolo (TLS puede interoperar con SSL), seleccionar los algoritmos criptográficos a usar para la privacidad de sus datos, autenticarse (opcionalmente) uno con el otro, y usan técnicas de criptografía de clave pública para generar secretos compartidos.

Los sub-protocolos utilizados por el Handshake Protocol son:

- **Change Cipher Spec Protocol:** Existe para señalar transiciones en estrategias de codificación.
- **Alert Protocol:** Los mensajes de Alerta se componen de la gravedad del mismo y alerta de descifrado. Estos con un nivel de resultado fatal resultan en la terminación inmediata de la conexión.

3.7.3. Mensajes intercambiados (resumen)

A continuación, presentaremos la secuencia de pasos (en forma narrada) que componen el Handshake de la apertura de una conexión segura usando el TLS Handshake Protocol:

Paso 1: El cliente le envía al servidor el número de versión de TLS (o bien de SSL), los cipher que quiere usar, datos generados aleatoriamente, y otros tipos de información que el server necesita para comunicarse con el cliente usando TLS. (Mensaje ClientHello).

Paso 2: El server le envía al cliente el número de versión del TLS (o SSL) del servidor, los cipher que quiere usar, datos generados aleatoriamente, y otros tipos de información que el cliente necesita para comunicarse con el server vía TLS. El server también manda su propio certificado X.509 y, si el servidor está prestando un servicio que requiera autenticación del cliente, le pide (al cliente) su certificado X.509.

Paso 3: El cliente usa parte de la información enviada por el servidor para autenticarlo. Si el servidor no puede ser autenticado, se le avisa del problema al usuario y se le informa que no se puede establecer una

conexión cifrada y autenticada con ese servidor. Si el servidor puede ser autenticado satisfactoriamente, el cliente va al Paso 4

Paso 4: Usando todos los datos generados en el Handshake hasta ahora, el cliente (con la cooperación del servidor, y dependiendo del cipher siendo usado) crea el premaster secret para esta sesión, lo cifra con la clave pública del server (la cual se obtuvo del certificado del server que éste mandó en el Paso 2), y envía el premaster secret cifrado hacia el server.

Paso 5: Si el server requirió la autenticación del cliente (un paso opcional en el Handshake), el cliente también firma (digitalmente) otra pieza de datos que es única a este Handshake y conocida por ambas partes. En este caso, el cliente manda los datos firmados y su propio certificado al server, junto con el premaster secret cifrado.

Paso 6: Si el server requirió la autenticación del cliente, el server intenta autenticar el cliente. Si el cliente no puede ser autenticado, la sesión es terminada. Si el cliente puede ser satisfactoriamente autenticado, el server usa su clave privada para descifrar el premaster secret, luego lleva a cabo una serie de cálculos (los cuales el cliente también ejecuta, empezando por el premaster secret) para generar el master secret.

Paso 7: Ambas partes (cliente y server) usan el master secret para generar session keys (las claves de la sesión), las cuales son claves simétricas usadas para cifrar y descifrar la información intercambiada durante la sesión TLS y para verificar su integridad (esto es, detectar cambios en los datos mientras éstos viajaban por la red, antes de ser recibidos por la conexión TLS).

Paso 8: El cliente envía un mensaje al server informando le que mensajes futuros desde los clientes serán cifrados con la session key. Luego éste manda un mensaje (cifrando) separado indicando que la parte cliente del handshake ha terminado.

Paso 9: El server manda un mensaje hacia el cliente informando que los futuros mensajes desde el server serán cifrados con la session key. Luego éste manda un mensaje (cifrado) separado indicando que la parte server del handshake ha terminado.

Paso 10: En este momento, el handshake TLS está completo, y la sesión TLS ha empezado. El cliente y el server usan las session keys para cifrar y descifrar los datos que se mandan uno con otro y para validar su integridad.

3.8. Local Mail Transfer Protocol (LMTP)

El Local Mail Transfer Protocol o LMTP (Protocolo de transporte local de correo) es un derivado de SMTP, el Simple Mail Transfer Protocol. LMTP es diseñado como una alternativa a SMTP para situaciones

donde el lado receptor no dispone de cola de correo (queue mail), como un MTA (Mail Delivery Agent) que entiende conversaciones SMTP.

LMTP es un protocolo de capa de aplicación, que corre en lo alto de TCP/IP.

Una conversación LMTP usa los mismos comandos que una conversación ESMTP con las siguientes excepciones:

- El verbo EHLO es reemplazado por LHLO
- ESMTP requiere un estado único para el mensaje completo desde el servidor tras el envío del mensaje DATA del cliente. LMTP requiere una respuesta por cada comando RCPT previamente aceptado.

La mayor diferencia es que LMTP rechazará un mensaje si no es derivado de inmediato a su destino final. Esto elimina la necesidad de una cola de correo. Por esta razón, se supone que un LMTP no ha de correr bajo el puerto 25/TCP.

3.9. Sieve

Es un lenguaje que puede usarse para crear filtros de correo electrónico en el momento de la entrega final del correo. No está ligado a ningún sistema operativo o servidor de correo en particular. Requiere el uso de la especificación de mensajes del RFC 822.

El lenguaje es suficientemente potente para ser útil, pero está limitado de modo que permita la creación de sistemas de filtrados seguros en el lado del servidor. El objetivo es no permitir a los usuarios hacer nada más complejo (y peligroso) que escribir sencillos filtros de correo, además de facilitar editores basados en interfaces gráficas de usuario.

El lenguaje no permite definir bucles o funciones, ni tampoco proporciona variables, se supone que el uso del lenguaje tiene lugar al final de la entrega, cuando el mensaje se mueve a una cuenta accesible por el usuario. En aquellos sistemas donde el MTA (Mail Transport Agent) realiza la entrega final (como es tradicional en los sistemas UNIX), es razonable clasificar cuando el MTA deposita el correo en la cuenta del usuario.

Sin embargo, los filtros Sieve pueden ser usados por varios puntos finales de entrega del sistema de correo: por el servidor SMTP, por un servidor IMAP o POP que archive una o más cuentas de usuario, o por un cliente de correo (MUA, Mail User Agent) que actúe como gestor de las entregas (por ejemplo, un cliente POP o IMAP sin conexión).

3.10. Amavisd-new

Amavisd-new es un interfaz de alto rendimiento y fiabilidad entre el MTA y uno o más filtros de contenidos: antivirus o el módulo Mail: SpamAssassin de Perl. Está escrito en Perl, asegurando alta fiabilidad, portabilidad y facilidad de mantenimiento. Se comunica con el MTA vía (E)SMTP o LMTP, o mediante el uso de otros programas. No existen problemas de sincronización en su diseño que pudieran causar pérdidas de correos.

Normalmente se posiciona dentro o cerca del gestor de correo principal, no necesariamente donde se ubiquen las cuentas de correo de los usuarios (donde tiene lugar el envío final). Si se está buscando una solución que soporte configuración por usuario y de mensajes pequeñas que se ubique al final del proceso de envío (p.e. llamado desde procmail o en sustitución de un agente local de envío), posiblemente puedan encontrarse otras soluciones más apropiadas.

Cuando está habilitado el uso de Mail SpamAssassin (SA), se llama a SA una sola vez por mensaje (independientemente del número de destinatarios). Amavisd-new se beneficia del uso del módulo de Perl Net Server, el cual ofrece un rápido entorno multihilo. Amavisd-new ofrece un servidor SMTP que cumple con el RFC 2821, un servidor LMTP que cumple con el RFC 2033, un cliente SMTP y genera notificaciones de estado de envío (o no) que cumplen los RFC 1892 y 1894. Esto lo hace adecuado para múltiples analizadores de virus y de correo publicitario en plataformas de correo donde la fiabilidad y el cumplimiento de los estándares son importantes.

3.11. ClamAV – Antivirus

ClamAV es una herramienta antivirus GPL para UNIX. El propósito principal de este software es la integración con los servidores de correo (escaneo de datos adjuntos). El paquete proporciona un servicio multi-hilo flexible y escalable, un analizador de línea de comandos y una utilidad para la actualización automática vía Internet. Los programas están basados en una librería distribuida con el paquete Clam AntiVirus, la cual puede ser usada por su propio software. Y lo más importante, la base de datos se mantiene actualizada constantemente.

Otras características destacables son el soporte de firmas digitales en la actualización de la base de datos, el análisis durante el acceso bajo Linux y FreeBSD, la detección de más de 20000 virus, gusanos y troyanos, el soporte integrado para archivos comprimidos con Rar, Zip, Gzip y Bzip2 y formatos de correo Mbox, Maildir y ficheros crudos de correo.

3.12. SpamAssassim

SpamAssassim es un filtro de correo que trata de identificar el spam mediante el análisis del texto y el uso en tiempo real de algunas listas negras a través de Internet.

A partir de su base de datos de reglas, utiliza un amplio abanico de pruebas heurísticas en las cabeceras y el cuerpo de los correos para identificar el spam, también conocido como correo electrónico comercial no solicitado. Una vez identificado, el correo puede ser opcionalmente marcado como spam o más tarde filtrado usando el cliente de correo del usuario.

SpamAssassim normalmente identifica acertadamente entre un 95 y un 99% del spam, dependiendo del tipo de correo que se reciba. También incluye soporte para informar de mensajes de spam, automática o manualmente, a bases de datos como Vipul's Razor.

3.13. Herramientas de Seguridad

3.13.1. Servicio de Seguridad

La autenticación puede contribuir al desarrollo de confianza entre las partes involucradas en todos los tipos de transacciones tras abordar sólo un conjunto de medidas de seguridad, aseguran que cada interlocutor es quién dice ser.

Define mecanismos para garantizar la procedencia de la información, ya sea a nivel de usuario o de computadora.

Permite a un usuario firmar un documento antes de enviarlo, lo cual permite:

- Tener certeza de que el documento no ha sido modificado puesto que ha sido firmado, si se alterara el mensaje la firma no sería válida.
- Verificar que el documento ha sido firmado por una determinada persona.

3.13.2. Soporte Criptográfico

Para asegurar la confidencialidad de la información es posible codificar la información intercambiada mediante el uso de la criptografía de mensajes. Los mensajes son cifrados por el remitente y descifrados por el destinatario, utilizando claves que solamente ellos conocen.

De esta manera, los datos de los correos electrónicos que transitan por las redes y servidores de Internet están codificados, y son totalmente ininteligibles para terceras personas que pudieran hacer un uso fraudulento de tales datos.

3.13.3. Manejo de Certificados digitales

Un certificado digital es un contenedor de datos que alberga identidades (por ejemplo, de una persona, sus nombres, dirección email) con un par de claves cifradas públicas y/o privadas. Los certificados se usan en una gran variedad de contextos de seguridad en red para establecer la autenticación y privacidad entre usuarios de red y usuarios de aplicaciones.

3.13.4. Estructura de los mensajes

La estructura de los mensajes determina la manera en que va a estar compuesto por que en ella se encuentran varios paquetes que indica de qué tipo de se trata y demás parámetros que contiene un mensaje de correo electrónico. Determina además como protege los datos o el flujo de información frente a accesos, modificaciones, pérdidas, etc.

3.13.5. Accesibilidad

Determinar si puede ser implementado un servicio de correo electrónico seguro en diferentes ámbitos en que van a hacer utilizados por un número de usuarios, la accesibilidad a una licencia, documentación para su utilización y un manejo adecuado del servicio.

3.14. Open-Xchange

Open-Xchange nació como alternativa directa a Microsoft Exchange, incluida inicialmente en la distribución SUSE Linux. Con el tiempo, desarrollo e inversión, Open-Xchange ha crecido hasta convertirse en un actor relevante con más de 100 millones de usuarios en todo el mundo, gracias a que es una de las opciones preferidas por proveedores de servicios de Internet.

A grandes rasgos Open-Xchange se bifurca en cuatro ramas:

- OX Cloud es una solución de productividad y correo electrónico administrada y alojada que combina OX App Suite con el backend OX Dovecot Pro.
- OX App Suite es una plataforma modular diseñada para ofrecer una amplia gama de servicios basados en la nube, como correo electrónico, almacenamiento en la nube, intercambio de archivos, edición de documentos, colaboración y más.
- OX Dovecot Pro es una solución de servidor IMAP altamente confiable, escalable y compatible, diseñada para empresas que dependen del correo electrónico.
- OX PowerDNS es una plataforma DNS completa para servidores de dominios e ISP. Ofrece resolución de DNS de alto rendimiento para infraestructuras autorizadas y recursivas.

Asimismo, tampoco es imprescindible la migración al adoptar Open-Xchange, ya que se integra con los servicios de terceros más conocidos, incluyendo por supuesto a Microsoft Exchange, por lo que la interoperabilidad está asegurada.

Open-Xchange OXtender 2 para Microsoft Outlook permite a los usuarios mantener su cliente Outlook familiar cuando su organización se traslada a Open-Xchange Server. Los usuarios se sienten como en casa trabajando con su interfaz de Outlook mientras, en segundo plano, OXtender sincroniza correos electrónicos, calendario, contactos y tareas, junto con las carpetas públicas, compartidas y del sistema. La sincronización en

tiempo real permite tiempos de respuesta rápidos, por lo que los equipos pueden trabajar de la manera más eficiente posible.

OX App Suite una plataforma de colaboración, comunicación y correo electrónico fácil de usar, brinda acceso a una amplia gama de aplicaciones de etiqueta blanca. Desde correo electrónico seguro hasta almacenamiento en la nube y capacidades de oficina en línea, OX App Suite está diseñado para brindar velocidad y eficiencia.

OX App Suite fue construida con estándares abiertos de fuente optimizada para compañías con 5 a 5.000 empleados. Permite a sus empleados de todo el mundo comunicar e intercambiar rápida y eficientemente la información. Usando apenas un navegador, los empleados pueden tener acceso a todos sus e-mails, así como su depósito de documentos, tareas, contactos, calendario, favoritos en cuestión de segundos, sin importar su localización física.

Para el usuario final el software de Open-Xchange es equiparable a soluciones en la nube como las repetidas Microsoft Office 365 o Google Apps y nada mejor que probarlo en la demo en línea. Para el administrador de sistemas encargado de implementarlo, no obstante, hay ventajas considerables, comenzando por su integración con las principales soluciones de automatización (CPanel, Parallels Plesk).

3.14.1. OX Documents (OX Text, OX Spreadsheet, OX Presentation)

Los documentos OX son productos basados en navegador, listos para la nube, de texto, hojas de cálculo y presentaciones que pueden funcionar con documentos de Microsoft Office y OpenOffice sin pérdidas. Y también puede colaborar con otras personas para editar documentos compartidos en varios dispositivos. OX Presentation es un editor de presentaciones en línea que se siente y funciona como un editor fuera de línea. OX Text es una solución de procesamiento de texto colaborativa basada en la nube. OX Spreadsheet es una solución de hoja de cálculo basada en la nube.

3.14.2. OX Drive

En OX App Suite, Open-Xchange proporciona un almacenamiento en la nube llamado OX Drive este permite almacenar y compartir sus fotos, archivos, documentos y videos, en cualquier momento y en cualquier lugar. Acceda a cualquier archivo que guarde en OX Drive desde todas sus computadoras, iPhone, iPad o desde el propio OX App Suite. Proporciona sincronización de archivos y carpetas en varios dispositivos de la forma más sencilla para el usuario final, totalmente optimizado para cada tipo de dispositivo.

3.14.3. OX Sync Conector para movilidad empresarial (ActiveSync)

La información y la comunicación móvil son factores clave para lograr el éxito en el mundo empresarial. Por tanto, es muy importante que los trabajadores sean capaces de sincronizar correo electrónico y datos almacenados entre el servidor groupware de la empresa y su teléfono móvil.

La solución que ofrece Open-Xchange para esta tarea es OXtender for Business Mobility y dispone de las siguientes características (se requiere una licencia válida de Open-Xchange):

- A nivel técnico, está basada en el protocolo Microsoft Exchange ActiveSync
- Permite la sincronización automática en modo push de correos electrónicos, citas, tareas y contactos entre el teléfono móvil y el servidor Open- Xchange.
- Fácil de instalar
- Se integra de forma transparente con las aplicaciones que ya incorporan los teléfonos móviles

3.14.4. Sincronización de contactos Open-Xchange con CardDAV y CalDAV

Se puede acceder al servidor Open-Xchange a través de sus interfaces CalDAV y CardDAV para permitir la sincronización de datos de calendario y contactos con aplicaciones externas como los clientes de agenda y libreta de direcciones de Mac OS.

CalDAV y CardDAV son protocolos estándar para el intercambio de datos de calendario y datos de direcciones, respectivamente. La interfaz de CalDAV publica todas las carpetas de calendario del usuario a través de CalDAV para que el usuario pueda suscribirse a ellas en una aplicación cliente. Del mismo modo, la interfaz CardDAV publica las carpetas de contactos del usuario. Dependiendo del cliente utilizado, el usuario puede suscribirse a una o más carpetas, o acceder a todos los datos disponibles de forma agregada.

3.14.5. OX Sync App

La aplicación OX Sync es una aplicación nativa para teléfonos móviles creada específicamente para usuarios de teléfonos inteligentes con Android, que también tienen una cuenta válida de OX App Suite. La aplicación está diseñada para permitir a los usuarios sincronizar su entorno de citas, tareas y contactos de OX App Suite directamente desde un cliente de teléfono móvil nativo. Sobre la base de la implementación como adaptador de sincronización, se integra perfectamente con las aplicaciones de contactos y calendario de Android predeterminadas.

3.14.6. OX Guard

Es un complemento de seguridad totalmente integrado a OX App Suite que proporciona a los usuarios finales una solución flexible de cifrado de archivos y correo electrónico. OX Guard es una solución altamente escalable, de múltiples servidores y rica en funciones que es tan fácil de usar que los usuarios finales realmente

la usarán. Con un solo clic, un usuario puede tomar el control de su seguridad y enviar correos electrónicos seguros y compartir archivos cifrados. Esto se puede hacer desde cualquier dispositivo tanto para los usuarios de OX App Suite como para los que no son de OX App Suite.

OX Guard utiliza cifrado PGP estándar para el cifrado de correo electrónico y archivos. PGP ha existido durante mucho tiempo, pero realmente no se ha popularizado entre las masas. Esto generalmente se atribuye a la confusión y las complicaciones de administrar las claves, comprender la confianza, los tipos de formato PGP y la falta de repositorios de claves centrales confiables. Guard simplifica todo esto, haciendo que el cifrado PGP sea tan fácil como un proceso de un clic, sin claves para realizar un seguimiento, pero las opciones de administración avanzada de PGP para aquellos que saben cómo hacerlo.

3.14.7. Herramientas y configuraciones adicionales de Open-Xchange

- **Visor de documentos Open-Xchange:** OX Document Viewer ofrece funciones de visualización de documentos sin complementos para Microsoft Office (.docx, .doc, .rtf, .pptx, .ppt, .xlsx, xls) y OpenDocument (.odt, .ods, .odp,. odg) tipos de archivo, así como para el formato de documento portátil (.pdf). Extiende OX App Suite con miniaturas de contenido y capacidades de vista previa (se requiere una licencia válida de Open-Xchange).
- **Convertidor de imágenes Open-Xchange:**

OX App Suite muestra imágenes (fotos y gráficos) de muchas formas diferentes:

1. Miniaturas
2. Iconos
3. Imágenes incrustadas en documentos
4. en correos electrónicos
5. en una ventana emergente propia.

El procesamiento de imágenes lo realiza el middleware OX y no un servicio dedicado, por lo que el middleware puede consumir mucho tiempo de la CPU solo para convertir imágenes a diferentes formatos de destino. Además, el middleware OX no almacena imágenes en caché durante más tiempo. Solo las miniaturas se almacenan en caché, ya sea por la base de datos o por el sistema de archivos. Estas imágenes se convierten a los formatos requeridos (por ejemplo, jpeg, png) cuando lo solicita una acción del usuario en la interfaz de usuario.

Con OX App Suite 7.10 existe una alternativa para procesar imágenes mediante el middleware OX. La conversión y entrega de imágenes se puede delegar a un servicio adicional, el servidor OX ImageConverter.

Su modelo de implementación corresponde exactamente al servidor de convertidor de documentos a través de un servicio cliente / servidor.

La separación del servicio ImageConverter tiene las siguientes ventajas:

Configuración y uso de uno o más almacenamientos separados Mejoras de rendimiento a través de caché persistente Procesamiento previo de formatos y tamaños predefinidos (los valores predeterminados son automático: 200x150, automático: 480x320, automático: 640x480, automático: 800x600, automático: 1280x720, automático: 1920x1080 ") si la resolución de la imagen de origen lo permite. El mejor tamaño coincidente se entregará sin una nueva conversión, si el navegador Middleware solicita una imagen, es capaz de almacenar en caché esas imágenes No hay límites para el tamaño de las imágenes El formato de destino predeterminado se especifica mediante configurado, formatos predefinidos. Al utilizar el formato de destino 'auto' (junto a 'jpg' o 'png'), las imágenes de origen opacas se convierten en imágenes de destino JPEG y las imágenes transparentes se convierten en imágenes de destino PNG. Reduzca la carga de OX Middleware.

3.14.8. Open-Xchange Presenter

OX Presenter permite presentaciones locales y remotas de documentos de presentación (se requiere una licencia válida de Open-Xchange).

3.14.9. Cluster-Setup

Para la comunicación entre OX a través de la red, varios servidores Open-Xchange pueden formar un clúster. Esto trae diferentes ventajas con respecto a la distribución y almacenamiento en caché de datos volátiles, equilibrio de carga, escalabilidad, seguridad ante fallas y robustez. Además, proporciona la infraestructura para las próximas funciones del servidor Open-Xchange. Las capacidades de agrupación en clústeres del servidor Open-Xchange se basan principalmente en Hazelcast, una plataforma de distribución de datos en clúster de código abierto y altamente escalable para Java.

3.15. Zimbra

La suite de colaboración Zimbra (en inglés, Zimbra Collaboration Suite o ZCS) es un programa informático colaborativo o Groupware que consta de un servicio de correo electrónico creado por Zimbra Inc. compañía ubicada en San Mateo, California. La compañía fue adquirida por Yahoo! Inc. por aproximadamente 350 millones de dólares en septiembre de 2007, acordando mantener sus estándares de código abierto El 12 de enero de 2010 fue nuevamente vendida por Yahoo a VMware En julio de 2013 Telligent adquirió la suite de VMware.

Zimbra se trata de un paquete de aplicaciones basado en la web y que se puede implementar como una nube privada en las instalaciones o en forma de servicio de nube pública externa. Está diseñada para la

implementación empresarial con el objetivo principal de integrar una gran cantidad de herramientas de colaboración.

Admite clientes de correo electrónico de escritorio, como Windows Outlook, y muestra compatibilidad con sistemas informáticos Windows, Linux y Apple. Además, proporciona sincronización inalámbrica con sistemas operativos de dispositivos móviles como iOS, Windows Mobile, BlackBerry y Android.

3.15.1. Mensajería y colaboración

Conecte a los usuarios a sus nubes personales con un buzón más inteligente que integra correo electrónico, tareas, libreta de direcciones, calendario, archivos y aplicaciones empresariales.

Chat institucional con Zimbra Chat

- Comuníquese con otros usuarios directamente desde Zimbra Web Client.
- Invita y elimina usuarios de la lista de amigos y asigna apodos.
- Comience a chatear con un simple clic.
- Muestra tu estado de ánimo en el chat con emojis.
- Cambia entre cuatro mensajes de estado: Disponible, Ausente, No molestar o Invisible.
- Active Zimbra Chat Zimlet y sus usuarios estarán listos para comenzar a chatear.

3.15.2. Administración simplificada

La Consola de Administración Web AJAX, simplificada y orientada a tareas, permite la administración en cualquier lugar Servicios integrados anti-Spam, antivirus y de directorio (LDAP, Active Directory).

Administre las características del usuario final, las cuotas y las políticas de almacenamiento a través de Class-of-Service (CoS).

Los asistentes de migración permiten a los clientes migrar rápida y fácilmente desde entornos de Microsoft Exchange y Domino a Zimbra.

3.15.3. En cualquier lugar y dispositivo

Sincronización con iOS (iPhone, iPad), teléfonos inteligentes y tabletas basados en Windows y Android, utilizando IMAP / POP, CalDAV y CarDAV.

Experiencia enriquecida basada en navegador para correo electrónico, contactos, calendario y archivos de Zimbra en cualquier dispositivo compatible con xHTML.

Podemos resumir entonces que Zimbra es una solución líder de administración de emails, calendario, contactos y tareas. Se trata de un software de groupware completo que ofrece enormes ventajas para usuarios corporativos y administradores de sistemas, tales como:

- **Ahorro:** con relación a otros programas similares comoB Roundcube o MS Exchange, los costes de gestión de Zimbra suponen un ahorro significativo, en algunos casos de más del 50%.
- **Plataforma OpenSource:** La versión de código abierto de Zimbra permite que los distintos desarrolladores de la comunidad puedan contribuir a ir mejorando el programa de forma sucesiva, multiplicando así las posibilidades del mismo.
- **Accesibilidad:** Al tratarse de un servicio alojado mediante cloud computing, permite al usuario el acceso desde cualquier lugar en el que disponga de una conexión a Internet.
- **Personalización:** las múltiples opciones que posibilita el trabajo de la comunidad nos permite una personalización según las necesidades del usuario.
- **Interfaz de administración basado en AJAX:** gracias a la combinación de Javascript con XML la web puede actualizar cambios sin necesidad de recargarse, creando de esta forma una aplicación interactiva.
- **Interfaz de comandos:** Incluye una consola para la introducción de comandos y de esta forma dar instrucciones al programa.
- **API para integración bidireccional con CRM, ERP, etc.**
- **Escalabilidad:** Zimbra nos permite incrementar la capacidad de trabajo sin perjudicar el funcionamiento del mismo, consiguiendo resultados realmente sorprendentes.
- **Seguridad:** gracias al sistema de código abierto podemos disponer de un programa extremadamente transparente y de esta forma mucho más seguro, puesto que este permite que el código sea revisado y se realicen controles de seguridad permanentemente.

3.15.4. Historia

El programa Zimbra apareció a finales de 2003, de la mano de tres informáticos que trabajaban en Silicon Valley: Satish Dharmaraj, Ross Dargahi y Roland Schemers. Tras la venta de la empresa en 2007, los tres se integraron en Yahoo!, así como el CEO Scott Dietzen Satish Dharmaraj abandonaría la compañía en 2009.

En un principio pensaron crear un programa de correo electrónico, cuyo primer prototipo desarrollaron rápidamente. Tras varios meses de trabajo, lograron ensamblar un sistema básico a partir de partes de código libre disponibles en la web. Lo bautizaron Zimbra, en honor a una canción del grupo estadounidense de rock Talking Heads. Publicaron el código en internet e invitaron a desconocidos a ofrecer sugerencias y el programa fue evolucionando gracias al aporte de colaboradores.

En octubre de 2005 la compañía lanzó comercialmente su producto a precio de descuento en un mercado dominado por Microsoft. Al igual que el programa de correo electrónico Exchange, de Microsoft, Zimbra permitía a los empleados de una empresa enviar, recibir, guardar y buscar los mensajes procesados cada día. En 2009 alcanzó la cifra de 40 millones de buzones de correo, superando los 31,4 millones de cuentas gratuitas que ofrecía Google Mail, en gran parte debido a la decisión de Comcast de usar Zimbra para sus cuentas de correo. En agosto de 2010 había superado el número de 60 millones de buzones de correo distribuidos entre 150.000 clientes.

3.15.5. Características

El servidor ZCS hace uso de proyectos de código abierto existentes como Postfix, MySQL, OpenLDAP y Lucene. cuenta con una interfaz de programación de aplicaciones basado en SOAP para toda su funcionalidad y actúa como servidor IMAP y POP3 de correo electrónico.

El cliente web ZCS es una interfaz de colaboración y administración completa creada empleando el Toolkit Zimbra. Soporta correos electrónicos y calendarios a través de una interfaz web basada en AJAX. Incluye capacidades de búsqueda avanzada, calendario compartido y relaciones de fechas.

ZCS es compatible con clientes propietarios tales como Microsoft Outlook, Novell Evolution y Apple Mail. También provee soporte de sincronización nativo de dos vías para muchos dispositivos móviles: Nokia serie E, BlackBerry y Blackeberry Enterprise Server, Windows Mobile, entre otros.

Proyectos open source en los que se basa:

- Postfix (servidor de correo).
- MySQL (gestor de bases de datos).
- OpenLDAP (servicio de directorio).
- Apache Tomcat, sustituido por Jetty desde la versión 5.0 (servidor web).
- Lucene (motor de búsquedas).
- Verity (motor de búsquedas).
- ClamAV (antivirus).
- SpamAssassin (filtro antispam).
- Amavis y Amavisd-new (antivirus para correo electrónico).
- DSPAM (filtro antispam).
- Aspell (corrector ortográfico).
- Apache James (servidor de correo).
- Sieve (filtro de correo electrónico).

- Perdition mail retrieval proxy (hasta la versión 4.5)
- nginx, desde la versión 5.0 (servidor web inverso).

3.15.6. Ventajas Generales

Según las empresas que ya han migrado a Zimbra, permite un ahorro de costes de al menos 50% en comparación con MS Exchange o IBM Lotus o Roundcube

El conector para MS Outlook permite una sincronización nativa al servidor Zimbra. Gracias al potente interfaz fácil e intuitivo, los usuarios de Zimbra se sienten muy cómodos trabajando con el producto.

Algunas otras ventajas de implementar Zimbra es su empresa son las siguientes:

Para el Administrador

- Bajo costo en la gestión del sistema.
- Sistema nativo de almacenamiento.
- Jerárquico (HSM / ILP).
- Soporte para Multi-Dominio con administración desde un único nodo.
- Restauración de un único buzón por usuario, desde la consola.
- Traspaso Online de buzones entre servidores (y backups).
- Solución de alta disponibilidad integrada.
- Interfaz de administración basado en AJAX.
- Dashboards gráficos de rendimiento.
- Interfaz de comandos por consola.
- Integración SOAP para labores de administración.
- Consolidación del servidor de hosting y el almacenamiento.
- Una copia del correo electrónico y los adjuntos por servidor, en vez de un correo electrónico por usuario.
- Reducción significativa del uso de la CPU – Multi-level caching y optimización del sistema.
- Compatibilidad con infraestructuras existentes.
- Web services – API para integración bidireccional con CRM, ERP, etc.
- Clientes – Outlook, Móviles, IMAP, POP, iCalendar, RSS, etc.
- Directory – Integración Active Directory/LDAP Messaging Server – Coexistencia y herramientas de migración Seguridad.
- Web security model – Single sign-on, TLS/SSL, no es necesario utilizar VPN.
- Apertura segura de adjuntos.

- SpamAssassin y ClamAV incluídos.
- Compatible con servicios anti-spam/anti-virus existentes (via Postfix y amavisd-new).

Para el Usuario

- Elección libre del cliente.
- Navegadores – Zimbra Ajax client.
- Clientes para PC – Outlook (Online, Offline, Modo Cache), Apple Mail e iCal, Eudora, Evolution, Thunderbird/Sunbird, RSS, etc. Móviles – Dispositivos.
- Inalámbricos «sincronización sin cables»: Blackberry, Palm, Nokia, Motorola, Good, PocketPC, etc.
- Perfecta organización de los buzones Avanzado y potente sistema de búsqueda (incluyendo los mensajes adjuntos).
- Guardado de las búsquedas más habituales.
- Visualización de los correos por conversación.
- Filtros de correo.
- Calendario en equipo.
- Gestión de reuniones libre/ocupado.
- Múltiples calendarios por usuario.
- Compartir y delegar calendarios.
- Suscripción a calendarios externos con formato .ics
- Integración del correo electrónico con otras aplicaciones, vía arrastrar y soltar.
- Intranet – ERP, CRM, Support, Finance, HR, VoIP phone, etc.
- Internet Google/Yahoo Maps, Skype, Travel, Package Tracking, etc.
- Sistema eficiente de comprensión de texto en los correos electrónicos.
- Ver/Crear citas en el calendario, tan sólo con pasar el ratón por una palabra o fecha dentro del correo electrónico.
- Crear/Editar contactos, con tan sólo pasar el ratón por encima del contacto dentro del correo electrónico.
- Vista rápida de la página Web, al pasar el ratón por encima del contacto dentro del correo electrónico.
- Desde cualquier equipo, a cualquier hora Potente interfaz Web con tecnología AJAX Seguridad sin VPN.
- Opción segura para abrir los adjuntos Sistema moderno de colaboración RSS/ATOM noticias.

3.16. Kopano

Kopano es una suite de aplicaciones de software colaborativo de código abierto originalmente basada en Zarafa. La versión inicial de Kopano Core (KC) se bifurcó a partir del lanzamiento actual de Zarafa Collaboration Platform, y reemplazó a ZCP en términos de linaje, ya que ZCP cambió al modo de mantenimiento con parches que fluyen desde KC. Kopano WebApp descendió de manera similar de Zarafa WebApp. Desde octubre de 2017, Kopano Core también se conoce más específicamente como Kopano Groupware Core, ya que Kopano BV desarrolló más productos que no requerían directamente componentes de groupware.

El complemento Kopano Outlook Extension para Outlook proporciona la funcionalidad de Outlook que ActiveSync por sí solo no admite. Esto incluye (por ejemplo) compatibilidad con Carpetas públicas o Fuera de la oficina. Por lo tanto, ActiveSync y Kopano Outlook Extension juntos pueden integrar completamente el backend de Kopano dentro de Outlook en un entorno corporativo.

Los complementos de aplicaciones web existen para realizar tareas grupales avanzadas, como acceder a soluciones de almacenamiento basadas en la nube (por ejemplo, owncloud / nextcloud), para videoconferencias integradas (reuniones web) o para manejar el correo electrónico S / MIME dentro de la aplicación web.

También está disponible una aplicación de escritorio, DeskApp. Tiene el mismo aspecto que la aplicación web, pero se integra directamente con el escritorio del usuario y está disponible para Windows, Linux o Mac.

Todos los componentes del lado del servidor (Kopano Core) y la aplicación web se publican bajo la licencia pública general de Affero (AGPL).

3.16.1. Tecnología

Microsoft Outlook, así como los clientes de Kopano / Zarafa, utilizan MAPI a nivel de código fuente. Los llamados proveedores MAPI (esencialmente complementos) abstraen y se encargan del mecanismo de transporte subyacente. Kopano-server expone su funcionalidad a través de sockets de flujo y utiliza el protocolo HTTP, y los datos se serializan mediante SOAP / XML. Los comandos enviados en los datos XML son específicos de Kopano / Zarafa. Por el contrario, el proveedor MAPI de Kopano implementa este protocolo en el lado del cliente. Estas conexiones HTTP se pueden proteger con TLS / SSL y, si se desea, se pueden utilizar como proxy.

Debido a que Exchange usa MAPI / RPC en el cable, el conector de Outlook estándar para Exchange no se podía usar y tradicionalmente requería la versión de Windows del proveedor MAPI de Zarafa (un producto que es propietario y no es compatible desde 2016-04). Las versiones de Outlook 2013 y 2016 son compatibles

con ActiveSync, un protocolo que también utilizan muchos clientes móviles, y al usar el software Z-push en el lado del servidor, las solicitudes de ActiveSync se pueden traducir y dichos clientes también pueden comunicarse de manera efectiva con un servidor Kopano.

Kopano Core generalmente almacena sus datos en una base de datos compatible con MySQL. Los archivos adjuntos se pueden guardar en el sistema de archivos, Amazon S3, o se puede usar la base de datos para colocar blobs fragmentados. El servidor puede obtener su información de usuario de LDAP / Active Directory, cuentas de usuario de Unix o la base de datos MySQL. Se proporcionan pasarelas adicionales para los protocolos IMAP, POP3 e iCalendar / CalDAV.

Kopano WebApp (y DeskApp, que es la aplicación independiente equivalente) son aplicaciones con todas las funciones que incluyen soporte para correo, calendarios, calendarios de grupo, carpetas públicas y muchas más funcionalidades. La aplicación web se puede integrar con muchos complementos que se pueden agregar a la instalación. Kopano proporciona varios complementos, como Archivos (acceso a la nube y almacenamiento dentro de la aplicación web), WebMeetings (videoconferencia) y S / MIME (que permite leer y enviar correo electrónico cifrado).

Sin embargo, cualquier desarrollador puede escribir complementos adicionales utilizando la API de complementos de la aplicación web.

3.16.2. Edición

Kopano está disponible como una edición comunitaria de descarga gratuita. La edición comunitaria brinda a los usuarios acceso a las compilaciones de la rama principal, que incluye el código más reciente como compilaciones nocturnas. La edición comunitaria Kopano incluye todas las funciones avanzadas y premium como WebMeetings (videoconferencia), Kopano Files (acceso al almacenamiento en la nube) y el complemento S / MIME (que permite enviar o recibir correo electrónico cifrado).

Kopano también está disponible como un producto de pago donde las versiones oficiales de Kopano QA probadas son proporcionadas y respaldadas directamente por Kopano.

Finalmente, Kopano está disponible en los repositorios oficiales de algunas distribuciones de Linux como OpenSUSE.

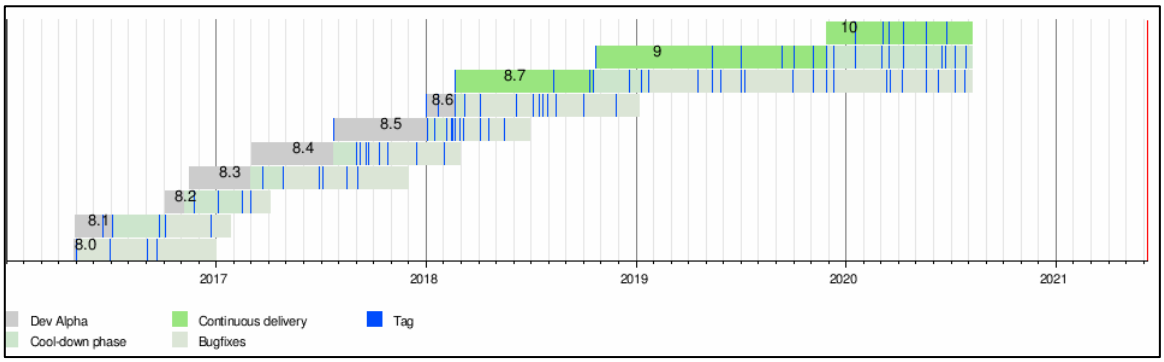

Figura 8. Ediciones KOPANO

3.16.3. Migración

La plataforma de colaboración de código abierto de Kopano es bien conocida como una de las mejores alternativas de Microsoft Exchange. Aquellos que migraron de Exchange a Kopano saben que pueden brindar más y mejores servicios y han visto que sus costos son incluso inferiores a los de los servicios en la nube como Office365 y Google Apps.

3.16.4. WebApp

Te ayuda a administrar tu correo electrónico con una vista limpia y completa de tus carpetas personales y compartidas con una interfaz muy similar a Microsoft Outlook.

Como WebApp funciona con la mayoría de los navegadores, no necesitará instalar ninguna aplicación para administrar sus comunicaciones dondequiera que se encuentre**.**

3.16.5. Kopano WebMeetings y chat

Los correos electrónicos siguen siendo la forma más eficiente de enviar mensajes que no requieren una respuesta inmediata pero seguramente nada mejor que poder interactuar con colegas, clientes o proveedores en tiempo real para intercambiar ideas.

Kopano integra una plataforma de videoconferencia y mensajería instantánea que te permite interactuar con otras personas con la mejor herramienta para la tarea estés donde estés.

Con Kopano puede participar en conferencias web utilizando la mayoría de los navegadores, ya que utiliza componentes nativos, como WebRTC, por lo que no es necesario instalar aplicaciones adicionales o esperar a que se carguen los subprogramas de Java.

Kopano WebMeetings le permite compartir presentaciones y la pantalla de su escritorio para realizar presentaciones profesionales, editar documentos con el equipo o brindar sesiones de soporte remoto.

Ya no es necesario reservar salas de videoconferencia, todo lo que necesita es solo un navegador. Puede invitar a sus colegas, que establezcan su presencia en línea como "Disponible", a reuniones web instantáneas y enviar a los participantes externos una invitación por correo electrónico con un par de clics.

3.16.6. Tus archivos donde los necesites

Archivos se integra perfectamente con todas las funciones de correo electrónico y calendario que ofrece WebApp. Crear un nuevo correo electrónico con la última versión de una presentación es fácil: se puede hacer con unos pocos clics sin tener que descargarlo primero.

Almacenar un archivo entrante es igual de fácil. Cualquier archivo adjunto se puede guardar en el almacenamiento de red existente de su empresa, donde se puede compartir con sus compañeros de trabajo. Y funciona desde cualquier navegador, en cualquier lugar.

Servicios de colaboración para cada necesidad

No todas las organizaciones que buscan un paquete de software colaborativo completo necesitan el mismo nivel de colaboración, rendimiento y soporte. Por lo tanto, puede obtener la plataforma de colaboración de código abierto de Kopano en varias ediciones diferentes:

- **Kopano Basic:** es ideal para pymes, ya que incluye todas las características que generalmente requieren un número menor de usuarios y un costo que compite muy bien incluso con las ofertas de Cloud.
- **Kopano Professional:** está diseñado para organizaciones que requieren funciones avanzadas como análisis de sistema extendido (a través de Kopano Dashboard), archivos avanzados para equipos y reuniones web, soporte por correo electrónico y teléfono.
- **Kopano Enterprise:** está dirigido a organizaciones que necesitan una solución agrupada. La compatibilidad con varios servidores se puede utilizar para admitir un mayor número de usuarios o para distribuir los buzones de correo en diferentes ubicaciones geográficas. Enterprise Edition combina las funciones de colaboración más amplias con el más alto nivel de soporte.

La siguiente tabla presenta un resumen de las principales diferencias entre versiones:

	Básico	Profesional	Empresa	Comunidad
Conector de Outlook (MAPI)	3 usuarios	✓	✓	✓
Aplicación Web	✓	✓	✓	✓
ActiveSync (Z-Push)	✓	✓	✓	✓
Puerta de enlace IMAP / POP3	✓	✓	✓	✓
Puerta de enlace iCal / CalDAV	✓	✓	✓	✓
Calendarios multiusuario avanzados		✓	✓	✓
Copia de seguridad a nivel de bloque		✓	✓	✓
Kit de herramientas del directorio activo		✓	✓	✓
Monitoreo de Kopano		Básico	Análisis extendido	Análisis multiservidor
Kopano Files Personal		✓	✓	✓
Archivos Kopano para equipos		Opción	✓	✓
Kopano WebMeetings		Opción	✓	✓
Herramientas de implementación automática			✓	✓
Soporte de alta disponibilidad			✓	✓
Soporte técnico de Kopano Archive			✓	✓
Multi Alquiler				✓
Soporte multiservidor				✓

3.16.7. ¿Qué es Univention Corporate Server?

Univention Corporate Server (UCS) es un sistema operativo de servidor basado en Linux para la operación y administración de infraestructuras de TI para empresas y autoridades. UCS implementa un concepto integrado y holístico con una administración central consistente y puede garantizar el funcionamiento de todos los componentes en un contexto de seguridad y confianza interrelacionado, el llamado dominio UCS. Al mismo tiempo, UCS admite una amplia gama de estándares abiertos e incluye amplias interfaces para componentes de infraestructura y herramientas de gestión de otros fabricantes, lo que significa que se puede integrar fácilmente en entornos existentes.

UCS consiste en un software de código abierto confiable probado y probado en organizaciones de diferentes tamaños. Estos componentes de software se integran juntos a través del sistema de gestión UCS. Esto permite la fácil integración y administración del sistema en entornos distribuidos o virtualizados simples y complejos.

Las funciones centrales de UCS son:

- Gestión de identidad / infraestructura flexible y extensa para la administración central de servidores, estaciones de trabajo, usuarios y sus permisos, aplicaciones de servidor y servicios web.
- Servicios para integrar la gestión de dominios de Microsoft Active Directory existentes o incluso la prestación de dichos servicios como alternativa a los sistemas de servidor basados en Microsoft.
- App Center para una instalación y gestión sencillas de extensiones y aplicaciones
- Funciones integrales para el funcionamiento de sistemas virtualizados (por ejemplo, ejecutar un sistema operativo Windows o Linux) en la nube o en sistemas UCS que se ejecutan localmente
- Servicios de red e intranet para la administración de DHCP y DNS
- Servicios de archivo e impresión
- Administración y monitoreo de computadoras
- Servicios de correo

Estas funciones las proporcionan diferentes paquetes de software en Univention Corporate Server y básicamente, los paquetes de software contenidos en UCS se pueden asignar a las siguientes tres categorías principales:

1. Sistema base
2. Sistema de gestión UCS con Univention Management Console

3. Univention App Center, que permite la instalación de más componentes y aplicaciones de otros proveedores de software.

El sistema base abarca el sistema operativo de la distribución UCS Linux mantenida por Univention y basada en Debian GNU / Linux. Incluye en gran medida la misma selección de software que Debian GNU / Linux, así como herramientas adicionales para la instalación, actualización y configuración de clientes y servidores.

El sistema de gestión UCS realiza un único punto de administración donde las cuentas de todos los miembros del dominio (usuarios, grupos y hosts) y servicios como DNS y DHCP se gestionan en un único servicio de directorio. Los componentes centrales del sistema de gestión son los servicios OpenLDAP (servicio de directorio), Samba (prestación de servicios de dominio, archivos e impresión para Windows), Kerberos (autenticación e inicio de sesión único), DNS (resolución de nombres de red) y SSL / TLS (seguridad transmisión de datos entre sistemas). Se puede utilizar a través de una interfaz web (Univention Management Console) o en la línea de comandos y en scripts individuales. El sistema de gestión UCS se puede ampliar con API (interfaces de programación de aplicaciones) y proporciona una arquitectura cliente-servidor flexible que permite que los cambios se transfieran a los sistemas implicados y se activen allí.

Los componentes adicionales de Univention y otros fabricantes se pueden instalar fácilmente usando el App Center. Amplían el sistema con numerosas funciones como groupware, gestión de documentos y servicios para Windows, lo que significa que también pueden ejecutarse desde un sistema UCS y administrarse a través del sistema de gestión UCS.

- **Descripción general de UCS**

Linux es un sistema operativo que siempre se centró en la estabilidad, seguridad y compatibilidad con otros sistemas operativos. Por lo tanto, Linux está predestinado para ser utilizado en sistemas operativos de servidor que sean estables, seguros y de alta disponibilidad.

Construido sobre esa base, UCS es un sistema operativo de servidor que está optimizado para la operación y administración simples y seguras de aplicaciones y servicios de infraestructura en empresas y autoridades. Para una gestión eficiente y segura, estas aplicaciones dependen de la estrecha integración en la gestión de permisos y usuarios del sistema de gestión UCS.

UCS puede utilizarse como base para la infraestructura de TI en empresas y autoridades y proporcionar el control central para ello. Esto hace una contribución considerable a la operación de TI segura, eficiente y

rentable. Las aplicaciones críticas para el negocio están integradas en un concepto uniforme, adaptadas entre sí y preconfiguradas para uso profesional. Alternativamente, se puede operar como parte de un dominio de Microsoft Active Directory existente.

- **Servicio de directorio LDAP**

Con el sistema de gestión UCS, todos los componentes del dominio UCS se pueden administrar de forma centralizada a través de la computadora, el sistema operativo y los límites del sitio. Por lo tanto, proporciona un único punto de administración para el dominio. Un elemento principal del sistema de gestión UCS es un directorio LDAP en el que se almacenan los datos necesarios en el dominio para la administración. Además de las cuentas de usuario y elementos similares, también se guarda allí la base de datos de servicios como DHCP. La gestión de datos central en el directorio LDAP evita no solo la entrada repetida de los mismos datos, sino que también reduce la probabilidad de errores e inconsistencias.

Un directorio LDAP tiene una estructura en forma de árbol, cuya raíz forma la denominada base del dominio UCS. El dominio UCS forma el contexto común de seguridad y confianza para sus miembros. Una cuenta en el directorio LDAP establece la membresía en el dominio UCS para los usuarios. Las computadoras reciben una cuenta de computadora cuando se unen al dominio. Los sistemas Microsoft Windows también pueden unirse al dominio de modo que los usuarios puedan iniciar sesión allí con su pasaporte de dominio.

UCS utiliza OpenLDAP como servidor de servicio de directorio. El directorio lo proporciona el controlador de dominio maestro y se replica en todos los controladores de dominio (DC) del dominio. El directorio LDAP completo también se replica en una copia de seguridad de CC, ya que puede reemplazar al maestro de CC en caso de emergencia. Por el contrario, la replicación en esclavos DC se puede restringir a ciertas áreas del directorio LDAP utilizando ACL (listas de control de acceso) para realizar una replicación selectiva. Por ejemplo, esto puede ser deseable si los datos solo deben almacenarse en el menor número posible de servidores por razones de seguridad. Para una comunicación segura de todos los sistemas dentro del dominio, UCS integra una CA raíz (autoridad de certificación).

4. Diseño Metodológico

4.1. Hardware

Tabla 1: Materiales Hardware

Material	Descripción	Presupuesto
Computadora personal	**Nombre del producto:** HP Pavilion Laptop 15 **Número de producto:** 2DS94UA#ABA. **Microprocesador:** Octava generación del procesador Intel® Core™ i7-8550U de dos núcleos a 2,2 GHz. **Memoria RAM:** SDRAM DDR3L de 24 GB (2 DIMM). **Disco duro:** Disco duro de 2 TB (5400 RPM).	**$ 900**
Router Tenda	**Modelo:** V5.2.2.12_en_TDE01. **Board ID:** 96318REF **Velocidad Máxima:** 3 Mbps. **Capacidad de usuarios:** 30 dispositivos vía Wifi simultáneamente.	**$ 50**
Cable USB	**Velocidad de Transferencia:** 2.0.	**$ 2**
	Total U$	**957.00**

4.2. Software

Tabla 2: Materiales Software

Software	Descripción
Sistemas Operativos Utilizados	
Sistema Operativo Ubuntu 20 LTS	Es una distribución de Linux basada en Debian, puede correr en computadores de escritorio y servidores. Está orientado al usuario promedio, con un fuerte enfoque en la facilidad de uso y en mejorar la experiencia del usuario.
Sistema Operativo Windows 10	Es un sistema operativo de computadora personal desarrollado y lanzado por Microsoft como parte de la familia de sistemas operativos Windows NT (Windows New Technology). Orientado a estaciones de trabajo y servidor de red. Presenta interfaz gráfica propia, estable y con características similares a los sistemas de red UNIX.
GNS3 2.2.19	Es un simulador gráfico de red lanzado en 2008, que te permite diseñar topologías de red complejas y poner en marcha simulaciones sobre ellos, permitiendo la combinación de dispositivos tanto reales como virtuales.
Oracle VM VirtualBox 6.1	Es un software de virtualización para arquitecturas x86/amd64. Actualmente es desarrollado por Oracle Corporation como parte de su familia de productos de virtualización

Wireshark 3.4.6	Es un analizador de protocolos utilizado para realizar análisis y solucionar problemas en redes de comunicaciones, para análisis de datos y protocolos, y como una herramienta didáctica.
Univention Corporate Server 5.0	Es un sistema operativo de servidor derivado de Debian GNU/Linux con un sistema de gestión integrado para la administración central y en plataformas cruzadas de servidores, servicios, clientes, escritorios y usuarios así como ordenadores virtualizados con operación en UCS.
OX App Suite 10.2.1	Es una plataforma modular de comunicación y colaboración. Basado en estándares abiertos, OX App Suite se puede integrar fácilmente en las infraestructuras de TI existentes. OX App Suite está dirigido a empresas, educación y autoridades.
Zimbra Colaboration 8.8.15	Es un programa informático colaborativo o groupware que consta de un servicio de correo electrónico creado por zimbra inc.
Kopano Core Community 4.4	Kopano es una suite de aplicaciones de software colaborativo de código abierto, originalmente basado en Zarafa.
Cisco IOS 7200 Series Routers	Los enrutadores cisco de la serie 7200 están diseñadas para las plataformas de interacción de centro de datos. Ofrecen un mejor rendimiento, una amplia gama de opciones de conectividad y una mejor capacidad de administración.
Cisco IOS 3600 Modular	Su arquitectura protege la inversión de los datos del cliente en las redes integradas.
Servidores Locales Utilizados	
Apache	Es un servidor web HTTP de código abierto para plataformas Unix-like (BSD, GNU/Linux, etc.), Windows, Macintosh y otras, que implementa el protocolo HTTP/1.1 y la noción de sitio virtual.
Bind9	Es un servidor de DNS más comúnmente utilizado en internet, específicamente en sistemas Unix en las cuales es un estándar de facto.
Postfix 2.6.6	Es un servidor de correo de software libre, un programa informático para el enrutamiento y envío de correo electrónico.
Dovecot v2.3.20	Dovecot puede trabajar en estándares mbox, Maildir y sus propios formatos activos dbox de alto rendimiento, es completamente compatible con implementaciones de servidores UW IMAP y Courier IMAP, así como con clientes que acceden a los buzones de correo

4.3. Etapas del Proyecto:

La metodología del presente trabajo es Teoría fundamentada con un Diseño sistemático. Para cumplir con los objetivos propuestos seguiremos el siguiente esquema:

4.3.1. Etapa I: Diseño de entorno de trabajo.

Análisis y diseño de la Topología a utilizar para desarrollar las pruebas entre Suite.

4.3.2. Etapa II: Recopilación de Información

Recolección y búsqueda de la información.

Selección de la información útil de acuerdo con el desarrollo de los contenidos de cada uno de los temas.

4.3.3. Etapa III: Configuración e implementación de las diferentes Suites y entorno de trabajo

Organización de la información seleccionada: la información será organizada según el nivel de complejidad que tiene cada uno de los temas a desarrollar en los aspectos teóricos, prácticos.

La secuencia de los contenidos teóricos será la siguiente:

- Correo Electrónico.
- Protocolos de Correo Electrónico.
- Sistemas seguros de Correo Electrónico.

La organización de pruebas propuestas será la siguiente:

- Pruebas de envío de emails entre las distintas suites.
- Pruebas de antispam,
- Pruebas de antivirus,
- Pruebas de videos llamadas
- Pruebas de envío de chats.
- Captura y Análisis de tráfico en las diferentes suites.
- Análisis y comparativa de las diferentes suites.

4.3.4. Etapa IV: Presentación del proyecto

Presentación de los documentos finales generados con los aspectos teóricos y enunciados de las pruebas, así como resolución y resultados de las pruebas que han sido propuestas.

5. Resultados

5.1. Topología en GSN3 a utilizar en las 3 suites.

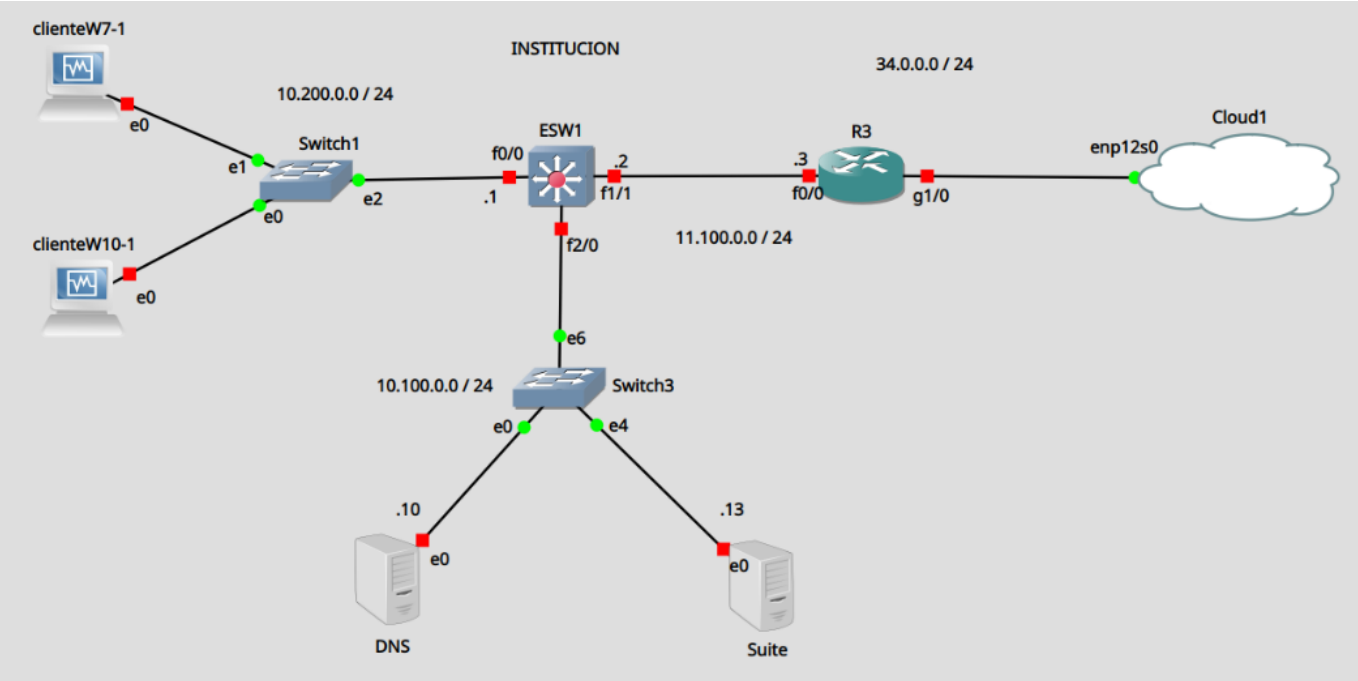

Figura 9. Topología en GNS3

El entorno en que se estará configurando la siguiente suite es un ambiente controlado y diseñado en el emulador de redes GNS3 2.2.19 la suite será instalada para las diferentes instituciones. Se determinará diferentes parámetros para que dicha topología quede funcional como una Red física, siguiendo los protocolos necesarios para ello.

Nuestra topología, contara con:

- 2 máquinas clientes (Windows 10 y Windows 7): Simularán ser usuarios donde se podrán conectar los clientes de la empresa para enviar correos dentro y fuera de la institución.
- Switch Multicapa: Emulará la infraestructura de red que pueda tener una institución además de realizar la conexión entre los servidores DNS y Suite de Correo electrónico, así como la asignación de IP por vía DHCP, así como tener conexión hacia el Router frontera.
- Servidor DNS: Realizara las traducciones para nuestro dominio utilizado para nuestra Suite de Correo que corresponda.
- Servidor Suite: Es que tendrá toda la funcionalidad de Correo Electrónico con todas sus características y prestaciones, almacenará toda la información y los parámetros de seguridad para garantizar su funcionamiento.

- Router Frontera: Este se encargará de realizar la traducción de IP publica a IP privada y viceversa implementando NAT dinámico y estático. Dinámico para que los clientes de dicha institución puedan tener conexión con el exterior y Estático para garantizar la conexión y comunicación con los servicios que ofrece esta institución ya sea para la recepción de correos o para poder acceder a la suite desde el exterior.
- Cloud: Estará conectado al Router frontera simulando la conectividad hacia el exterior contando con una conexión hacia nuestra maquina física y permita las demás empresas puedan comunicarse entre sí para facilitar compartir los correos electrónicos.

5.1. Configuración de OpenXchange.

OX App Suite puede ser instalado de dos forma diferentes, una de ellas es a través de consola ejecutando los comando correspondientes y configurando todo lo requerido para su buen funcionamiento y la otra es a través del software Univention App Center Univention Corporate Server (UCS) en el presente documento se usó la segunda opción ya que nos ahorra mucho trabajo para la instalación de la suite y sus componentes ya que este software realiza la configuración mínima requerida y funcional para que OX App Suite funcione correctamente.

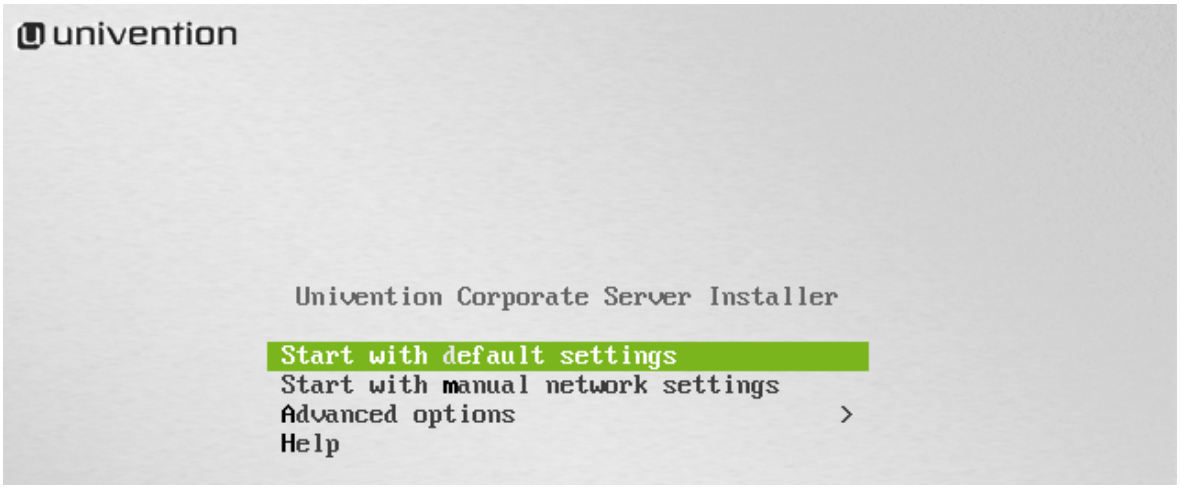

Figura 10. Instalador de OpenXchange

Este software también nos proporciona mejor manejo de información ya que la instalación de los paquetes para OX App Suite suele presentar problemas de instalación ya sea para la suite o alguno de sus componentes, estos problemas suelen darse porque los componentes de nuestro servidor no sean los adecuados o la versión del sistema operativo no sea la correcta, además de los requerimientos que se necesitan en nuestro gestor de base de datos para configurar OX App Suite entonces para evitar todos estos problemas a futuro se escoge UCS para su instalación y administración.

Univention Corporate Server (UCS) está disponible como imagen ISO para la instalación o como imagen de máquina virtual preinstalada para VMware, Virtualbox, Hyper-V y KVM. Con estas imágenes, puede utilizar UCS de forma instantánea y gratuita como UCS Core Edition

Después de iniciar con la configuración por defecto pasaremos a seleccionar el idioma del servidor como esta es una iso basada en una distro linux los pasos de instalación son muy similares a los pasos de instalación de distros como debian o ubuntu es por ello que solo recalcaremos aspectos importantes con respecto a la instalación. La instalación comienza y junto con una variedad de pasos diferentes, como la configuración del idioma, los discos duros montados se dividen. En muchos casos, la sugerencia de partición

simplemente puede ser adoptada. Si desea aumentar la seguridad de falla del almacenamiento en disco con un RAID de software o partición expandida, esto se puede configurar de forma manual.

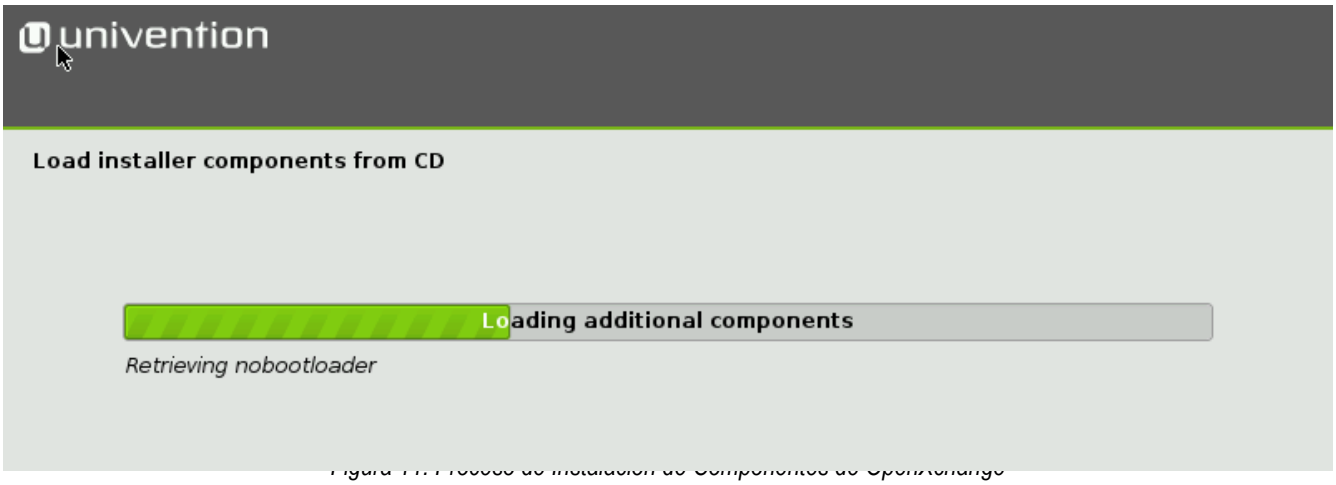

Figura 44: Proceso de instalación de Componentes de OpenXchange

Las credenciales que se usarán serán:

superusuario: **root**

contraseña: **abcdx1234**

Tenga en cuenta que las contraseñas elegidas en esta guía son débiles y deben reemplazarse por contraseñas más seguras

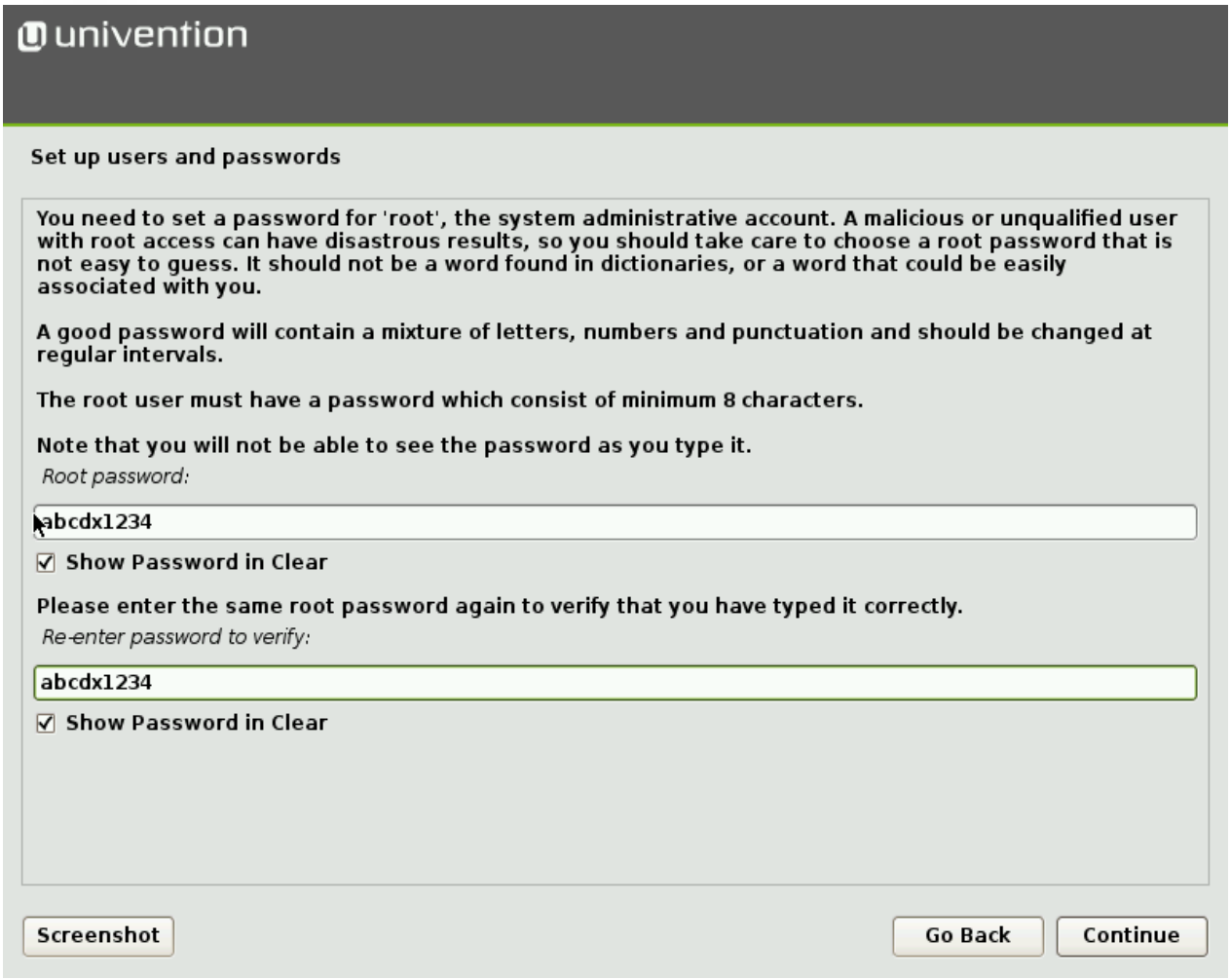

Figura 12. Configuración de Claves SU en OpenXchange

Realizando esta configuración nuestro sistema empezara su instalación base, así como los componentes necesarios para su correcto funcionamiento esto podría tomar unos minutos en completarse.

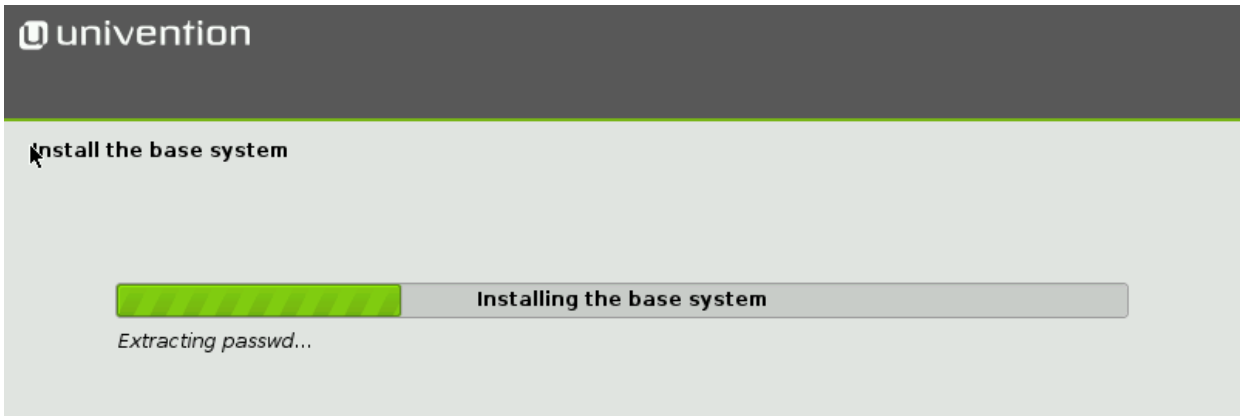

Figura 13. Instalación final de OpenXchange

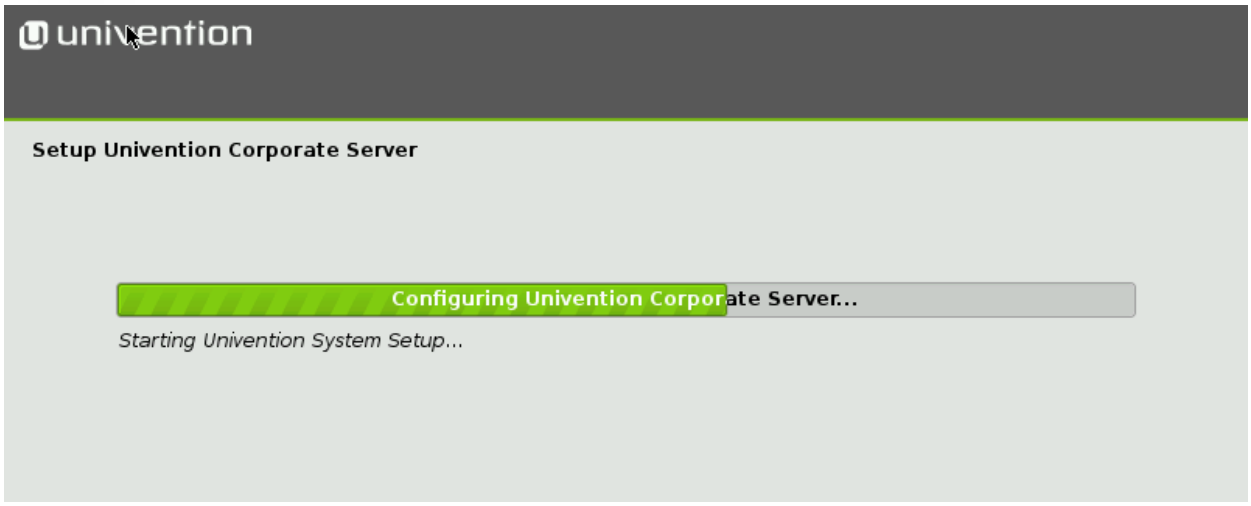

Figura 14. Instalación final de OpenXchange

Configuraciones de dominio

Una vez que haya finalizado la instalación del sistema operativo procederemos a configurar nuestro dominio para eso entraremos a la opcion Create a new UCS domain como se ve en la siguiente imagen

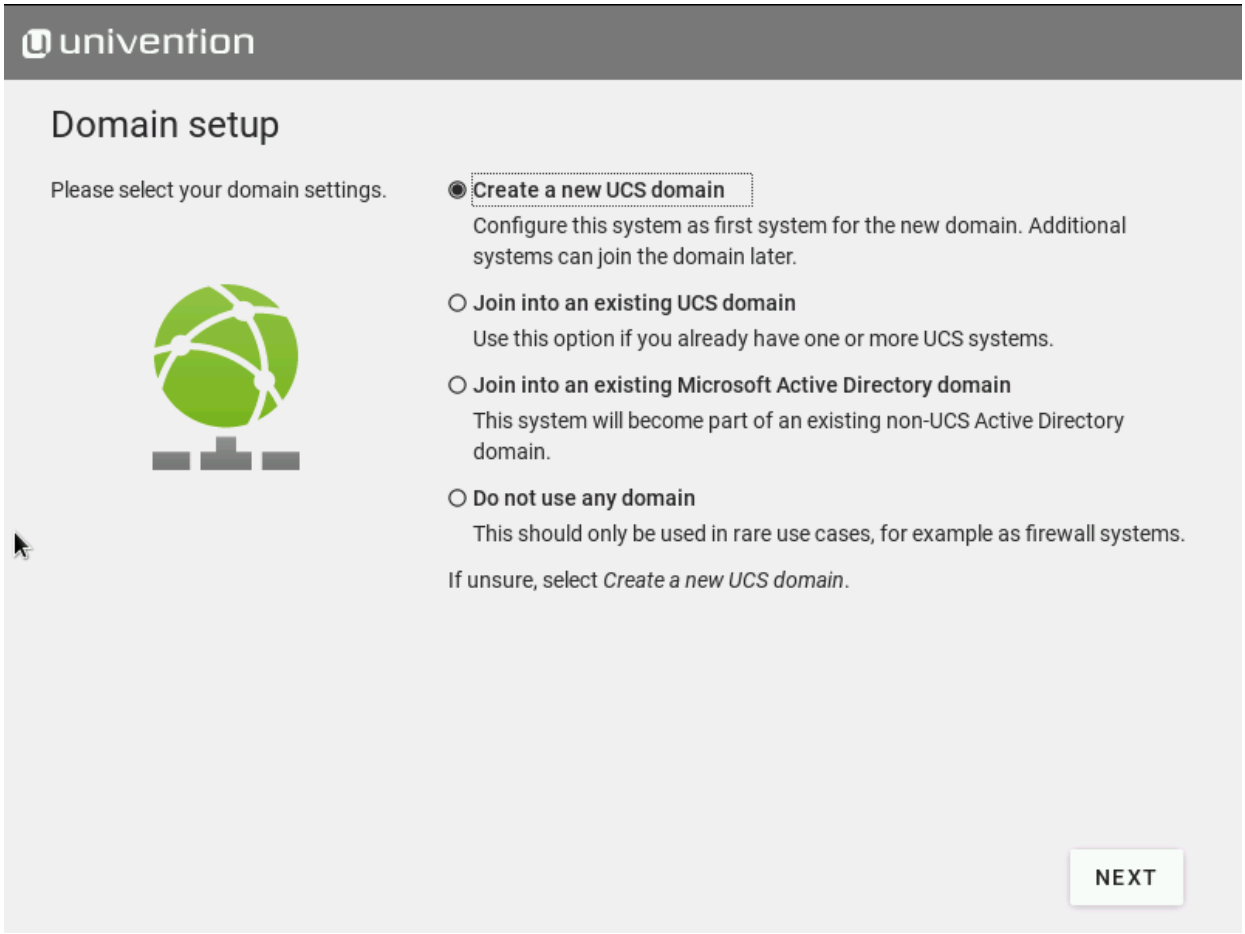

Figura 15. Instalación final de OpenXchange

Luego de haber seleccionado el modo Crear un nuevo dominio UCS, se solicita un nombre de organización, una dirección de correo electrónico, un nombre de dominio completo y una base LDAP en los dos pasos siguientes.

La especificación de un nombre de organización es opcional y se utiliza en el segundo paso para generar un nombre de dominio y la base LDAP automáticamente.

Si se especifica una dirección de correo electrónico válida, se utiliza para activar una licencia personalizada, que es necesaria para el uso de Univention App Center. La licencia se genera automáticamente y se envía inmediatamente a la dirección de correo electrónico especificada. Luego, la licencia se puede importar a través del cuadro de diálogo de licencia de la Consola de administración de Univention.

El nombre del sistema UCS que se configurará y el nombre del dominio DNS se determinan a partir del nombre de dominio completo (nombre de host incluido el nombre de dominio) ingresado aquí. Se genera una sugerencia automáticamente a partir del nombre de la organización ingresado en el paso anterior.

En esta sección introduciremos el nombre y un correo de Teknova ya que este será el nombre de la institución que vamos a utilizar para realizar las pruebas descritas en próximos apartados por lo tanto nuestro nombre de dominio seria Teknova.com.

Es necesario especificar una base LDAP para la inicialización del servicio de directorio. Aquí también se deriva una sugerencia automáticamente del nombre de dominio completo. Por lo general, este valor se puede adoptar sin cambios.

Figura 16. Ajustes Finales en OpenXchange

Selección de componentes de software UCS

El paso de configuración del software ofrece la posibilidad de instalar componentes UCS adicionales durante la instalación. Las aplicaciones también están disponibles después de la instalación a través del Univention App Center en la categoría de componentes UCS y se pueden instalar y desinstalar allí posteriormente. Para este escenario vamos a instalar los componentes:

- Mail Server
- Fetchmail

Ya que este en este servidor será alojada nuestra suite y por lo tanto necesitaremos los servicios SMTP e IMAP además de contar con un mail service provider que nos proporciona el componente Fetchmail.

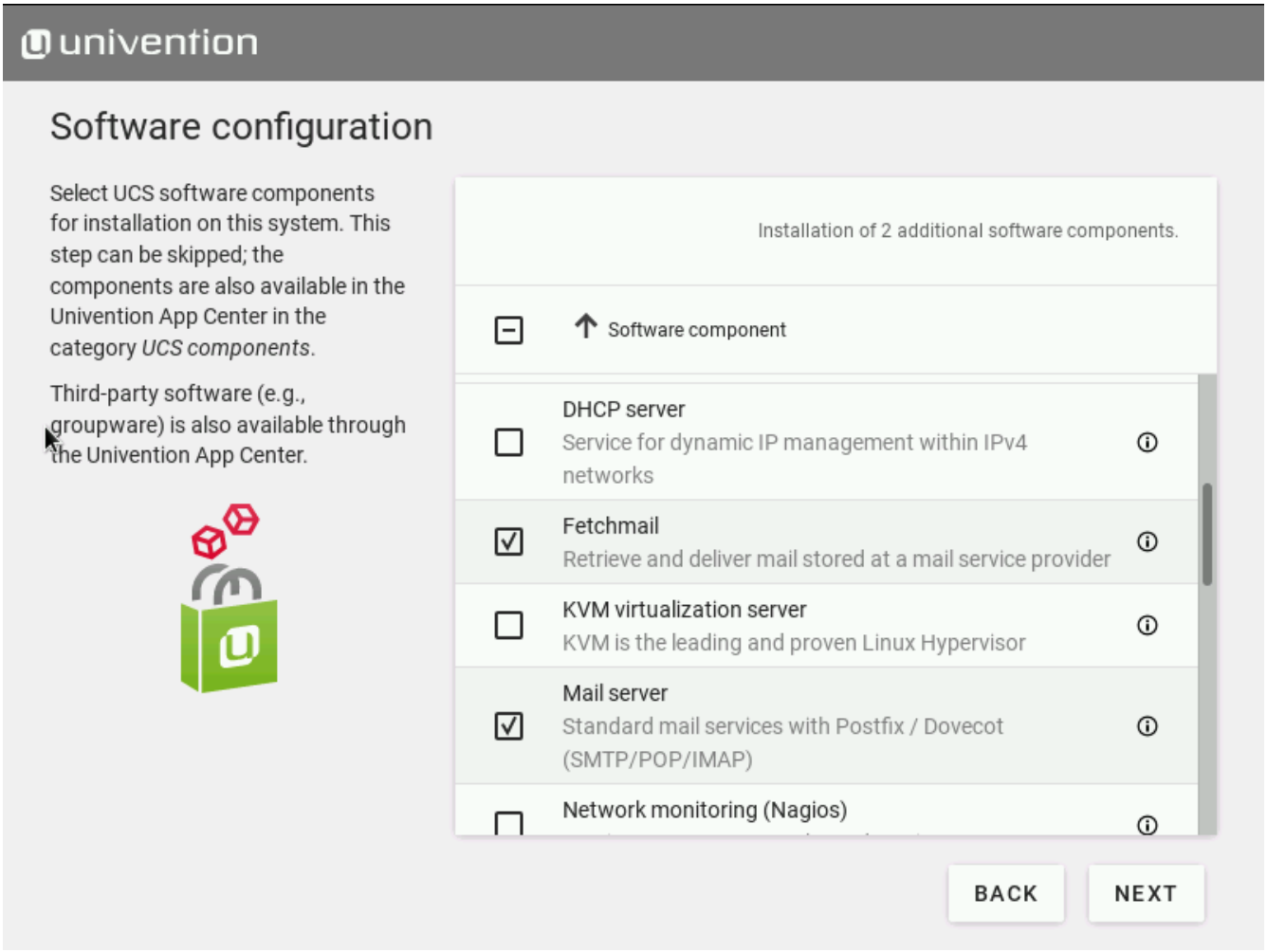

Figura 17. Ajustes Finales en OpenXchange

Confirmar la configuración

Este diálogo muestra los principales ajustes que se realizaron. Si todos los ajustes son correctos, el botón Configurar sistema se puede utilizar para iniciar la configuración del sistema UCS,

La opción Actualizar sistema después de la instalación permite la instalación automática de las actualizaciones de erratas disponibles. Además, todas las actualizaciones de nivel de parche y las actualizaciones de erratas disponibles se instalan en un controlador de dominio maestro. En todas las demás funciones del sistema, todas las actualizaciones de nivel de parche se configuran según el estado de instalación del controlador de dominio maestro. (Debe iniciar sesión en el controlador de dominio maestro para verificar el

estado de la instalación. Esto se hace utilizando los datos de inicio de sesión especificados en las opciones de unión).

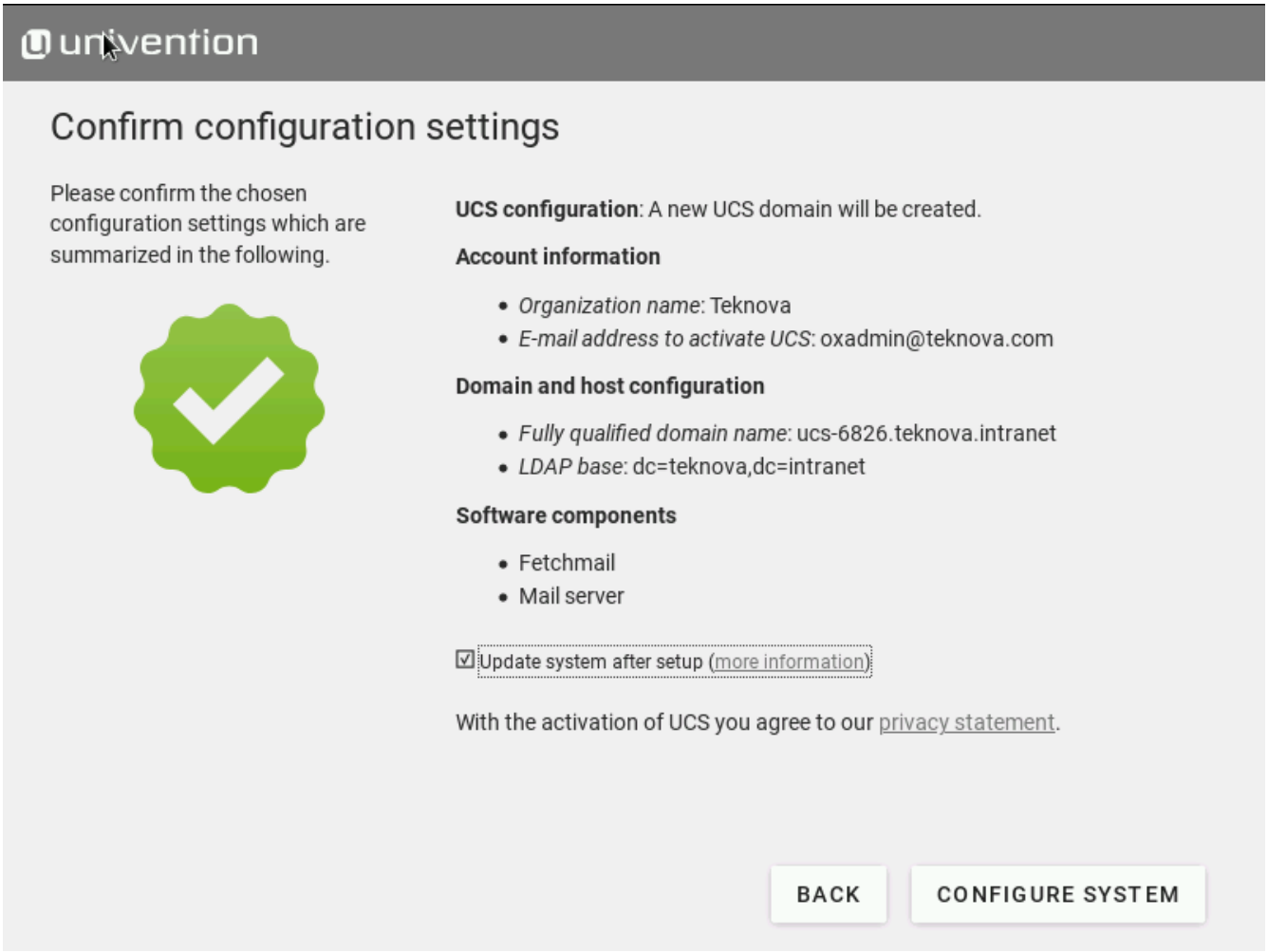

Figura 18. Ajustes Finales en OpenXchange

Durante la configuración, una barra de progreso muestra el progreso de la instalación.

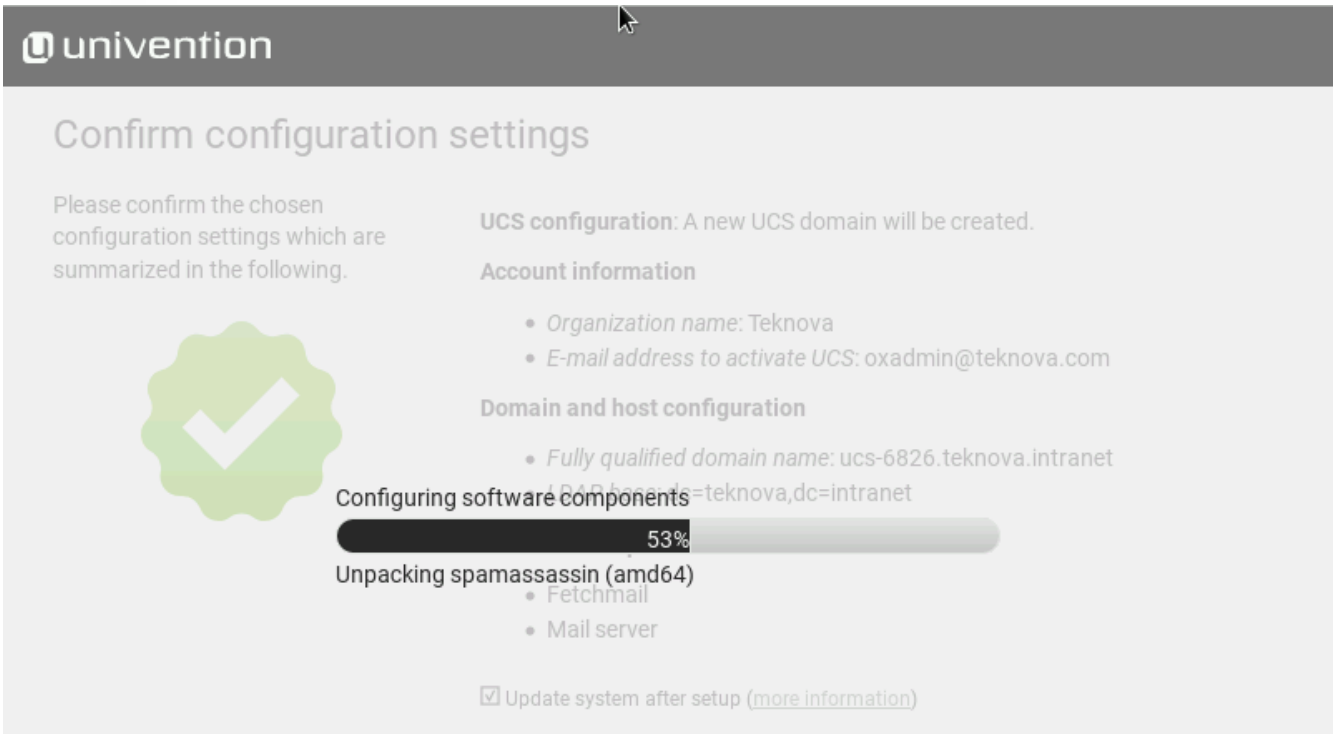

Figura 19. Ajustes Finales en OpenXchange

El protocolo de instalación del Univention Installer se guarda en los siguientes archivos:

/var/log/installer/syslog

/var/log/univention/management-console-module-setup.log

La finalización de la configuración debe confirmarse con el botón Finalizar. Luego, el sistema UCS se prepara para el primer procedimiento de arranque y se reinicia.

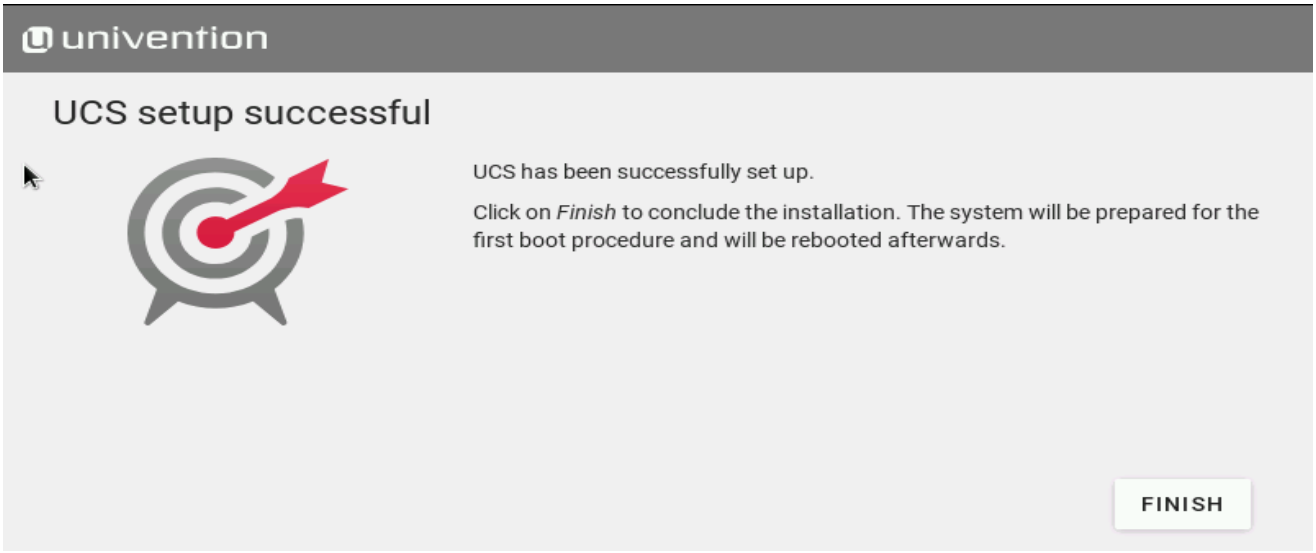

Figura 20. Ajustes Finales en OpenXchange

A continuación, el sistema se iniciará desde el disco duro. Después del procedimiento de inicio, los usuarios raíz y administrador pueden iniciar sesión a través de la interfaz web Univention Management Console, a la que se puede acceder con la dirección IP establecida durante la instalación o el nombre de host.

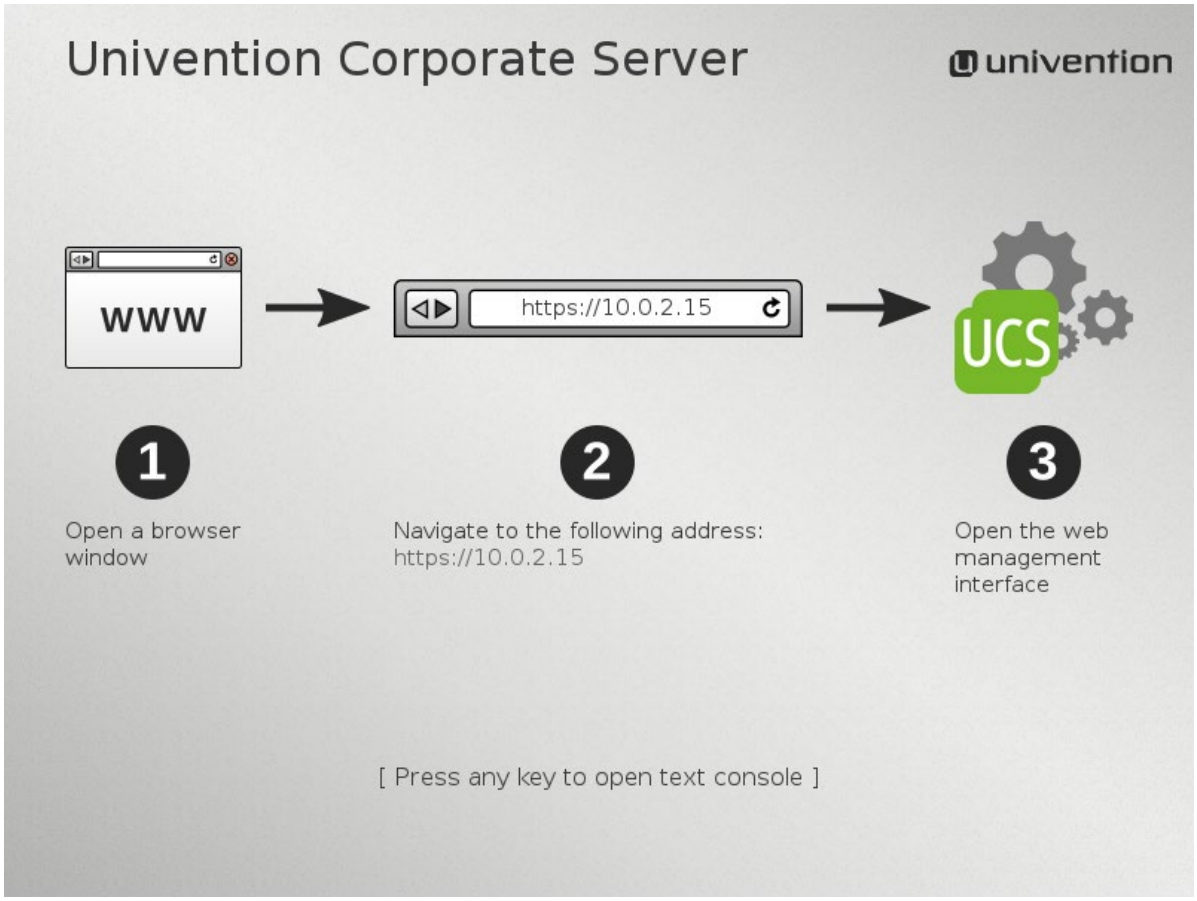

Figura 21. Interfaz inicial de OpenXchange al finalizar instalación

La interfaz web UCS se puede abrir en cualquier sistema UCS a través de la URL https: // nombre del servidor /. Alternativamente, el acceso también es posible a través de la dirección IP del servidor. En determinadas circunstancias, puede ser necesario acceder a los servicios a través de una conexión insegura (por ejemplo, si aún no se han creado certificados SSL para el sistema). En este caso, se debe utilizar http en lugar de https en la URL.

Figura 22. Interfaz inicial de OpenXchange al finalizar instalación

UCS viene con una página de inicio de sesión central. De forma predeterminada, se realiza un inicio de sesión único (SSO) a través de SAML (consulte la Sección 3.8) siempre que se pueda acceder a ucs-sso.domainname. Después de iniciar sesión correctamente, una sesión es válida para todos los sistemas UCS del dominio, así como para aplicaciones de terceros si estas admiten SSO basado en web. En caso de que no se pueda acceder a ucs-sso.domainname, el inicio de sesión se realiza en el sistema UCS local. Entonces, la sesión solo es válida para las páginas web UCS en el mismo sistema. Es posible forzar un inicio de sesión en el sistema local haciendo clic en el enlace Iniciar sesión sin inicio de sesión único.

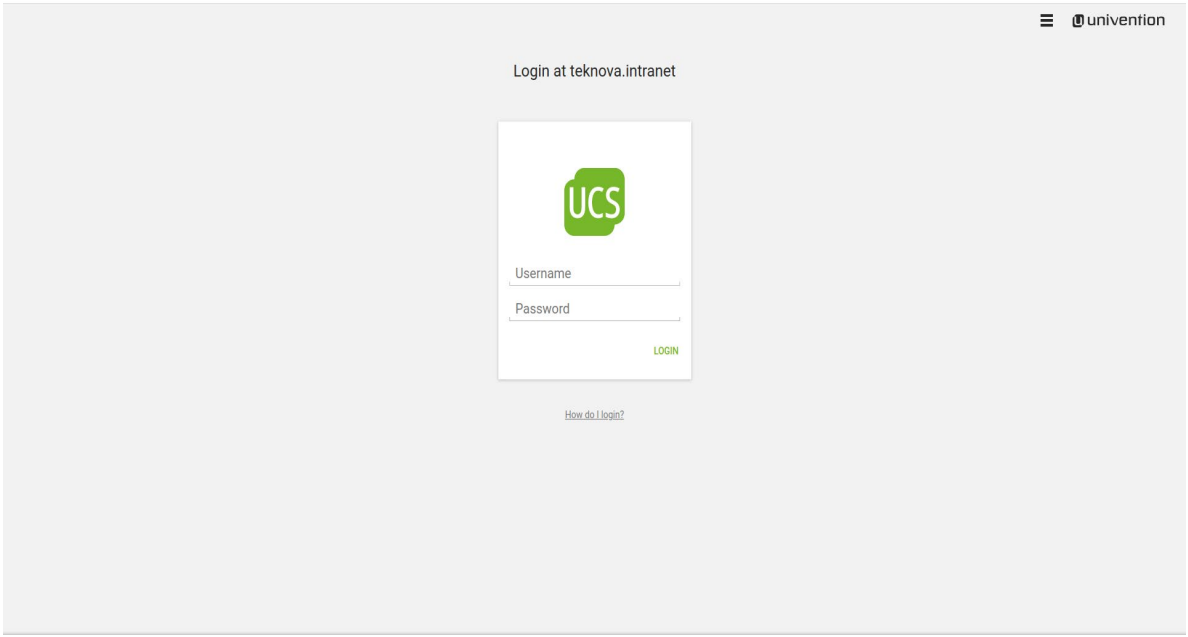

Figura 23. Login

La contraseña inicial de esta cuenta se ha especificado en el asistente de configuración durante la instalación. Corresponde a la contraseña inicial de la cuenta raíz local. El administrador también es la cuenta que debe usarse para el inicio de sesión inicial en un sistema de controlador de dominio maestro recién instalado.

Luego de ello nos vamos a dirigir al panel de administración de UCS y nos pedirá que introduzcamos nuestra licencia para ello daremos cancelar al modal que nos muestra y nos vamos a la parte posterior derecha y le daremos “Activation UCS” este nos pedirá un correo electrónico al que se nos enviara nuestra licencia.

La instalación de varias aplicaciones y aplicaciones de terceros desde App Center requiere la activación de UCS.

Una vez que tengamos nuestra licencia procederemos a activar nuestro UCS para poder instalar aplicaciones de tercero como lo es open-xchange.

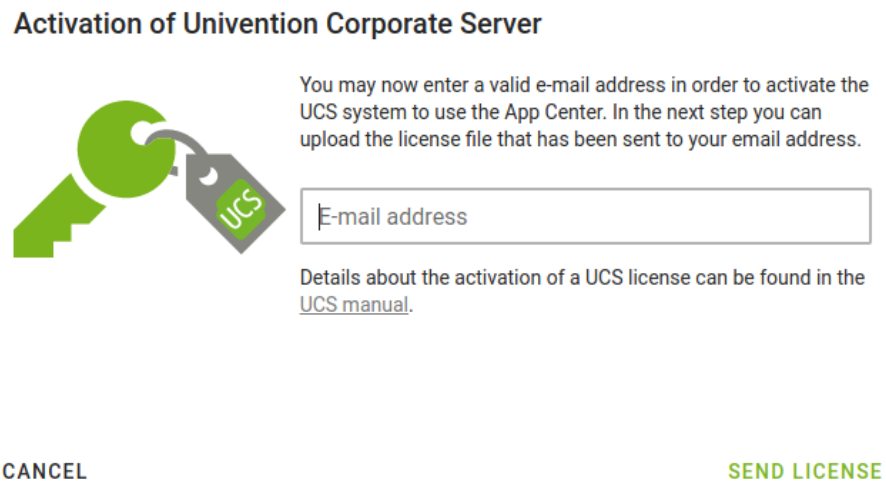

Figura 24. Proceso de Activación de OpenXchange

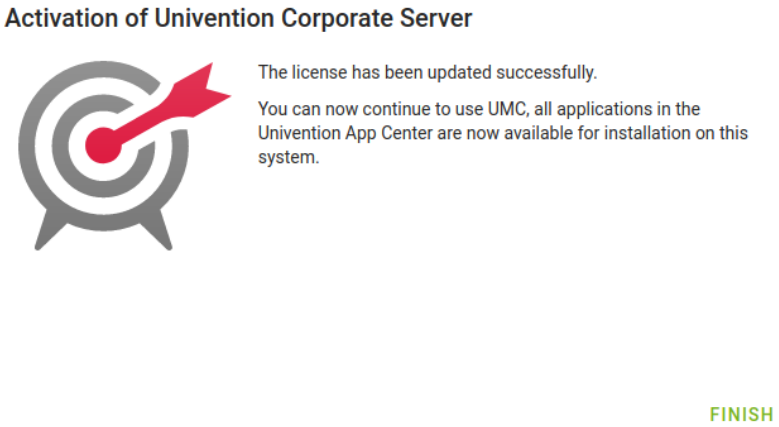

Figura 25. Proceso de Activación de OpenXchange

Para realizar la instalación de open-xchange y sus componentes necesarios para su correcta funcionalidad es necesario instalarlo a través de interfaz web y para ello nos iremos a la sección de App Center y buscaremos “OX App Suite”, “OX Documents” y “OX Guard”.

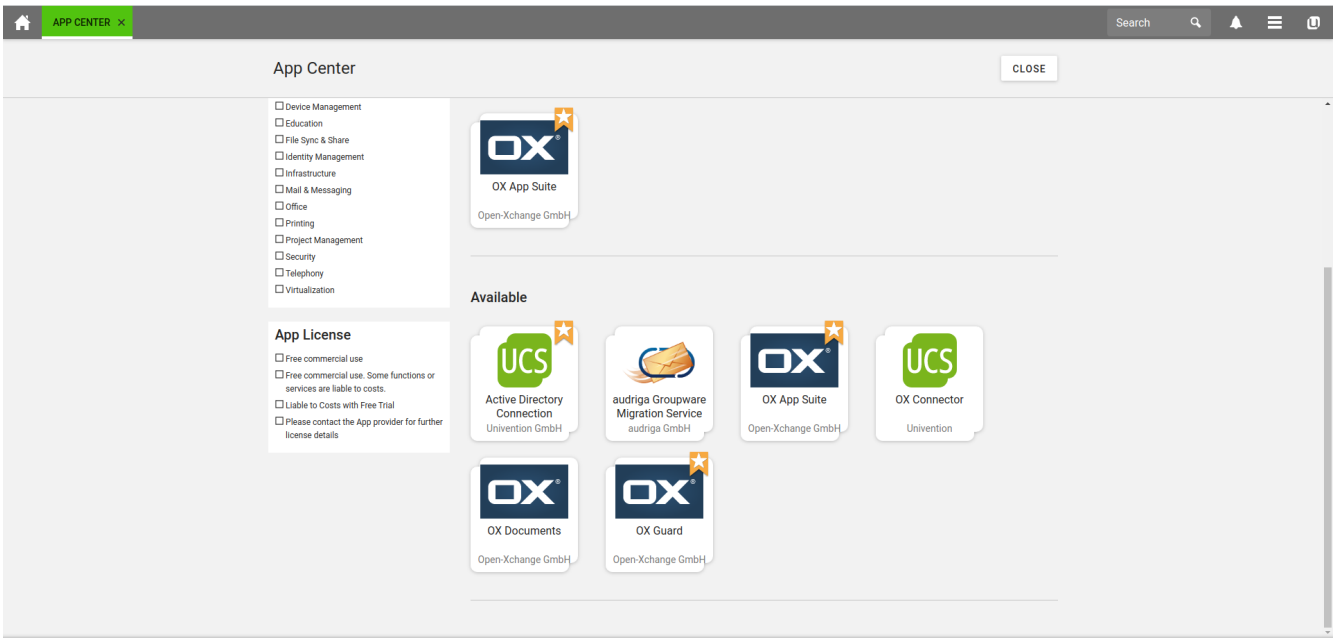

Figura 26. AppCenter de OpenXchange

Procederemos a instalar OX App suite ya que esta es requerida para poder realizar la instalación de los demás componentes, basta con solo dar clic en la sección y presionar el botón instalar entonces UCS empezara a descargar los paquetes necesarios para la instalación correcta de la suite.

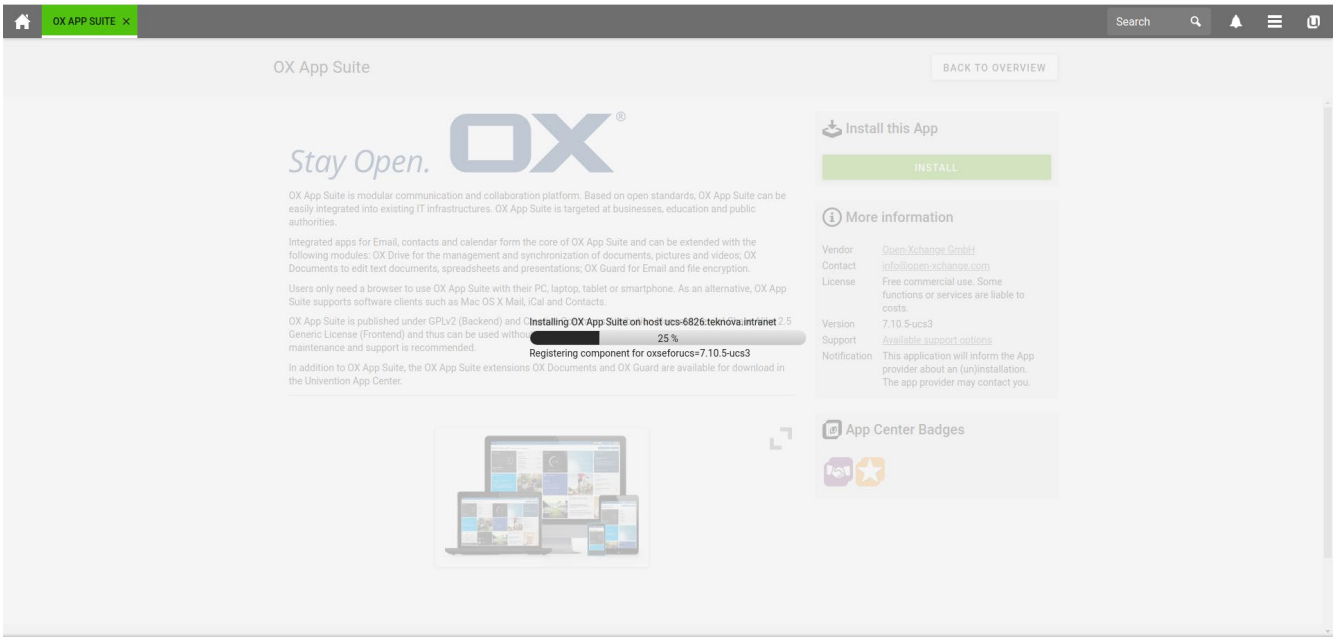

Figura 27. Instalación de Complementos de OX.

Una vez que tengamos instalado OX App suite procederemos a realizar la instalación de los demás componentes como lo es OX Documents para que nuestra suite pueda manejar documentos ya sea Excel o Word y OX Guard que nos otorga otro nivel de seguridad en nuestra suite.

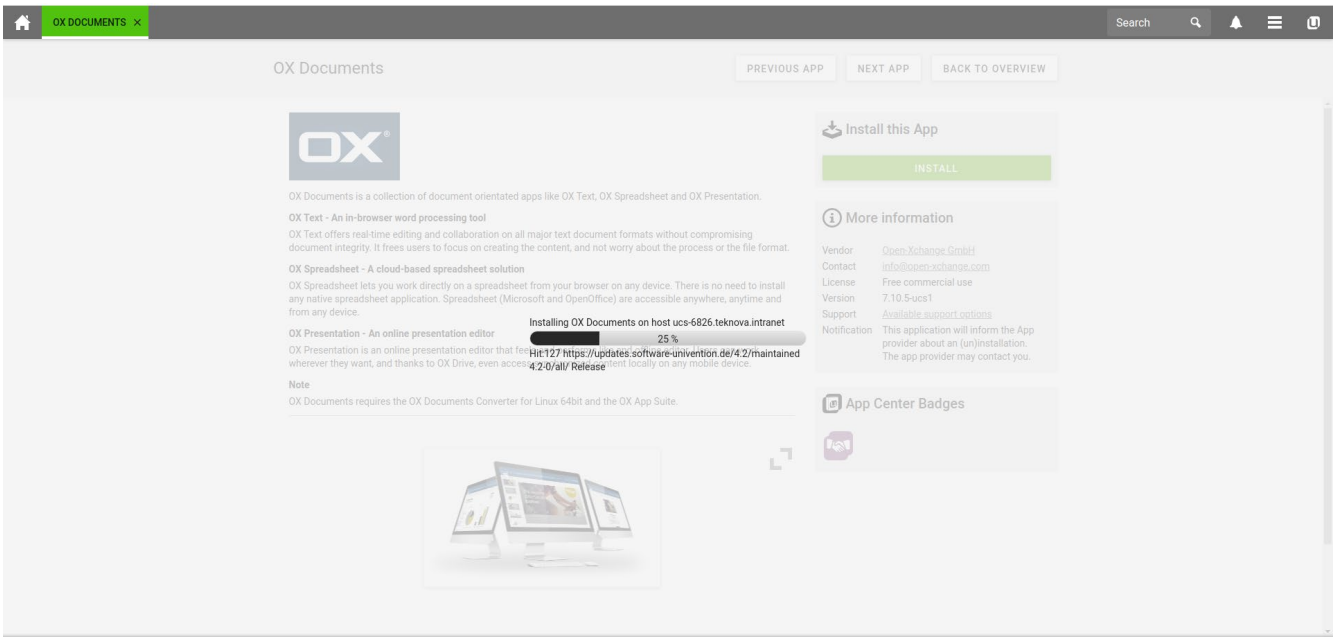

Figura 28. Instalación de Complementos de OX.

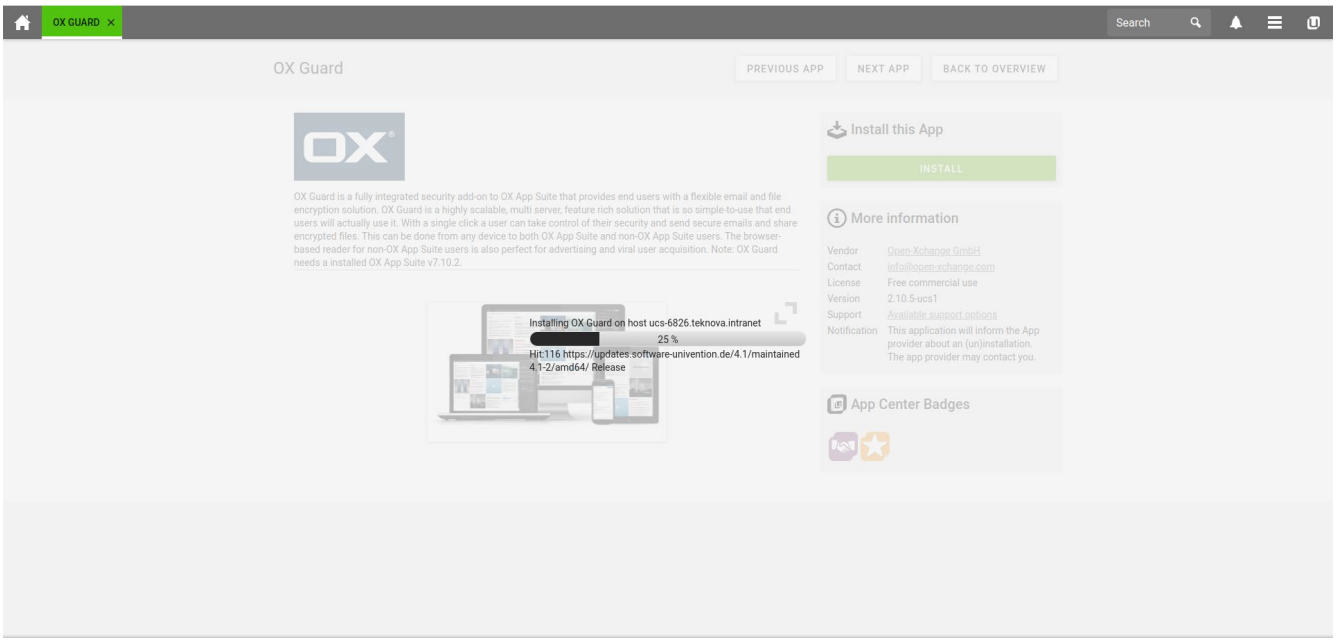

Figura 29. Instalación de Complementos de OX.

Luego de que el sitio nos haya indicado la correcta instalación de todos los componentes tendríamos instalado OX App suite con su correcto funcionamiento ya solo nos faltaría acceder al sitio de nuestra suite para ello nos iremos a inicio, entramos a la opcion OX App suite.

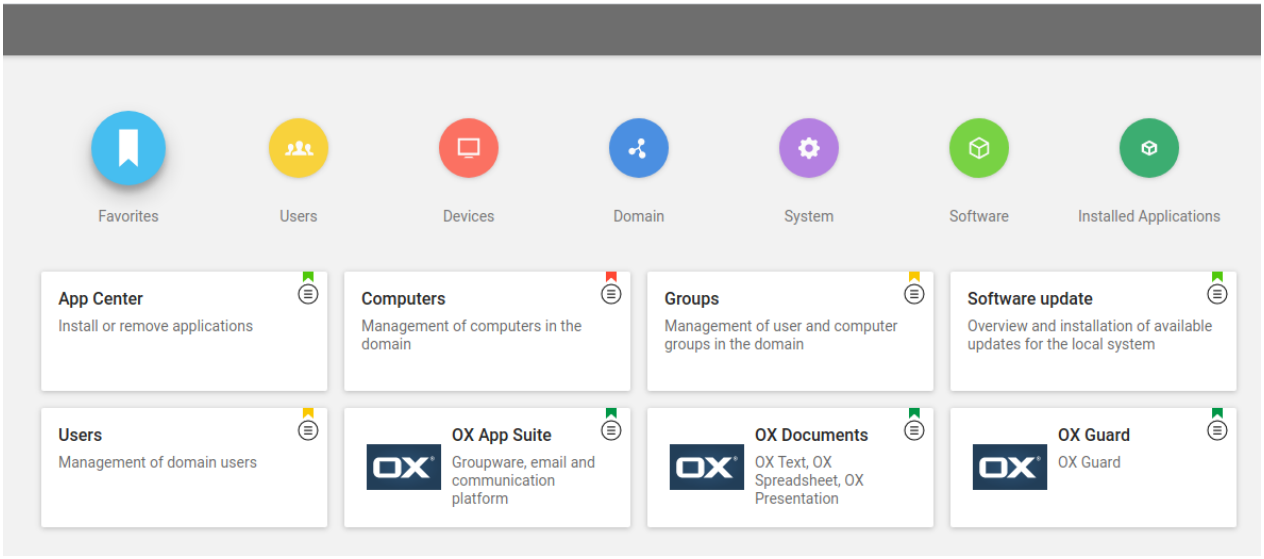

Figura 30. Panel de Administración de OX

Y datemos clic en open esto nos abrirá una nueva venta de inicio de sesión donde iniciaremos sesión con los usuarios creados desde el panel de administración de UCS seleccionando la opcion open-xchange groupware account de esta forma estamos indicando que el usuario a crear será parte de groupware de open-xchange.

Como usuario de prueba estaremos utilizando el siguiente (estos datos son sensible y deben administrarse correctamente usamos una contraseña tan frágil con fines de prueba, pero dicha clave debe seguir un cierto régimen de caracteres especiales):

Name: Fabian Sandoval

username: fabian

contraseña: abcdx1234

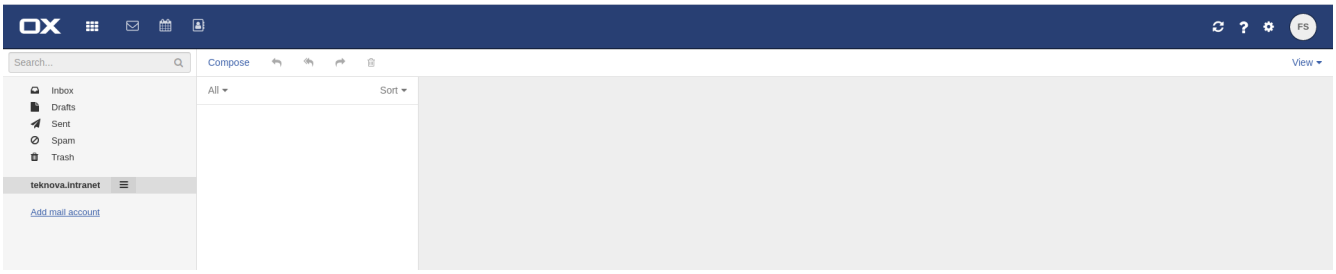

Figura 31. Interfaz de Correo Electrónico en OX

Con ello nuestra instalación ha sido exitosa y la suite esta lista para empezar con las pruebas para dicho análisis

5.2. Configuración de Kopano.

Manual de Instalación

La siguiente documentación describe cómo instalar Univention Corporate Server (UCS). El sistema UCS se instala desde el DVD. La instalación es interactiva y solicita todos los ajustes necesarios del sistema en una interfaz gráfica.

El DVD de instalación está disponible para la arquitectura de computadora amd64 (64 bits). Además de la compatibilidad con los sistemas BIOS ampliamente distribuidos, el DVD también incluye compatibilidad con el estándar Unified Extensible Firmware Interface (UEFI). El soporte UEFI en el DVD también es capaz de iniciar sistemas con SecureBoot activado e instalar UCS allí.

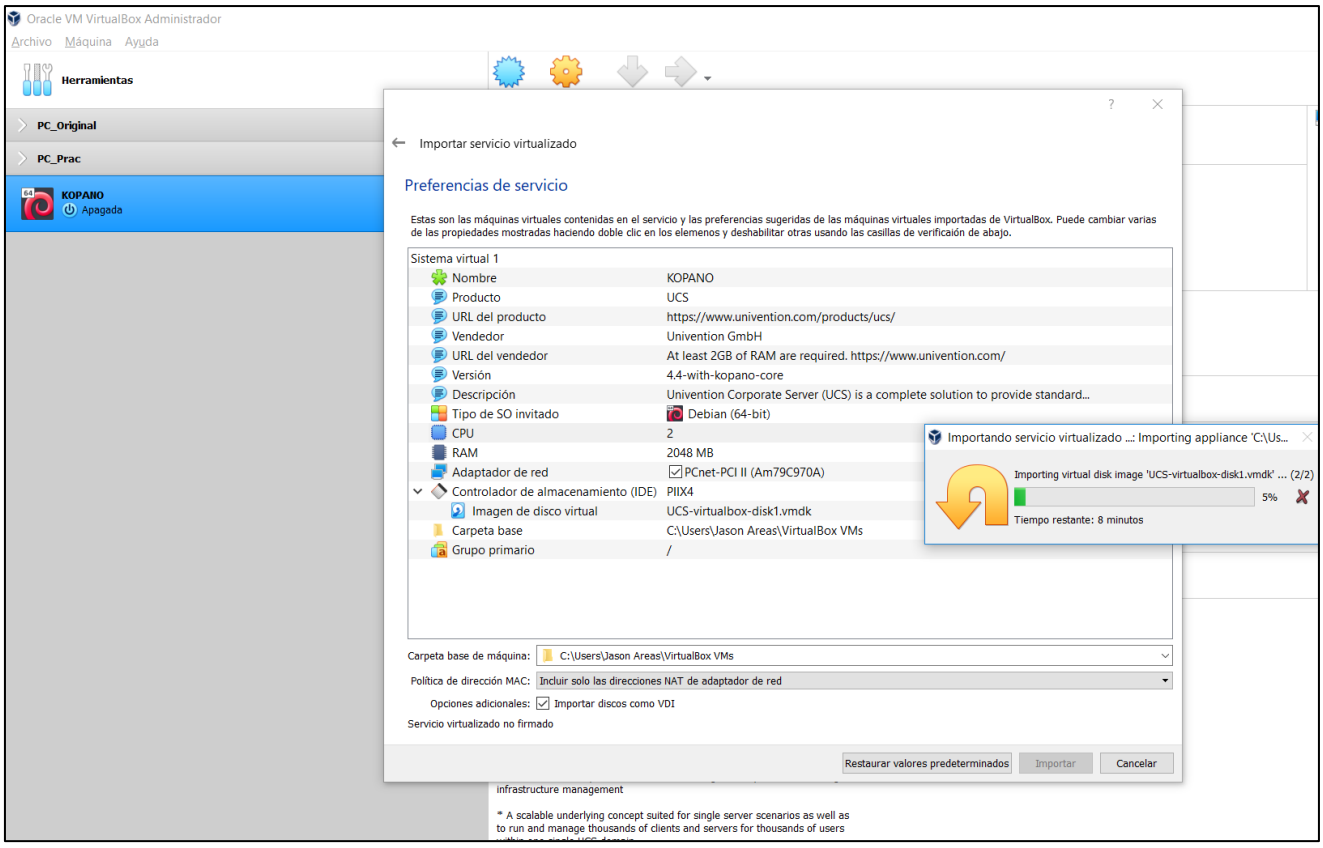

Figura 32. Instalación de Imagen Virtual de Kopano

Seleccionar el modo de instalación

Comenzar con la configuración predeterminada: inicia la instalación gráfica interactiva. Durante la instalación, el sistema solicita una serie de parámetros como la configuración de red, las particiones del disco duro, la configuración del dominio y la selección de componentes de software para el sistema UCS que se instalará y luego realiza la instalación y la configuración.

Comenzar con la configuración de red manual

realiza una instalación estándar, donde la red no se configura automáticamente a través de DHCP. Esto es práctico en sistemas donde la red debe configurarse manualmente.

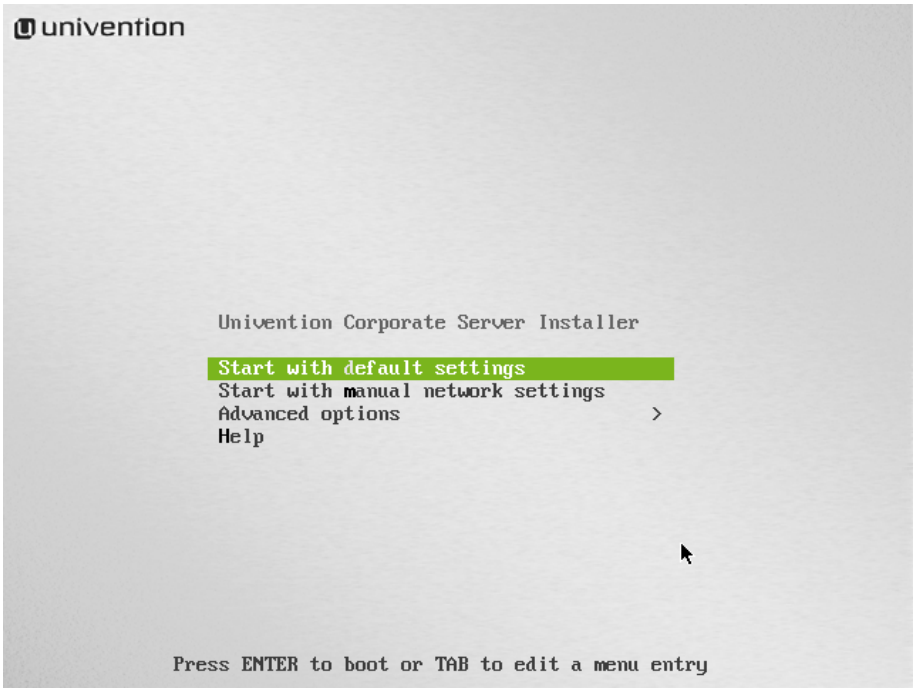

Figura 33. Instalación Inicial de KOPANO

Seleccionar la distribución del teclado

La distribución del teclado se puede seleccionar independientemente del idioma del sistema. El idioma seleccionado aquí debe ser compatible con el teclado utilizado, ya que de lo contrario podría causar problemas operativos.

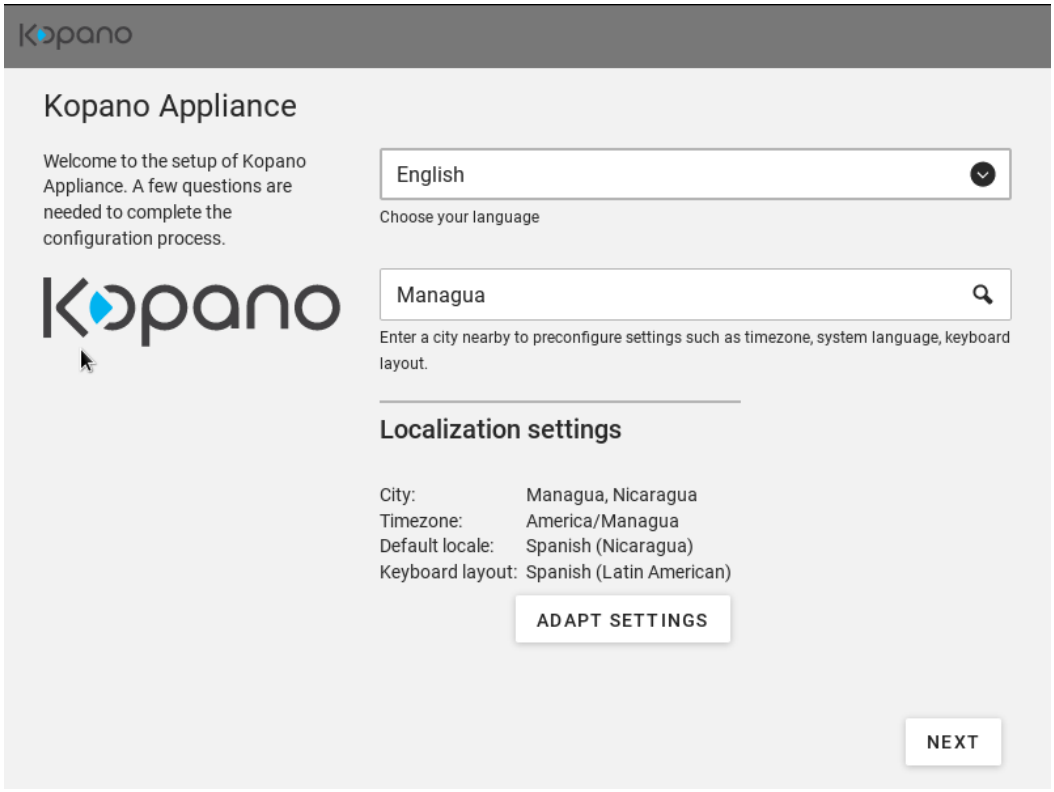

Figura 34. Configuraciones Básicas de KOPANO

Configuración de la red

Inicialmente, Univention Installer intenta configurar las interfaces de red automáticamente. Esto se puede desactivar seleccionando el elemento de menú Iniciar con configuración de red manual en el menú del gestor de arranque. En primer lugar, se intenta determinar una dirección IPv6 mediante la configuración automática de direcciones sin estado (SLAAC). Si esto no tiene éxito, el instalador de Univention intenta solicitar una dirección IPv4 a través del Protocolo de configuración dinámica de host (DHCP). Si tiene éxito, se omite la configuración de red manual de Univention Installer.

Configuración de red automática

Si no hay un servidor DHCP presente en la red local o se requiere una configuración estática de la interfaz de red, se puede seleccionar el botón Cancelar. El instalador de Univention ofrece entonces repetir la configuración automática o configurar la interfaz manualmente.

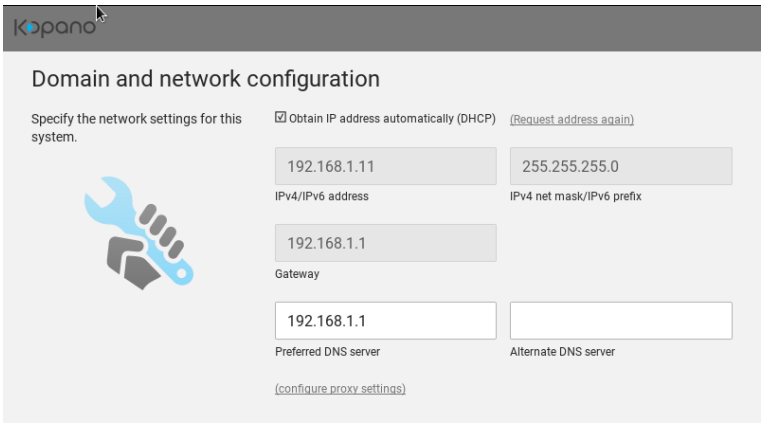

Figura 35

Al instalar el primer sistema UCS en un nuevo dominio UCS, se debe ingresar la dirección IP del enrutador local (si proporciona el servicio DNS) o el servidor DNS del proveedor de Internet.

Al instalar cada sistema UCS adicional, la dirección IP de un sistema controlador de dominio UCS debe especificarse como servidor DNS. Esto es esencial para que funcione la detección automática del maestro del controlador de dominio. En caso de duda, se debe ingresar la dirección IP del sistema maestro del controlador de dominio UCS.

Si el sistema UCS va a unirse a un dominio de Active Directory de Windows durante la instalación, la dirección IP de un sistema controlador de dominio de Active Directory debe especificarse como servidor DNS. Esto es esencial para que funcione la detección automática del controlador de dominio de Windows Active Directory.

Configuraciones de dominio

La configuración final del sistema UCS se inicia seleccionando un modo de dominio. Hay cuatro modos disponibles, que influyen en los siguientes pasos de configuración:

En el primer modo, Crear un nuevo dominio UCS, se configura el primer sistema en un nuevo dominio UCS: un sistema UCS con la función de sistema de controlador de dominio maestro. En los siguientes pasos de configuración, se solicita la información necesaria para configurar un nuevo servicio de directorio, servicio de autenticación y servidor DNS. Un dominio UCS puede comprender uno o varios sistemas UCS. Se pueden agregar sistemas UCS adicionales en un momento posterior utilizando el modo Unirse a un dominio UCS existente.

Únase a un dominio de Active Directory existente: este modo, en el que UCS se opera como miembro de un dominio de Active Directory, es adecuado para expandir un dominio de Active Directory con aplicaciones disponibles en la plataforma UCS. Las aplicaciones instaladas en la plataforma UCS están disponibles para que

las utilicen los usuarios del dominio de Active Directory. Al seleccionar este modo, se solicita toda la información relevante para la unión del dominio de Active Directory y se configura el sistema UCS correspondientemente.

Seleccionar el modo Unirse a un dominio UCS existente permite configurar el sistema UCS para unirse a un dominio UCS existente. La función del sistema UCS que debe asumir en el dominio se consulta en una etapa posterior.

Si se selecciona el modo No usar ningún dominio, no hay funciones de administración basadas en web ni funciones de dominio disponibles en el sistema. El sistema UCS tampoco puede convertirse posteriormente en miembro de un dominio UCS o de Active Directory existente o encontrar un nuevo dominio UCS en un momento posterior. Además, el Univention App Center no está disponible en este modo. Por esta razón, este modo solo se usa raramente y en escenarios especiales (por ejemplo, como un sistema de firewall).

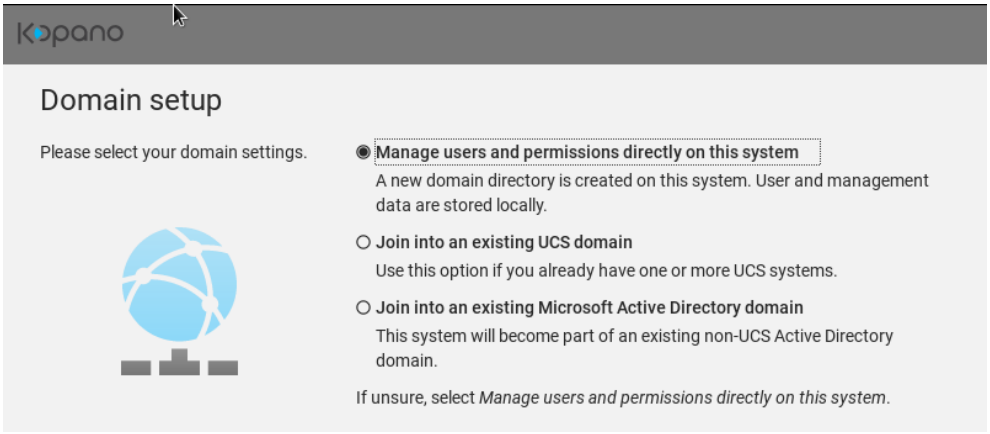

Figura 36. Configuraciones Básicas de KOPANO

Modo "Crear un nuevo dominio UCS"

Una vez que se ha seleccionado el modo Crear un nuevo dominio UCS, se solicita un nombre de organización, una dirección de correo electrónico, un nombre de dominio completo y una base LDAP en los dos pasos siguientes.

La especificación de un nombre de organización es opcional y se utiliza en el segundo paso para generar un nombre de dominio y la base LDAP automáticamente.

Si se especifica una dirección de correo electrónico válida, se utiliza para activar una licencia personalizada, que es necesaria para el uso de Univention App Center. La licencia se genera automáticamente y se envía inmediatamente a la dirección de correo electrónico especificada. Luego, la licencia se puede importar a través del cuadro de diálogo de licencia de la Consola de administración de Univention.

El nombre del sistema UCS que se configurará y el nombre del dominio DNS se determinan a partir del nombre de dominio completo (nombre de host incluido el nombre de dominio) ingresado aquí. Se genera una sugerencia automáticamente a partir del nombre de la organización ingresado en el paso anterior. Se recomienda no utilizar un dominio DNS disponible públicamente, ya que esto puede ocasionar problemas durante la resolución de nombres.

Es necesario especificar una base LDAP para la inicialización del servicio de directorio. Aquí también se deriva una sugerencia automáticamente del nombre de dominio completo. Por lo general, este valor se puede adoptar sin cambios.

Especificación del nombre de host y base LDAP

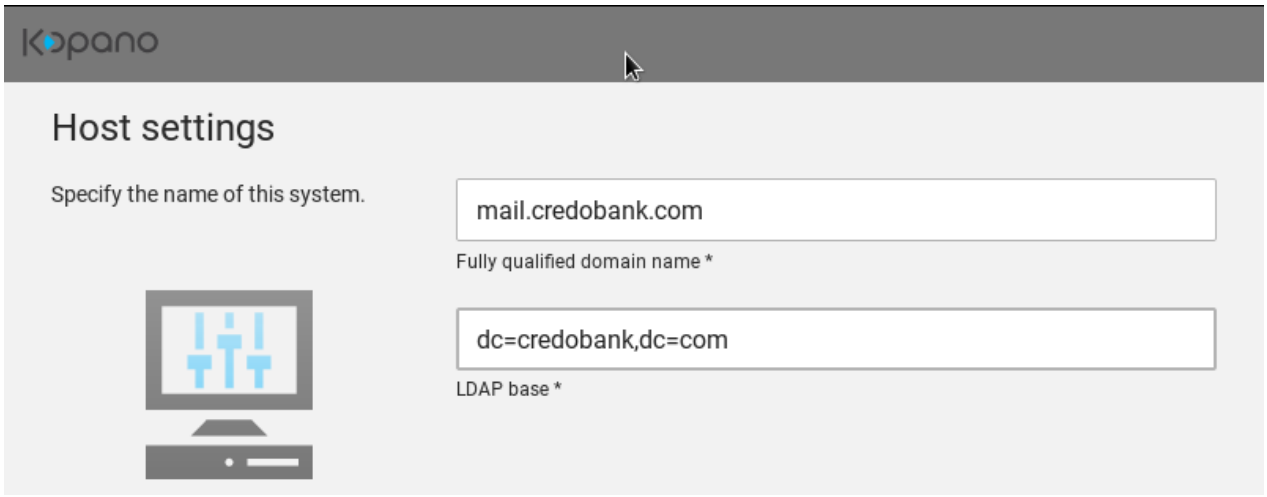

Figura 37. Configuraciones Básicas de KOPANO

Configurar la contraseña de root

Es necesario establecer una contraseña para el usuario root para iniciar sesión en el sistema instalado. Si se instala un controlador de dominio maestro, esta contraseña también se emplea para el usuario administrador. En una operación posterior, las contraseñas de los usuarios root y administrador se pueden administrar de forma independiente entre sí. La contraseña debe volver a introducirse en el segundo campo de entrada.

La contraseña debe contener al menos ocho caracteres por razones de seguridad.

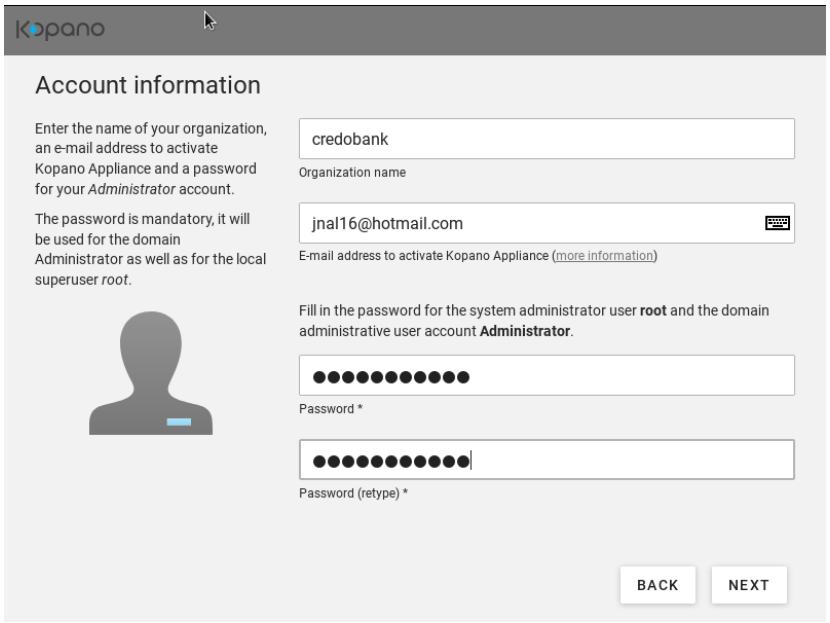

Figura 38. Configuraciones Básicas de KOPANO

Una vez finalizado todos los pasos confirmamos los parámetros que se van a configurar.

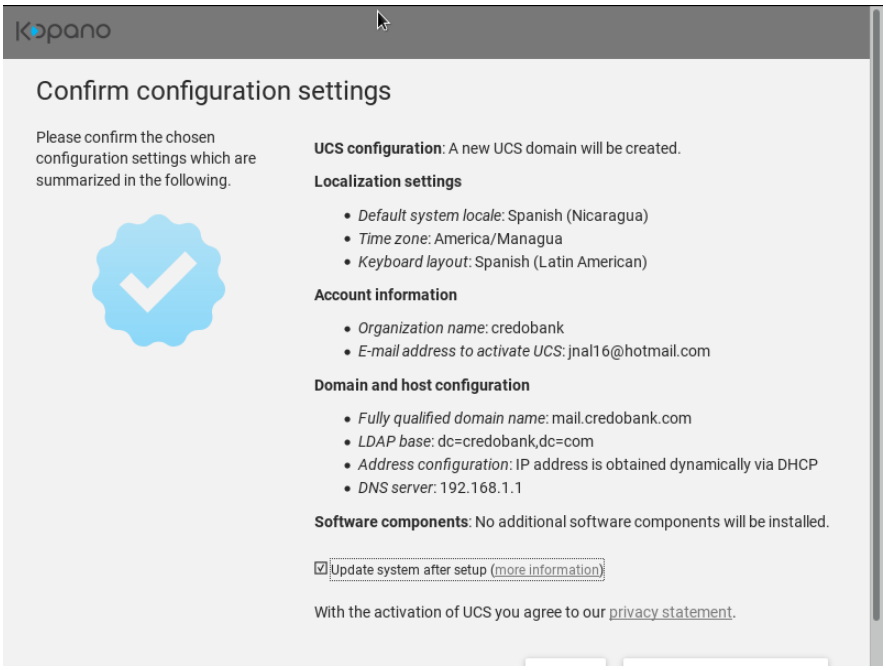

Figura 39. Resumen de Configuraciones Básicas de KOPANO

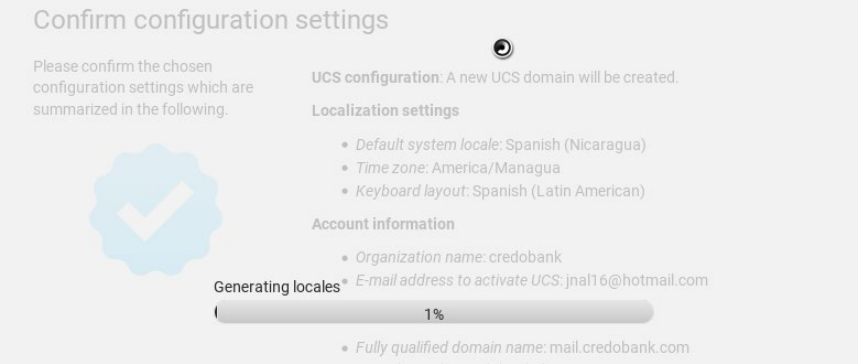

Figura 40. Configuraciones Básicas de KOPANO

5.3. Configuración de Zimbra.

El Servidor de Correo es uno de los Servidores más importantes y críticos para cualquier organización, ya que la mayoría de las comunicaciones empresariales se realizan únicamente a través del correo electrónico.

En el mundo del código abierto hay un par de servidores de correo electrónico gratuitos, pero Zimbra es uno de los principales servidores de correo. Zimbra Mail Server también conocido como ZCS (Zimbra Collaboration Suite) viene en dos versiones, Open Source y Enterprise.

Requisitos previos de Zimbra Mail Server (ZCS)

- Ubuntu server 16.04 lts mínimo
- 8 GB de RAM
- Al menos 5 GB de espacio libre en /opt
- FQDN (Fully Qualified Domain Name), en mi caso es «mail.redone.com.com».
- Registro A & MX para su servidor

En este artículo vamos a demostrar cómo instalar Open Source ZCS 8.8.15 en Ubuntu server 16.04 lts.

Preinstalación

Inicie sesión en su servidor Ubuntu y aplique las últimas actualizaciones usando el siguiente comando apt y luego reinicie

```
~]# apt update -y ; reboot
```

Después de reiniciar, configure el nombre de host de su servidor, en mi caso lo estoy configurando como «mail.redone.com».

```
~]# hostnamectl set-hostname "mail.redone.com"
```

Añada las siguientes líneas en el fichero /etc/hosts:

```
 GNU nano 2.5.3                  Archivo: /etc/hosts

127.0.0.1       localhost
172.168.10.5    mail.redone.com mail

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

Figura 41.

Luego llega el turno de editar el archivo de configuración del servidor dns, entramos a la siguiente ruta: cd /etc/bind/named.config.local

Dejamos los siguientes campos de la zona directa tal y como aquí lo mostramos:

```
Debian 10 dns (Instantánea 2) [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
 GNU nano 3.2                    named.conf.local                    Modificado

//
// Do any local configuration here
//

// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";

zone "redone.com" {
        type master;
        file "/var/lib/bind/redone.com.hosts";
        };
zone "10.168.172.in-addr.arpa" {
        type master;
        file "/var/lib/bind/172.168.10.rev";
```

Figura 42. Configuración Archivo Hosts en Zimbra

Creando archivos de búsqueda directa en la ruta que hemos declarado en el named.config.local

creamos el archivo redone.com.hosts

abrimos el siguiente archivo con nano */var/lib/bind/redone.com.hosts*

Dejamos los siguientes campos como lo muestra la imagen.

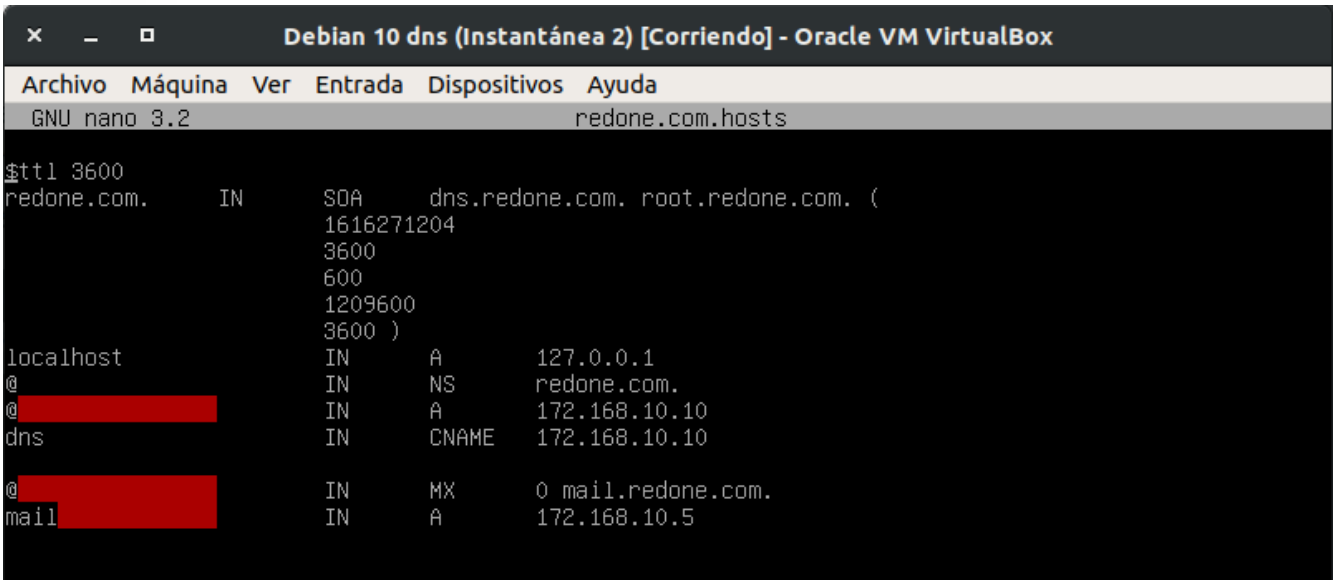

Figura 43. Configuración Archivo Hosts en Zimbra

Guardamos y reiniciamos el equipo:

sudo reboot

Comprobación de Registro Interno

Figura 44. Configuración Archivo Hosts en Zimbra

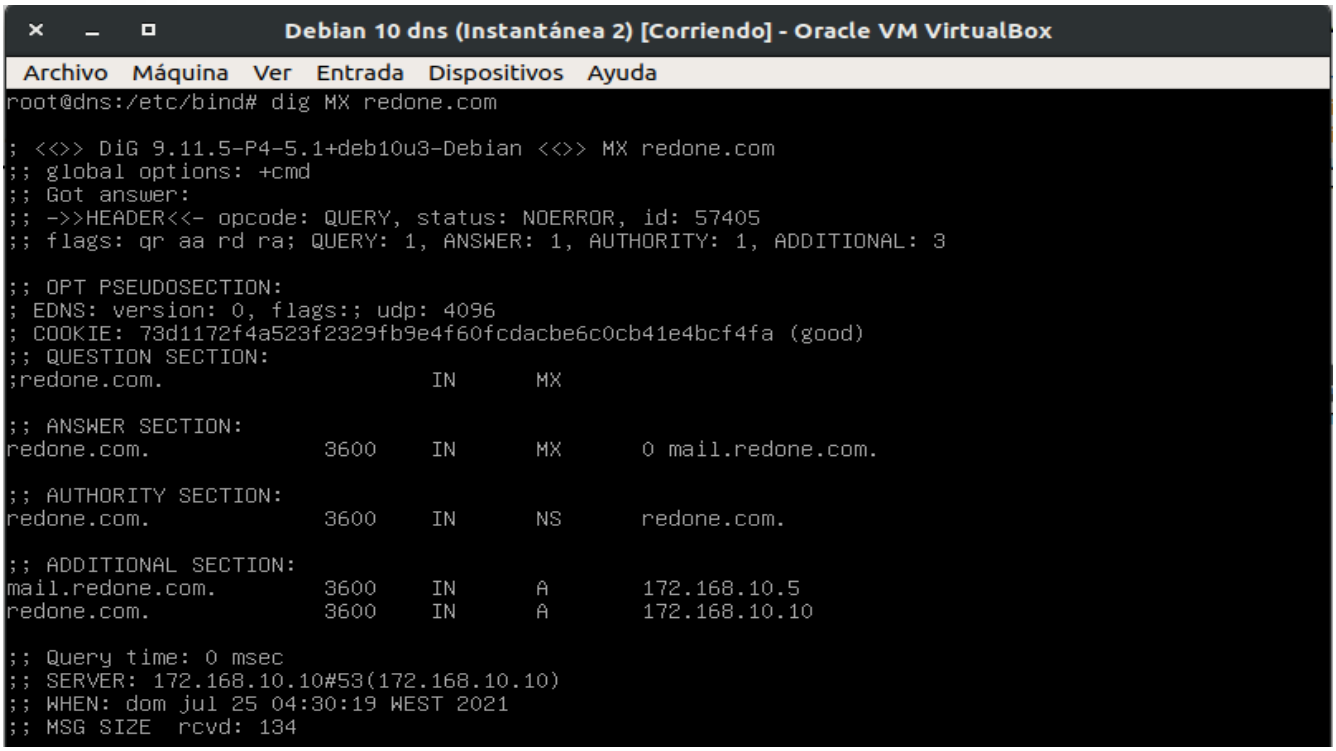

Figura 45. Configuración Archivo Hosts en Zimbra

Instalación

Lo primero que tendremos que hacer es descargar la última Release de Zimbra Collaboration, en este caso 8.8.15 para Ubuntu 16.04 LTS con el siguiente comando:

root@mail**:/home#wget** https://files.zimbra.com/downloads/8.**8.15_GA/zcs-8.8.15_GA_3869.UBUNTU16_64.20190918004220.tgz**

Después procederemos a descomprimir el fichero con el siguiente comando:

root@mail:/home#tar xzvf zcs-8.8.15_GA_3869.UBUNTU16_64.20190918004220.tgz

Nos moveremos hasta la nueva carpeta:

root@mail:/home#cd zcs-8.8.15_GA_3869.UBUNTU16_64.20190918004220.tgz

E instalaremos todos los paquetes necesarios para nuestro Single-Server, en mi caso he omitido dnscache, atentos a la opción extra que añado -s, para que simplemente instale los paquetes, sin añadir ninguna configuración. Este proceso dura 1 minuto y 10 segundos aproximadamente.

root@mail:/home/zcs-8.8.15_GA_3869.UBUNTU16_64.20190918004220# ./install.sh -s

Operations logged to /tmp/install.log.bd7JLFVk

Checking for existing installation...

zimbra-drive...NOT FOUND

zimbra-imapd...NOT FOUND

zimbra-patch...NOT FOUND

zimbra-mta-patch...NOT FOUND

zimbra-proxy-patch...NOT FOUND

zimbra-license-tools...NOT FOUND

zimbra-license-extension...NOT FOUND

zimbra-network-store...NOT FOUND

zimbra-network-modules-ng...NOT FOUND

zimbra-chat...NOT FOUND

zimbra-talk...NOT FOUND

zimbra-ldap...NOT FOUND

zimbra-logger...NOT FOUND

zimbra-mta...NOT FOUND

zimbra-dnscache...NOT FOUND

zimbra-snmp...NOT FOUND

zimbra-store...NOT FOUND

zimbra-apache...NOT FOUND

zimbra-spell...NOT FOUND

zimbra-convertd...NOT FOUND

zimbra-memcached...NOT FOUND

zimbra-proxy...NOT FOUND

zimbra-archiving...NOT FOUND

zimbra-core...NOT FOUND

PLEASE READ THIS AGREEMENT CAREFULLY BEFORE USING THE SOFTWARE.

SYNACOR, INC. ("SYNACOR") WILL ONLY LICENSE THIS SOFTWARE TO YOU IF YOU FIRST ACCEPT THE TERMS OF THIS AGREEMENT. BY DOWNLOADING OR INSTALLING THE SOFTWARE, OR USING THE PRODUCT, YOU ARE CONSENTING TO BE BOUND BY THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, THEN DO NOT DOWNLOAD, INSTALL OR USE THE PRODUCT.

License Terms for this Zimbra Collaboration Suite Software:

https://www.zimbra.com/license/zimbra-public-eula-2-6.html

Do you agree with the terms of the software license agreement? [N] Y

Aquí nos preguntara si deseamos utilizar los repositorios de Zimbra, presionaremos y damos Enter

Use Zimbra's package repository [Y] y

Importing Zimbra GPG key

Configuring package repository

Checking for installable packages

Found zimbra-core (local)

Found zimbra-ldap (local)

Found zimbra-logger (local)

Found zimbra-mta (local)

Found zimbra-dnscache (local)

Found zimbra-snmp (local)

Found zimbra-store (local)

Found zimbra-apache (local)

Found zimbra-spell (local)

Found zimbra-memcached (repo)

Found zimbra-proxy (local)

Found zimbra-drive (repo)

Found zimbra-imapd (local)

Found zimbra-patch (repo)

Found zimbra-mta-patch (repo)

Found zimbra-proxy-patch (repo)

Select the packages to install

Esta parte es la más importante, vamos a instalar sólo los paquetes necesarios **y además instalaremos el nuevo Chat y Drive. Para seleccionar, pulsaremos** *Enter***.**

Select the packages to install
Install zimbra-ldap [Y]
Install zimbra-logger [Y]
Install zimbra-mta [Y]
Install zimbra-dnscache [Y] N - IMPORTANTE ESCRIBIR (N)!!!!!!!!!!
Install zimbra-snmp [Y]
Install zimbra-store [Y]
Install zimbra-apache [Y]
Install zimbra-spell [Y]
Install zimbra-memcached [Y]
Install zimbra-proxy [Y]
Install zimbra-drive [Y]
Install zimbra-imapd (BETA - for evaluation only) [N]

Install zimbra-chat [Y]

Checking required space for zimbra-core

Checking space for zimbra-store

Checking required packages for zimbra-store

zimbra-store package check complete.

Installing:

- **zimbra-core**
- **zimbra-ldap**
- **zimbra-logger**
- **zimbra-mta**
- **zimbra-snmp**
- **zimbra-store**
- **zimbra-apache**
- **zimbra-spell**
- **zimbra-memcached**
- **zimbra-proxy**
- **zimbra-drive**
- **zimbra-patch**
- **zimbra-mta-patch**
- **zimbra-proxy-patch**
- **zimbra-chat**

Presionaremos *"y"* **para modificar el sistema:**

The system will be modified. Continue? [N] Y

Beginning Installation - see /tmp/install.log.TAoCzw2g for details...

zimbra-core-components will be downloaded and installed.

zimbra-timezone-data will be installed.

zimbra-common-mbox-conf-rights will be installed.

zimbra-common-mbox-conf-attrs will be installed.

zimbra-common-mbox-native-lib will be installed.

zimbra-common-core-jar will be installed.

zimbra-common-mbox-docs will be installed.

zimbra-common-mbox-db will be installed.

zimbra-common-core-libs will be installed.

zimbra-common-mbox-conf-msgs will be installed.

zimbra-common-mbox-conf will be installed.

zimbra-core will be installed.

zimbra-ldap-components will be downloaded and installed.

zimbra-ldap will be installed.

zimbra-logger will be installed.

zimbra-mta-components will be downloaded and installed.

zimbra-mta will be installed.

zimbra-snmp-components will be downloaded and installed.

zimbra-snmp will be installed.

zimbra-store-components will be downloaded and installed.

zimbra-jetty-distribution will be downloaded and installed.

zimbra-mbox-war will be installed.

zimbra-mbox-admin-console-war will be installed.

zimbra-mbox-store-libs will be installed.

zimbra-mbox-conf will be installed.

zimbra-mbox-service will be installed.

zimbra-mbox-webclient-war will be installed.

zimbra-store will be installed.

zimbra-apache-components will be downloaded and installed.

zimbra-apache will be installed.

zimbra-spell-components will be downloaded and installed.

zimbra-spell will be installed.

zimbra-memcached will be downloaded and installed.

zimbra-proxy-components will be downloaded and installed.

zimbra-proxy will be installed.

zimbra-drive will be downloaded and installed (later).

zimbra-patch will be downloaded and installed (later).

zimbra-mta-patch will be downloaded and installed (later).

zimbra-proxy-patch will be downloaded and installed (later).

zimbra-chat will be downloaded and installed (later).

Downloading packages (10):

zimbra-core-components

zimbra-ldap-components

zimbra-mta-components

zimbra-snmp-components

zimbra-store-components

zimbra-jetty-distribution

zimbra-apache-components

zimbra-spell-components

zimbra-memcached

zimbra-proxy-components

...done

Removing /opt/zimbra

Removing zimbra crontab entry...done.

Cleaning up zimbra init scripts...done.

Cleaning up /etc/security/limits.conf...done.

Finished removing Zimbra Collaboration Server.

Installing repo packages (10):

zimbra-core-components

zimbra-ldap-components

zimbra-mta-components

zimbra-snmp-components

zimbra-store-components

zimbra-jetty-distribution

zimbra-apache-components

zimbra-spell-components

zimbra-memcached

zimbra-proxy-components

...done

Installing local packages (25):

zimbra-timezone-data

zimbra-common-mbox-conf-rights

zimbra-common-mbox-conf-attrs

zimbra-common-mbox-native-lib

zimbra-common-core-jar

zimbra-common-mbox-docs

zimbra-common-mbox-db

zimbra-common-core-libs

zimbra-common-mbox-conf-msgs

zimbra-common-mbox-conf

zimbra-core

zimbra-ldap

zimbra-logger

zimbra-mta

zimbra-snmp

zimbra-mbox-war

zimbra-mbox-admin-console-war

zimbra-mbox-store-libs

zimbra-mbox-conf

zimbra-mbox-service

zimbra-mbox-webclient-war

zimbra-store

zimbra-apache

zimbra-spell

zimbra-proxy

...done

Installing extra packages (5):

zimbra-drive

zimbra-patch

zimbra-mta-patch

zimbra-proxy-patch

zimbra-chat

...done

Running Post Installation Configuration:

Operations logged to /tmp/zmsetup.20200329-004453.log

Installing LDAP configuration database...done.

Setting defaults…

Ahora tendremos que cambiar el dominio por defecto, cuidado al realizar este cambio.

DNS ERROR resolving MX for mail.redone.com

It is suggested that the domain name have an MX record configured in DNS

Change domain name? [Yes]

Create domain: [mail.redone.com] redone.com

MX: mail.redone.com (172.168.10.5)

Interface: 127.0.0.1

Interface: ::1

Interface: ::2

Interface: 172.168.10.5

Interface: 192.168.1.12

done.

Vamos a cambiar la password de admin. Vamos a entrar en el menú 6 **del principal y luego el** submenú 4 **para cambiar la password de administrador de zimbra:**

Select, or 'r' for previous menu [r] 4

Password for admin@redone.comcom (min 6 characters): [jqR3yaoTrT] mipassword

Store configuration

1) Status: Enabled

2) Create Admin User: yes

3) Admin user to create: admin@redone.comcom

*****4) Admin Password set**

5) Anti-virus quarantine user: virus-quarantine.2ednpmku@redone.com

6) Enable automated spam training: yes

7) Spam training user: spam.oyqjuc6c@redone.com

8) Non-spam(Ham) training user: ham.yifkpjdo@redone.com

9) SMTP host: mail.redone.com

10) Web server HTTP port: 8080

11) Web server HTTPS port: 8443

12) Web server mode: https

13) IMAP server port: 7143

14) IMAP server SSL port: 7993

15) POP server port: 7110

16) POP server SSL port: 7995

17) Use spell check server: yes

18) Spell server URL: http://mail.redone.comcom:7780/aspell.php

19) Enable version update checks: TRUE

20) Enable version update notifications: TRUE

21) Version update notification email: admin@redone.com

22) Version update source email: admin@redone.com

23) Install mailstore (service webapp): yes

24) Install UI (zimbra,zimbraAdmin webapps): yes

Pulsamos Enter para regresar al menú principal

Select, or 'r' for previous menu [r] r

Main menu

1) Common Configuration:

2) zimbra-ldap: Enabled

3) zimbra-logger: Enabled

4) zimbra-mta: Enabled

5) zimbra-snmp: Enabled

6) zimbra-store: Enabled

7) zimbra-spell: Enabled

8) zimbra-proxy: Enabled

9) Default Class of Service Configuration:

s) Save config to file

x) Expand menu

q) Quit

Presionamos a **para aplicar los cambios**

***** CONFIGURATION COMPLETE - press 'a' to apply**

Select from menu, or press 'a' to apply config (? - help) a

Pulsamos Enter

Save configuration data to a file? [Yes]

Pulsamos Enter nuevamente

Save config in file: [/opt/zimbra/config.13192]

Saving config in /opt/zimbra/config.13192...done.

Escribimos YES para modificar el sistema

The system will be modified - continue? [No] YES

Operations logged to /tmp/zmsetup.20200329-004453.log

Setting local config values…

Ahora debemos esperar que el proceso de instalación finalice, puede tardar hasta 10 minutos o en otras ocasiones un poco más.

Al finalizar la instalación le preguntar si desea notificar a Zimbra, le daremos que no.

Finished installing common zimlets.

Restarting mailboxd...done.

Creating galsync account for default domain...done.

You have the option of notifying Zimbra of your installation.

This helps us to track the uptake of the Zimbra Collaboration Server.

The only information that will be transmitted is:

The VERSION of zcs installed (8.8.15_GA_3869_UBUNTU16_64)

The ADMIN EMAIL ADDRESS created (admin@redone.com)

Notify Zimbra of your installation? [Yes] NO

Abrimos el navegador y como vemos ya podemos entrar a la página principal de zimbra

Figura 46. Login de Zimbra

Configuración necesaria de zimbra después de la instalación

lo primero es acceder al panel del administrador

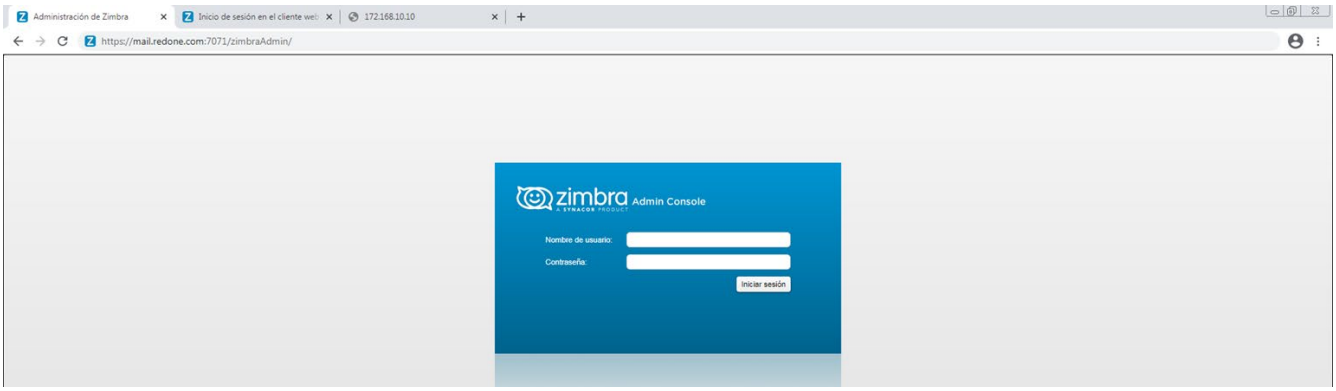

Figura 47. Login de Zimbra

Si nos olvidamos de la clave del admin, se puede cambiar con el comando /opt/zimbra/bin/zmprov sp admin@cloudperu.pe "NuevaClaveSuperFuerte"

Al acceder al panel nos nuestra primero el estado de servicios, el cual a veces no funciona bien, por ello

Ejecutar, mejor en consola para ver el estado real de los servicios

su - zimbra -c "zmcontrol status"

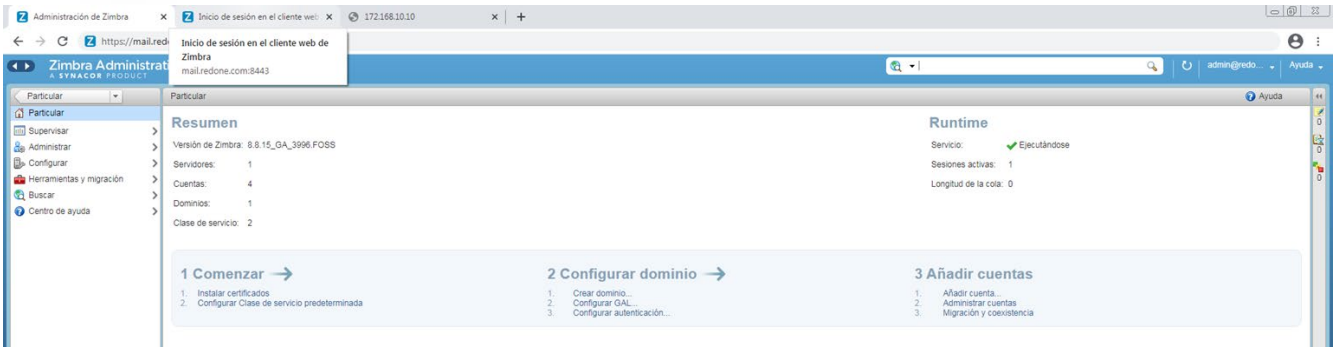

Figura 48. Panel de Administración de Zimbra

Menús Principales

Al lado izquierdo tenemos los siguientes Menús

- **Supervisar**
- **Administrar**
- **Configurar**
- **Herramientas y Migración**
- **Buscar**

Sin embargo; cuando queremos desplegar por primera vez Zimbra, veremos el siguiente orden.

Configurar, Administrar, Supervisar, Buscar, Herramientas y Migración

Configuración General (Le afecta todos los servidores)

Tamaño máximo que podemos subir en upload Tamaño máximo de un archivo cargado desde el escritorio (KB): 10240

pero como administradores tenemos el poder de modificar dichos valores

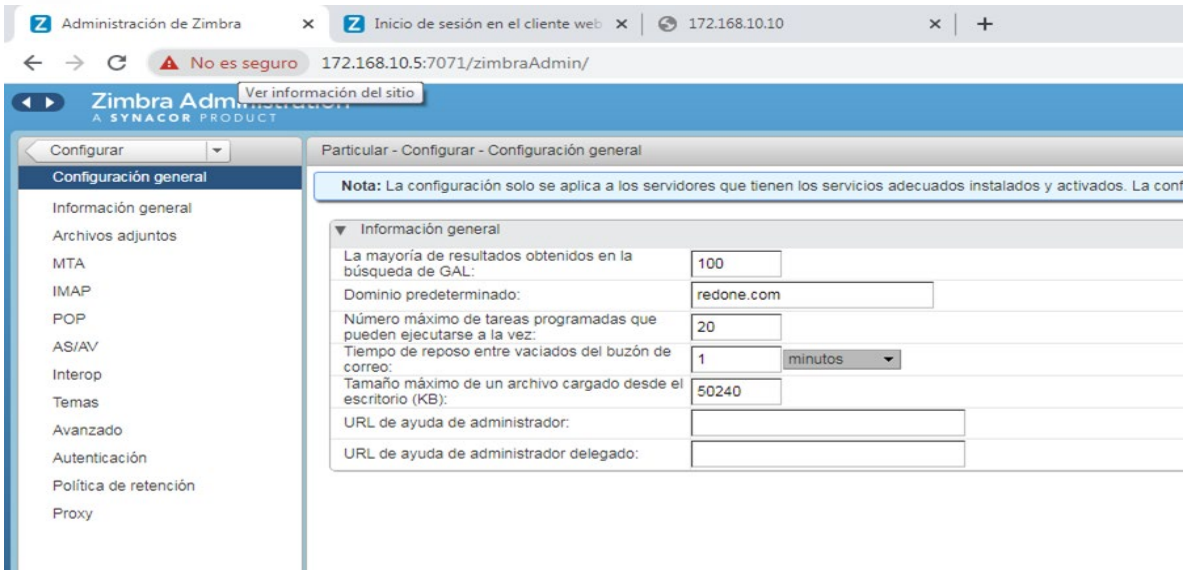

Figura 49. Configuraciones Básicas de Zimbra

en la anterior imagen lo hemos modificado a una cantidad mucho mayor

Archivos Adjuntos

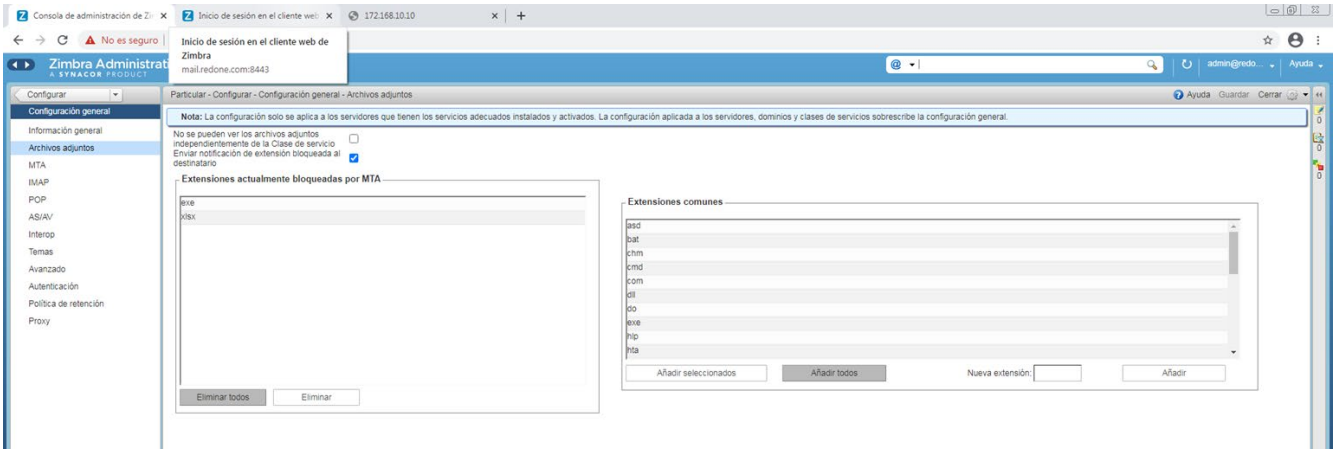

Figura 50. Configuraciones Básicas de Zimbra

Enviar notificación de extensión bloqueada al destinatario, el administrador tiene el poder de bloquear todas las extensiones que crea peligrosas y tener un mejor control en él envió de archivos maliciosos.

5.4. Pruebas Suite Kopano

5.4.1. Prueba de envío de correo entre Suite:

Para comprobar que existe comunicación entre las distintas suites es necesario el envío de información través de las plataformas de correo que hemos instalado en cada institución, así como la verificación de datos en los archivos logs para saber que sucedió y que mensajes indica el sistema los estatus de correo.

Para ello se enviarán 3 tipos de archivos a través de correo electrónico, y serán texto plano, un archivo .zip y archivo .exe

Envío de correo Kopano hacia Zimbra y Open Xchange

De: Jason96@credobank.com a: Fabian@teknova.com smith@redone.com

Texto Plano

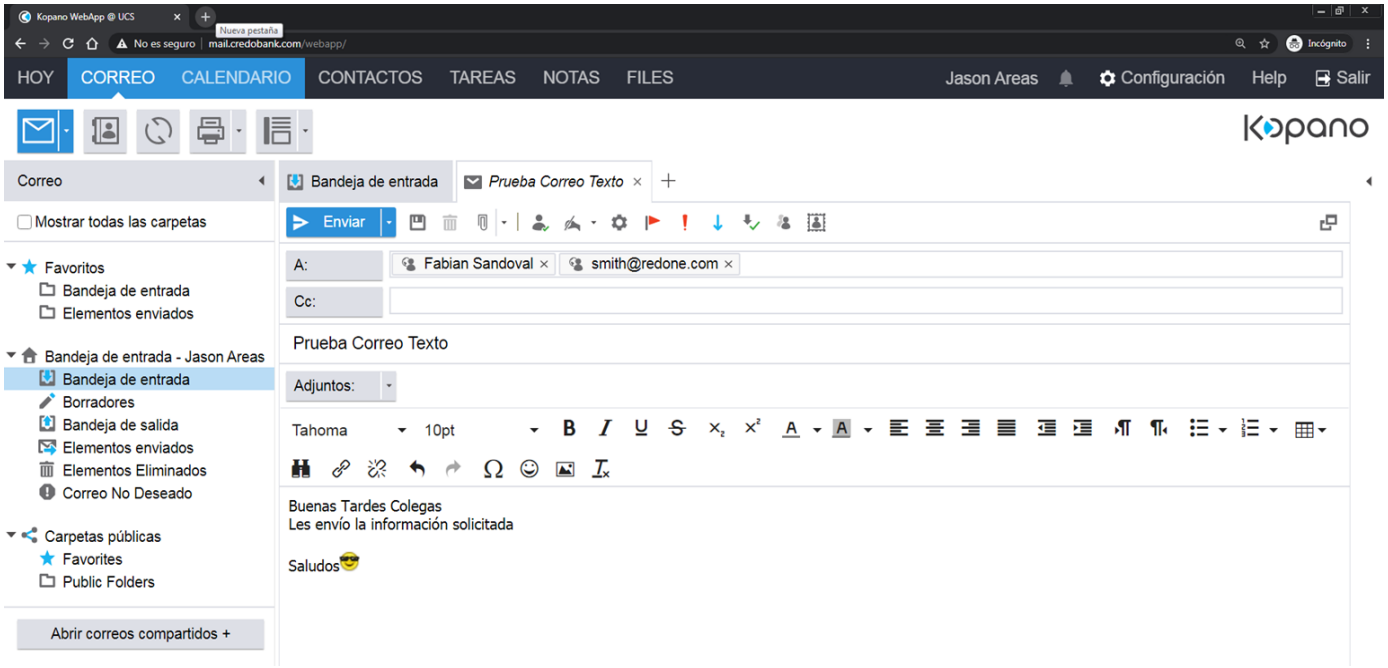

Figura 51. Envío de correo Kopano hacia Zimbra y Open Xchange

Como podemos ver se ha enviado correo a 2 de nuestros colegas de otras empresas con un simple texto de mensaje.

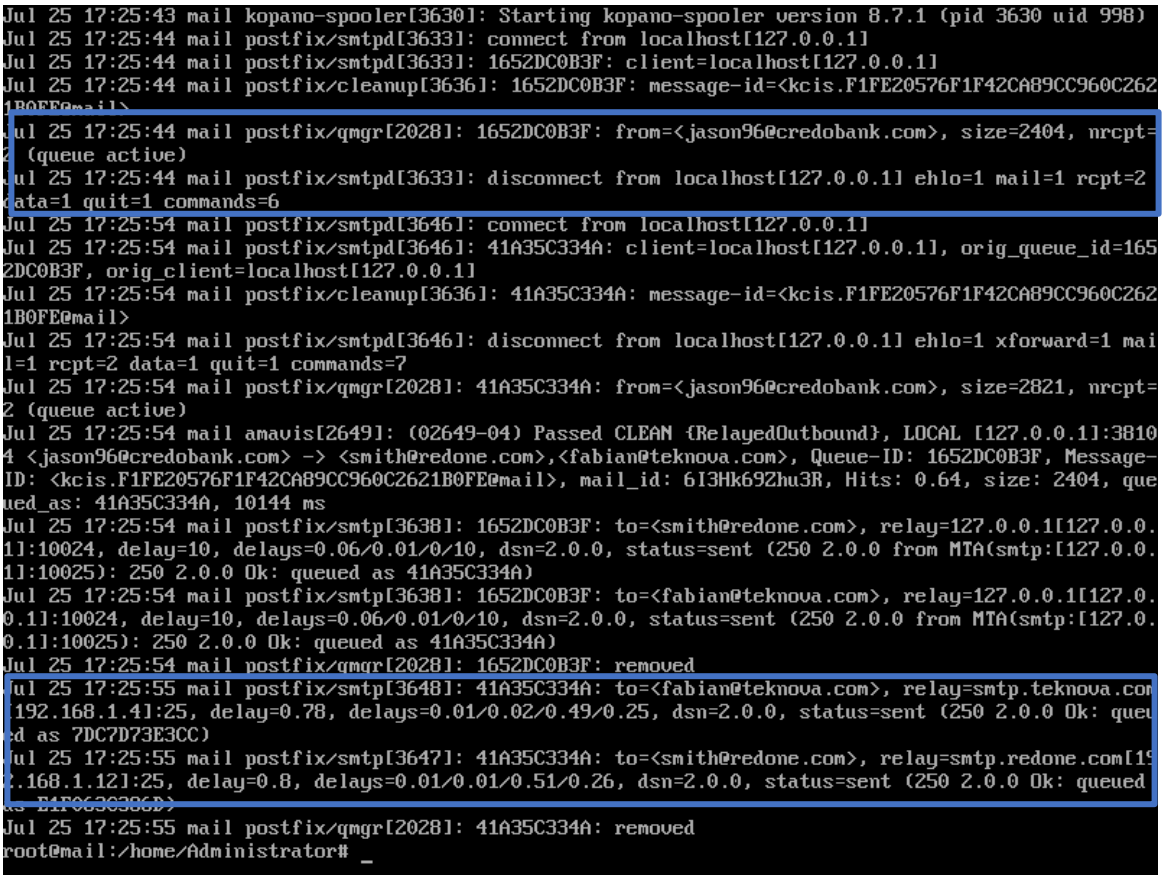

Figura 52. Log de Envío de correo Kopano hacia Zimbra y Open Xchange

Como podemos observar antes de hacer el envío de los correos se ha realizado un análisis interno con el motor de detección de virus para verificar la integridad y seguridad a fin de que no sea utilizado el servicio para fines dañinos o riesgosos para los demás usuarios.

Se registró el envío del correo hacia las direcciones que hemos indicado en el campo de destinatario en la plataforma de correo de Kopano, y como podemos ver en nuestro servidor encontró que dichas direcciones de correo son válidas por comprobación de dominio y que si se pudo entregar hacia el servidor destinatario con un mensaje de confirmación de entrega en nuestro Log.

La entrega final dependerá de las políticas o filtros internos de los servidores de correo externas.

Envío Archivo .Zip: De: Jason96@credobank.com a: Fabian@teknova.com smith@redone.com

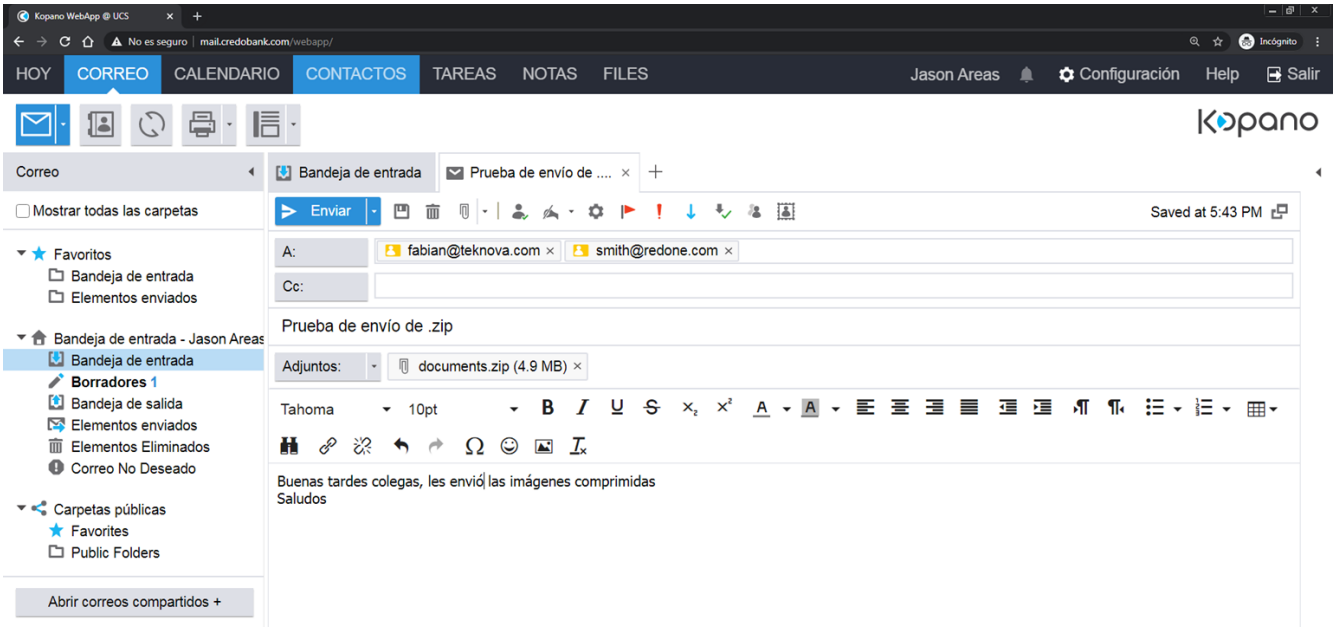

Figura 53. Envío de correo Kopano hacia Zimbra y Open Xchange

```
k.com Ok)
Jul 25 17:38:04 mail postfix/qmgr[2028]: 7D228C334A: removed
Jul 25 17:41:13 mail postfix/anvil[3791]: statistics: max connection rate 1/60s for (smtp:192.168.1.
4) at Jul 25 17:36:06
Jul 25 17:41:13 mail postfix/anvil[3791]: statistics: max connection count 1 for (smtp:192.168.1.4)
at Jul 25 17:36:06
Jul 25 17:41:13 mail postfix/anvil[3791]: statistics: max cache size 1 at Jul 25 17:36:06
Jul 25 17:43:34 mail kopano-spooler[4084]: Starting kopano-spooler version 8.7.1 (pid 4084 uid 998)
Jul 25 17:43:35 mail postfix/smtpd[4087]: connect from localhost[127.0.0.1]
Jul 25 17:43:35 mail postfix/smtpd[4087]: 51EA1C0B3F: client=localhost[127.0.0.1]
Jul 25 17:43:35 mail postfix/cleanup[4090]: 51EA1C0B3F: message-id=<kcis.C89B71D155904EBCABBE24486BD
74875@mail>
Jul 25 17:43:35 mail postfix/qmgr[2028]: 51EA1C0B3F: from=<jason96@credobank.com>, size=6999742, nrc
pt=2 (queue active)
Jul 25 17:43:35 mail postfix/smtpd[4087]: disconnect from localhost[127.0.0.1] ehlo=1 mail=1 rcpt=2
data=1 quit=1 commands=6
Jul 25 17:43:44 mail postfix/smtpd[4096]: connect from localhost[127.0.0.1]
Jul 25 17:43:44 mail postfix/smtpd[4096]: 2EBC8C334A: client=localhost[127.0.0.1], orig_queue_id=51E
A1C0B3F, orig_client=localhost[127.0.0.1]
Jul 25 17:43:44 mail postfix/cleanup[4090]: 2EBC8C334A: message-id=<kcis.C89B71D155904EBCABBE24486BD
74875@mail>
Jul 25 17:43:44 mail postfix/smtpd[4096]: disconnect from localhost[127.0.0.1] ehlo=1 xforward=1 mai
l=1 rcpt=2 data=1 quit=1 commands=7
Jul 25 17:43:44 mail postfix/qmgr[2028]: 2EBC8C334A: from=<jason96@credobank.com>, size=7000159, nrc
pt=2 (queue active)
Jul 25 17:43:44 mail amavis[2649]: (02649-05) Passed CLEAN {RelayedOutbound}, LOCAL [127.0.0.1]:3858
4 <jason96@credobank.com> -> <smith@redone.com>,<fabian@teknova.com>, Queue-ID: 51EA1C0B3F, Message-
ID: <kcis.C89B71D155904EBCABBE24486BD74875@mail>, mail_id: tPB5plVo8N3j, Hits: -0.999, size: 6999742
, queued_as: 2EBC8C334A, 8854 ms
Jul 25 17:43:44 mail postfix/smtp[4091]: 51EA1C0B3F: to=<smith@redone.com>, relay=127.0.0.1[127.0.0.
1]:10024, delay=9, delays=0.13/0.04/0/8.9, dsn=2.0.0, status=sent (250 2.0.0 from MTA(smtp:[127.0.0.
1]:10025): 250 2.0.0 Ok: queued as 2EBC8C334A)
Jul 25 17:43:44 mail postfix/smtp[4091]: 51EA1C0B3F: to=<fabian@teknova.com>, relay=127.0.0.1[127.0.
0.1]:10024, delay=9, delays=0.13/0.04/0/8.9, dsn=2.0.0, status=sent (250 2.0.0 from MTA(smtp:[127.0.
0.1]:10025): 250 2.0.0 Ok: queued as 2EBC8C334A)
Jul 25 17:43:44 mail postfix/qmgr[2028]: 51EA1C0B3F: removed
root@mail:/home/Administrator#
```

Figura 54. Log Envío de correo Kopano hacia Zimbra y Open Xchange

Al igual que con la prueba anterior se registró un análisis del archivo enviado, ya que Amavis como antivirus, no solo analiza el contenido de correo sino también los archivos adjuntos comprimidos.

Envío de archivo particular. De: Jason96@credobank.com a: Fabian@teknova.com smith@redone.com

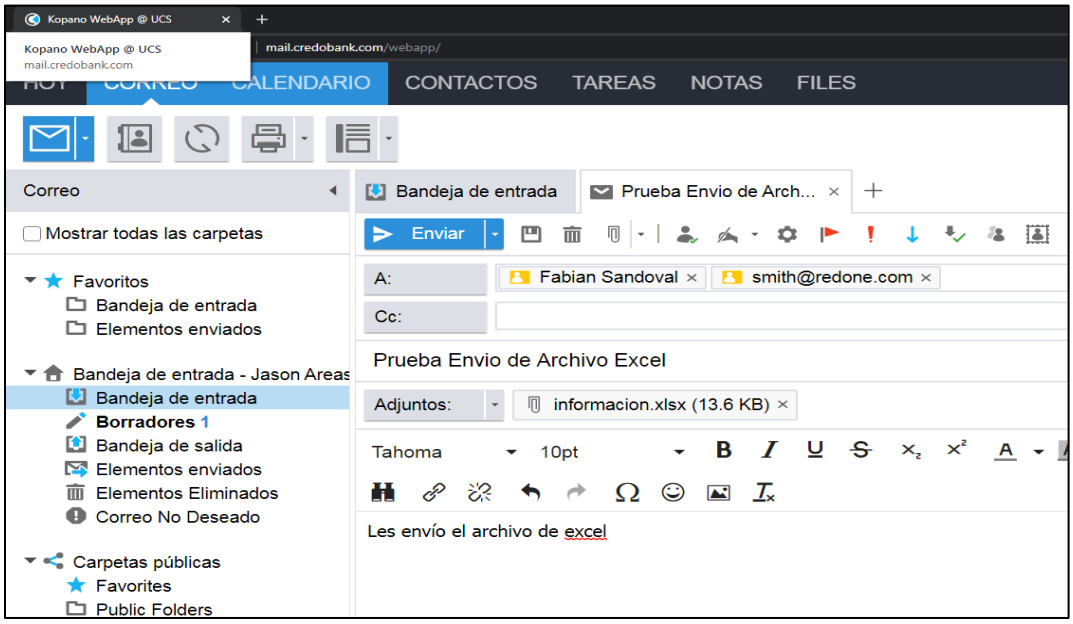

Figura 55. Envío de correo Kopano hacia Zimbra y Open Xchange

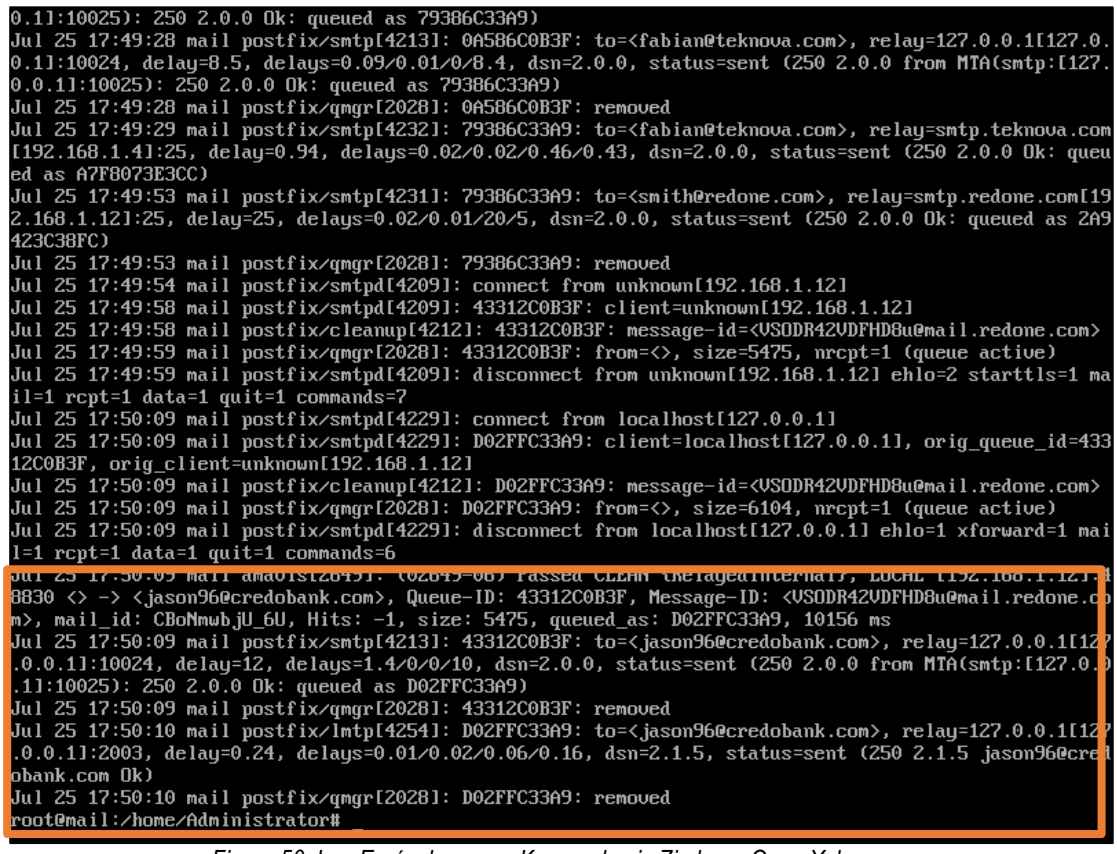

Figura 56. Log Envío de correo Kopano hacia Zimbra y Open Xchange

En esta prueba enviamos a nuestros colegas un archivo Excel, para confirmar que se puede enviar diversos archivos no solo texto plano. La diferencia entre un archivo Excel y un archivo comprimido es que el Excel es un solo archivo como tal y el comprimido puede contener muchos elementos contaminados de alguna amenaza.

5.4.2. Pruebas de correo Spam

Para esta sección, estaremos configurando y evaluando las diferentes opciones que nos brindan las suites para hacer filtrado de correo o reglas AntiSpam

Se realizarán pruebas simples de SPAM para clasificar correos electrónicos entrantes. Las reglas que estaremos aplicando se basarán en la recepción de hipervínculos tanto en el asunto como en el cuerpo del mensaje, palabras claves que no indiquen que es un correo no deseado, además de clasificar como Spam ciertos correo que posean un Tamaño total mayor a 4 mb.

Configuración y prueba en Kopano

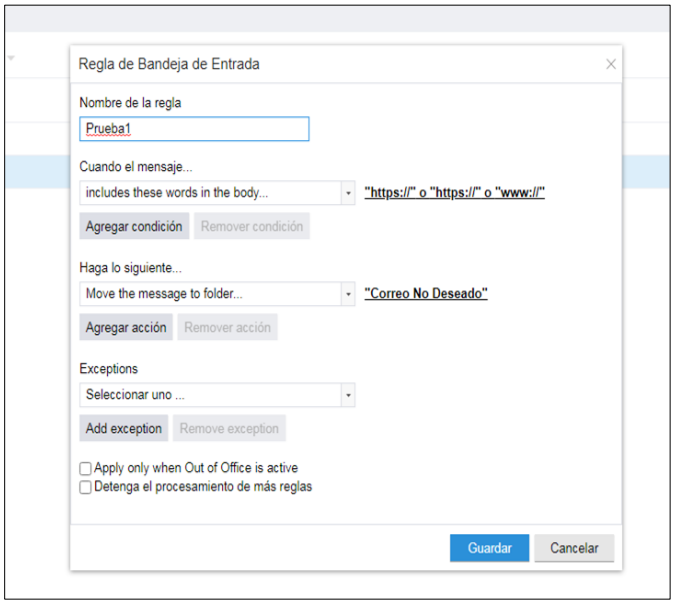

Figura 57. Ajustes para SPAM

Para aplicar esta regla debemos ubicarnos en la sección de configuración y acceder al módulo de "reglas" y definimos los parámetros necesarios que deseamos se cumplan.

Las otras 2 suites enviaran correo conteniendo un sitio web, para ver si los filtros SPAM no permiten la recepción de correos con sitios web. A: Jason96@credobank.com De: Fabian@teknova.com smith@redone.com

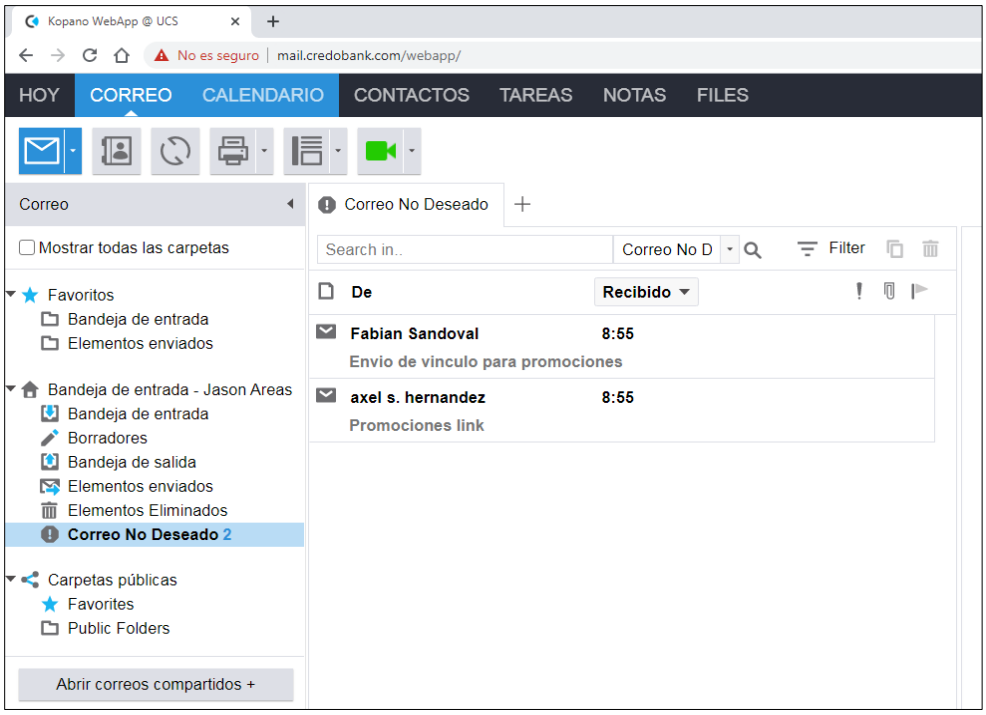

Figura 58. Bandeja de SPAM en KOPANO

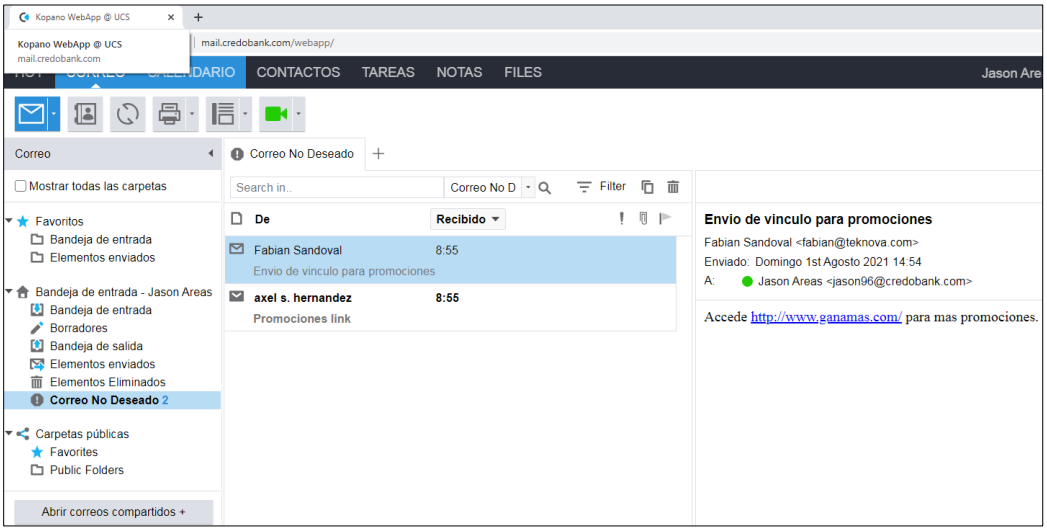

Figura 59. Bandeja de SPAM en KOPANO

Como podemos observar nos enviaron 2 correo que contienen Link a otros sitios, y el sistema lo clasifica como Spam de forma inmediata y nos lo presenta en la carpeta de correo no deseado.

Spam con palabras claves de Correo Spam en el cuerpo del mensaje.

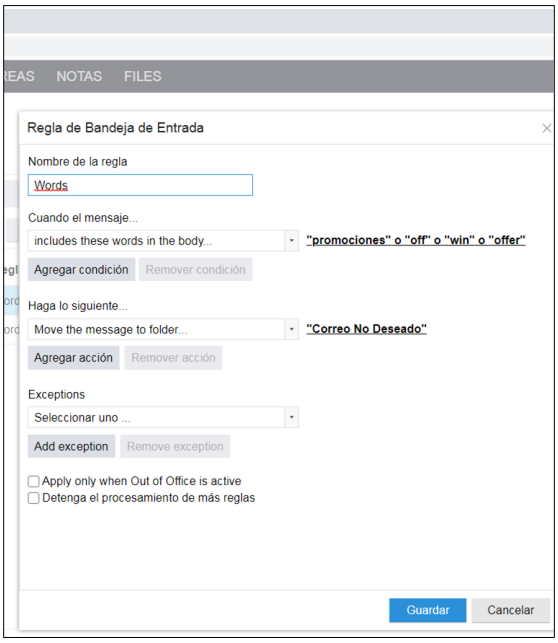

Figura 60. Ajustes para SPAM

Configuración de Spam con palabras en el asunto:

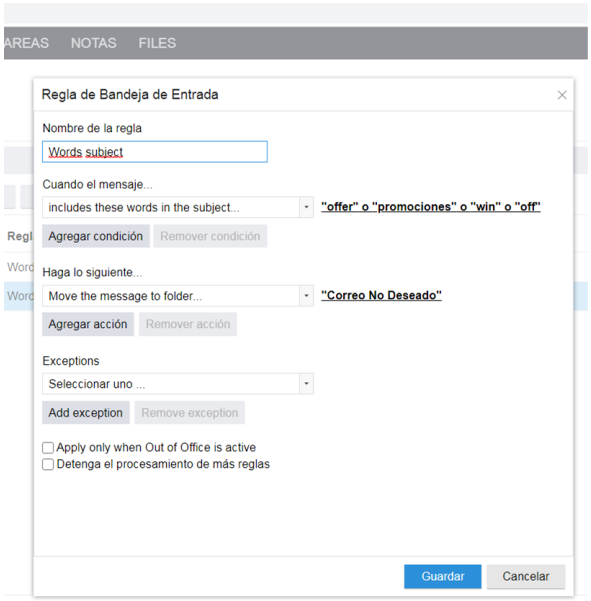

Figura 61. Ajustes para SPAM

La finalidad de definir estos parámetros es para que cuando se detecte frases o palabras usuales en correos SPAM sean detectados desde que se analice el asunto y/o cuerpo del mensaje.

Por lo tanto, el filtro si ha funcionado correctamente.

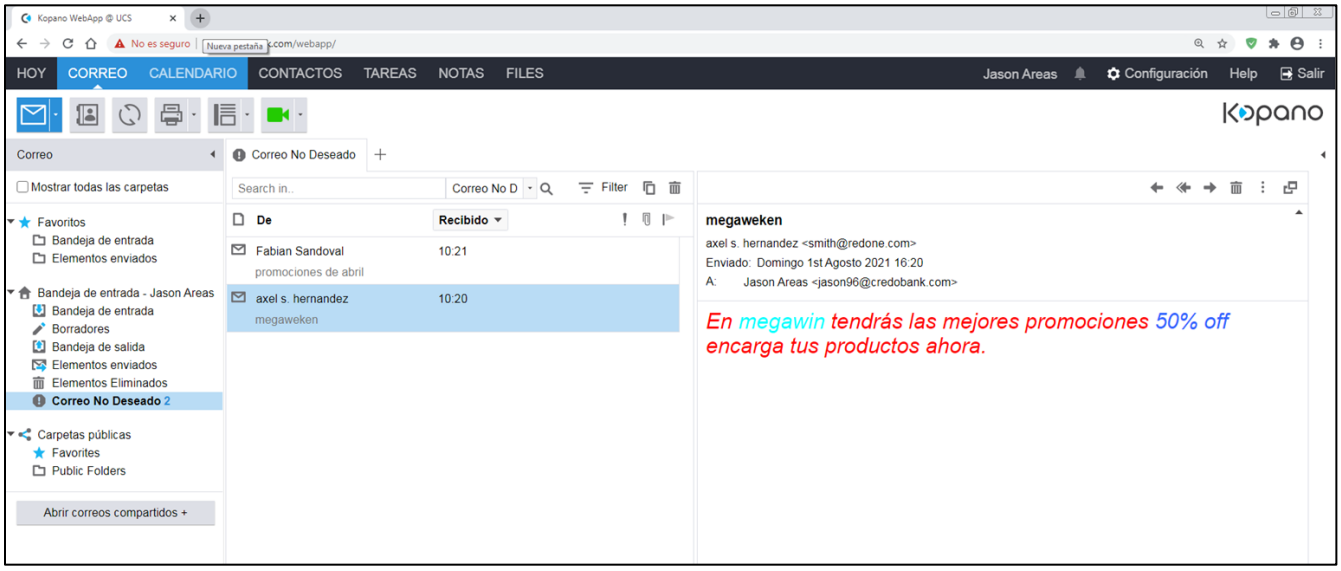

Figura 62. Bandeja SPAM en KOPANO

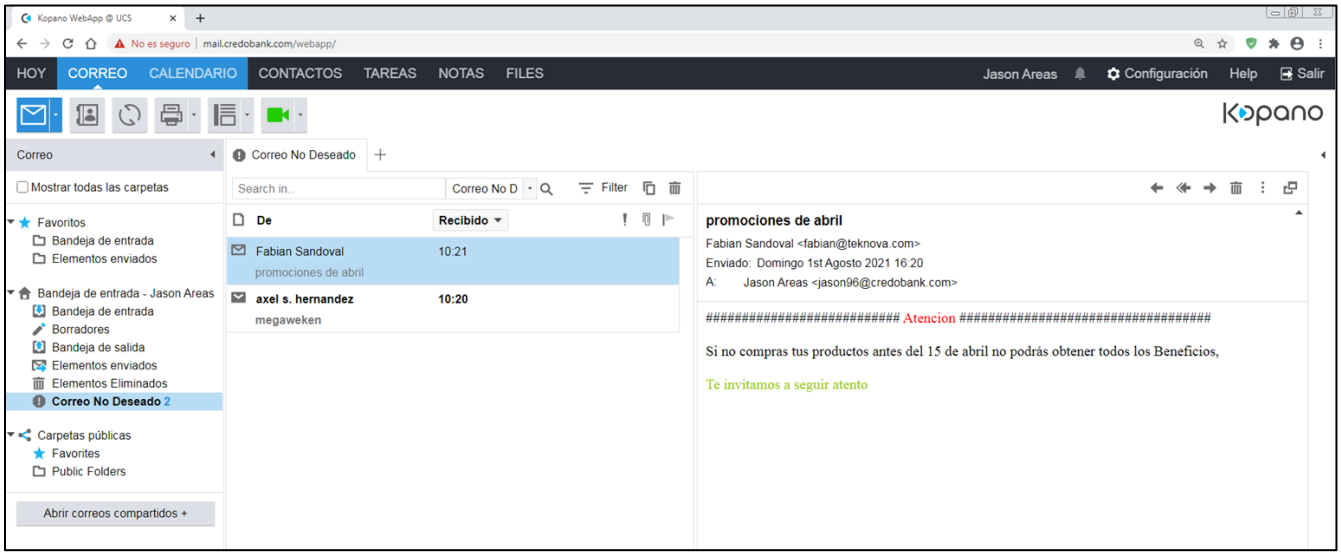

Figura 63. Bandeja SPAM en KOPANO

Ahora realizaremos la prueba de correo Spam por tamaño de mensaje mayor a 4MB. Entraremos a las opciones de configuración general y buscaremos la sección de reglas, ahí definiremos que le mensaje en tu totalidad tenga un peso mayor o igual a 4MB suponiendo que con ese peso se envíen mensajes con contenido basura por ello utilizaremos como referencia ese parámetro solo para comprobar funcionalidad.

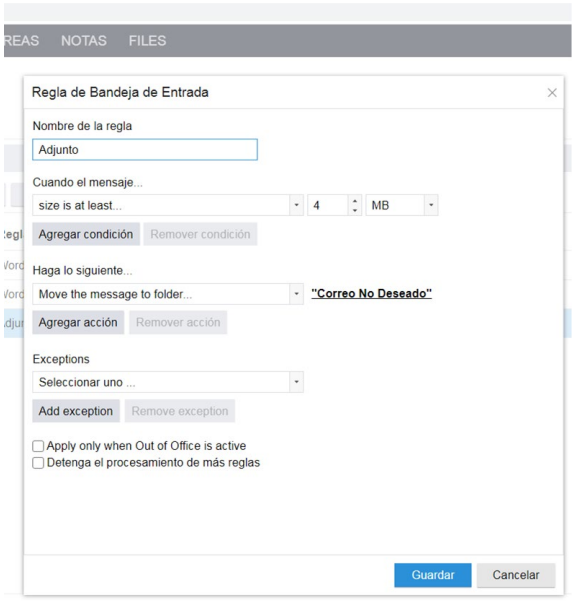

Figura 64. Ajustes SPAM

Obtenemos como resultado Final:

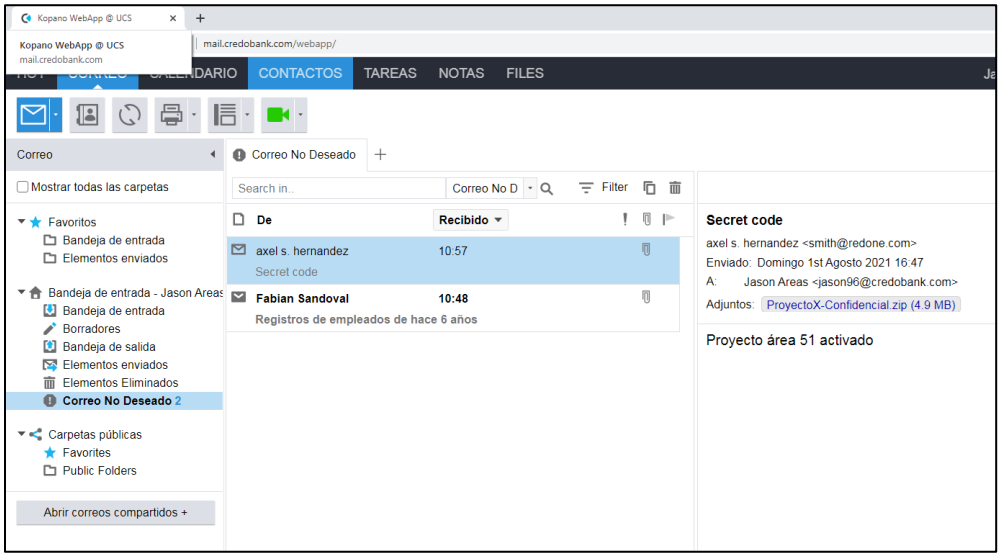

Figura 65. Bandeja SPAM en KOPANO

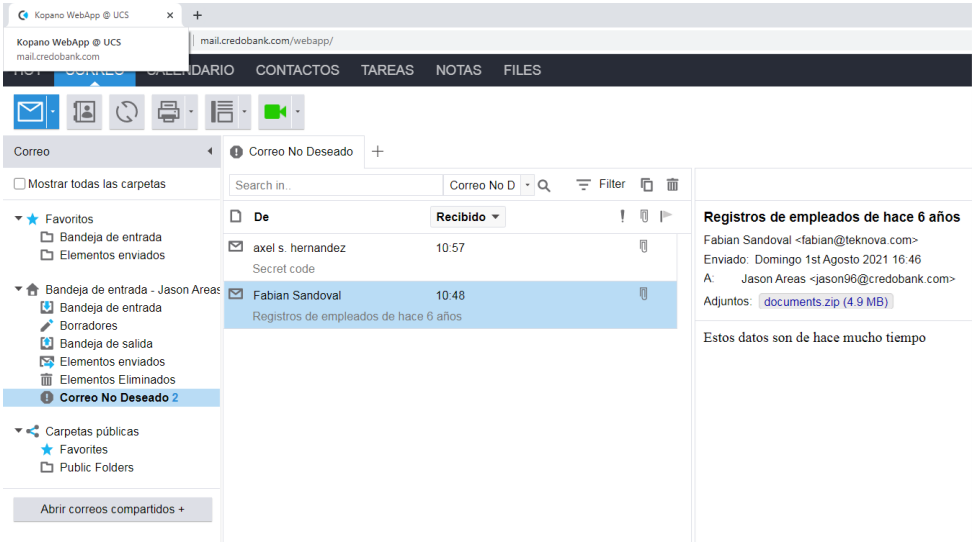

Figura 66. Bandeja SPAM en KOPANO

5.4.3. Pruebas Antivirus

Una de las principales características que deben poseer los servicios de correo, es la seguridad y no solo incluyendo la manera en cómo se transmite la información que en su mayoría es muy delicada por tratarse de información sensible de una empresa o documentos personales, la seguridad en un correo debe incluirse la temprana detección de contenido malicioso para así evitar ser una fuente de propagación de virus, para así en vez de ser una solución para la comunicación y no ser un problema para los usuarios de dichos servicios.

Procederemos a enviar un correo electrónico con un archivo adjunto PDF con contenido de código malicioso de prueba, para poner a prueba que tan eficaz es nuestro motor de análisis de Virus de Amavis.

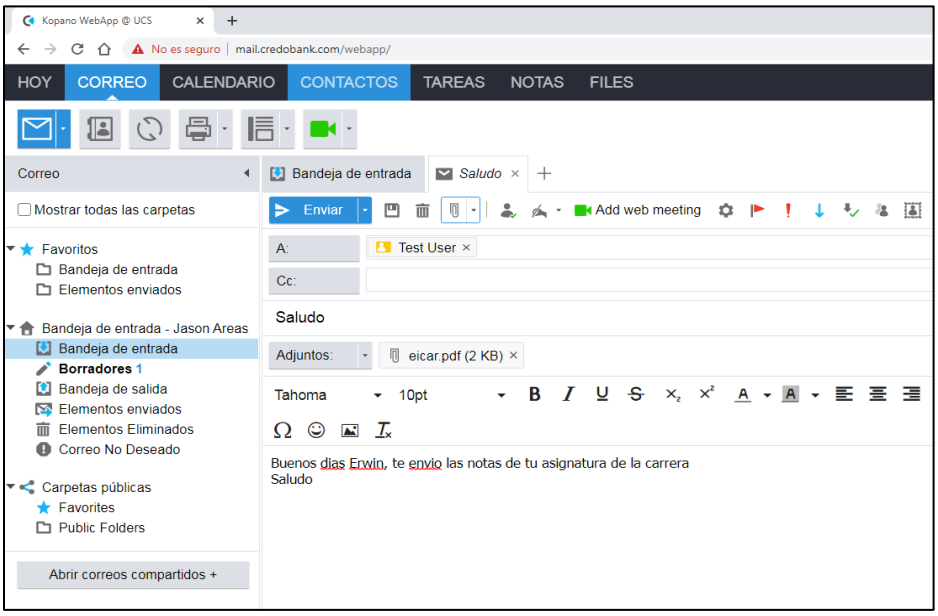

Figura 67. Prueba de Antivirus KOPANO

Intentamos enviar un correo común y corriente con código malicioso de prueba, cabe destacar que esta prueba es para comprobar que nuestra configuración de antivirus esta correcta y que analiza todo el contenido que se envía y recibe.

Se envió correo a nuestro contacto de OpenXchange con un documento PDF falso de notas escolares.

```
root@mail:/home/Administrator# tail -n 20 /var/log/mail.log
Aug  8 11:47:14 mail postfix/smtpd[3391]: disconnect from unknown[192.168.1.4] commands=0/0
Aug  8 11:50:34 mail postfix/anvil[3393]: statistics: max connection rate 1/60s for (smtp:192.168.1.
4) at Aug  8 11:42:14
Aug  8 11:50:34 mail postfix/anvil[3393]: statistics: max connection count 1 for (smtp:192.168.1.4)
at Aug  8 11:42:14
Aug  8 11:50:34 mail postfix/anvil[3393]: statistics: max cache size 1 at Aug  8 11:42:14
Aug  8 11:51:37 mail kopano-spooler[3707]: Starting kopano-spooler version 8.7.1 (pid 3707 uid 998)
Aug  8 11:51:37 mail postfix/smtpd[3710]: connect from localhost[127.0.0.1]
Aug  8 11:51:37 mail postfix/smtpd[3710]: B58FBC038F: client=localhost[127.0.0.1]
Aug  8 11:51:37 mail postfix/cleanup[3713]: B58FBC038F: message-id=<kcis.364CB7FFEA27446A9D97C40E566
4D428@mail>
Aug  8 11:51:37 mail postfix/qmgr[1775]: B58FBC038F: from=<jason96@credobank.com>, size=5115, nrcpt=
1 (queue active)
Aug  8 11:51:37 mail postfix/smtpd[3710]: disconnect from localhost[127.0.0.1] ehlo=1 mail=1 rcpt=1
data=1 quit=1 commands=5
Aug  8 11:51:37 mail postfix/smtpd[3718]: connect from localhost[127.0.0.1]
Aug  8 11:51:37 mail postfix/smtpd[3718]: E9F63C0390: client=localhost[127.0.0.1]
Aug  8 11:51:37 mail postfix/cleanup[3713]: E9F63C0390: message-id=<VAJHiWhfld8BfT@mail.credobank.co
m>
Aug  8 11:51:37 mail postfix/qmgr[1775]: E9F63C0390: from=<postmaster@mail.credobank.com>, size=2381
, nrcpt=1 (queue active)
Aug  8 11:51:37 mail postfix/smtpd[3718]: disconnect from localhost[127.0.0.1] ehlo=1 mail=1 rcpt=1
data=1 quit=1 commands=5
Aug  8 11:51:37 mail amavis[3603]: (03603-01) Blocked INFECTED (Pdf.Dropper.Agent-6299277-0) {Discar
dedOutbound,Quarantined}, LOCAL [127.0.0.1]:38034 <jason96@credobank.com> -> <fabian@teknova.com>, q
uarantine: J/virus-JHiWhfld8BfT, Queue-ID: B58FBC038F, Message-ID: <kcis.364CB7FFEA27446A9D97C40E566
4D428@mail>, mail_id: JHiWhfld8BfT, Hits: -, size: 5115, 185 ms
Aug  8 11:51:37 mail postfix/smtp[3714]: B58FBC038F: to=<fabian@teknova.com>, relay=127.0.0.1[127.0.
0.1]:10024, delay=0.25, delays=0.05/0.01/0.01/0.18, dsn=2.7.0, status=sent (250 2.7.0 Ok, discarded,
 id=03603-01 - INFECTED: Pdf.Dropper.Agent-6299277-0)
Aug  8 11:51:37 mail postfix/qmgr[1775]: B58FBC038F: removed
Aug  8 11:51:37 mail postfix/local[3719]: E9F63C0390: to=<systemmail@mail.credobank.com>, orig_to=<p
ostmaster@mail.credobank.com>, relay=local, delay=0.04, delays=0.02/0.01/0/0, dsn=2.0.0, status=sent
 (delivered to mailbox)
Aug  8 11:51:37 mail postfix/qmgr[1775]: E9F63C0390: removed
root@mail:/home/Administrator#
```

Figura 68. Log Prueba de Antivirus KOPANO

Como Vemos nuestro antivirus Amavis de KOPANO, lo ha analizado y detenido para posterior enviarlo a cuarentena y no permite que el remitente lo reciba, para evitar propagación de virus. Incluso si se pretende detener el servicio de antivirus, el sistema no permitirá que se envié ningún correo porque como medida de seguridad debe pasar por el scan para análisis que sea seguro nuestro correo.

Y al final el mismo sistema nos informa que el correo no fue enviado

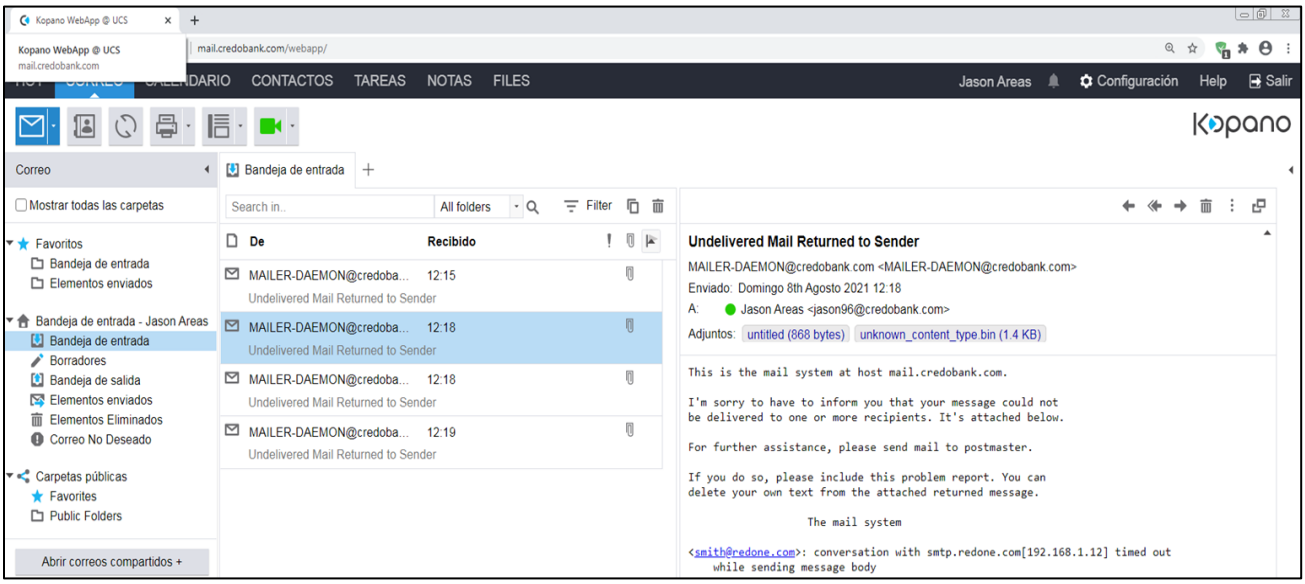

Figura 69. Bandeja de Entrada KOPANO - Antivirus

5.4.4. Prueba de envío de correo entre usuarios KOPANO

Desde el Usuario jason96@credobank.com se intentó enviar correo al usuario erwinsan@credobank.com y según el log fue identificado como Virus y el remitente recibo un correo de notificación que se ha intentado mandar un correo con contenido malicioso, el archivo que enviamos fue un PDF con líneas de código de Eicar Test.

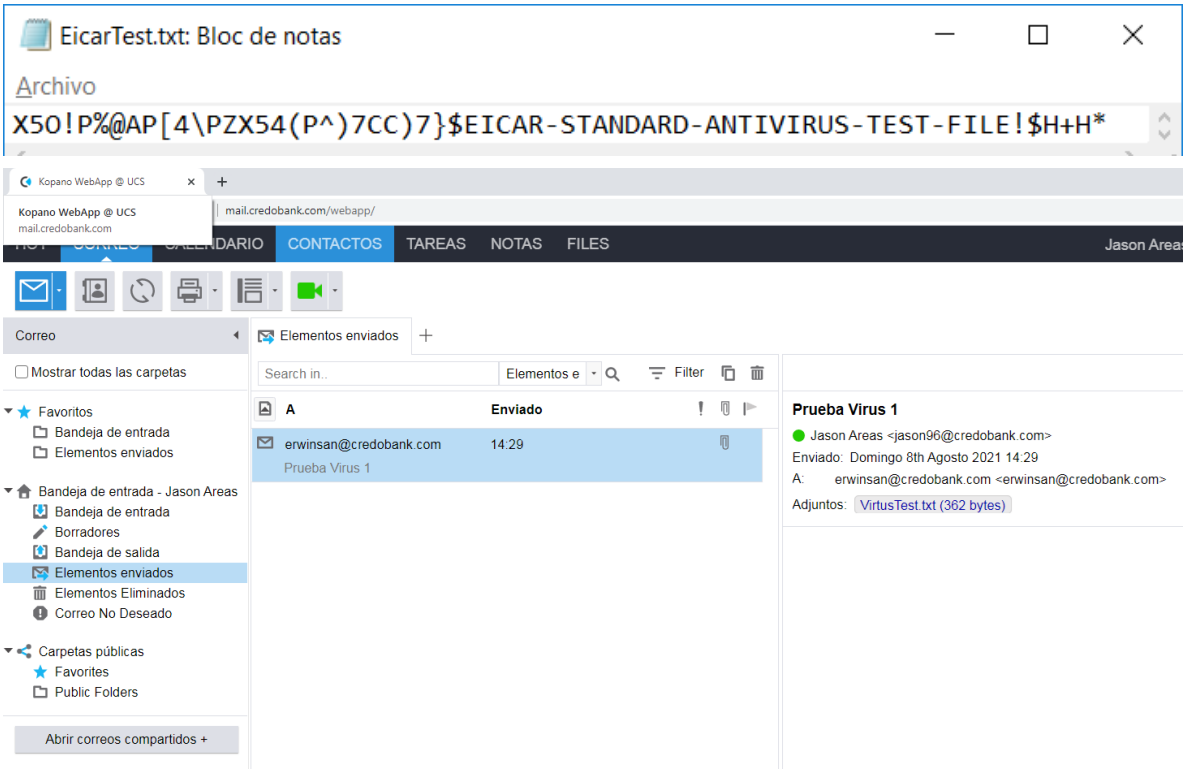

Figura 70. Envío de Correo entre Usuarios KOPANO

Cuando enviamos correo entre Usuarios Kopano de la misma compañía, nuestro servidor envía un correo informando a nuestro destinatario la incidencia de que se está tratando de enviar un correo malicioso desde una cuenta de correo X. con el fin de que dicho usuario tome las medidas necesarias.

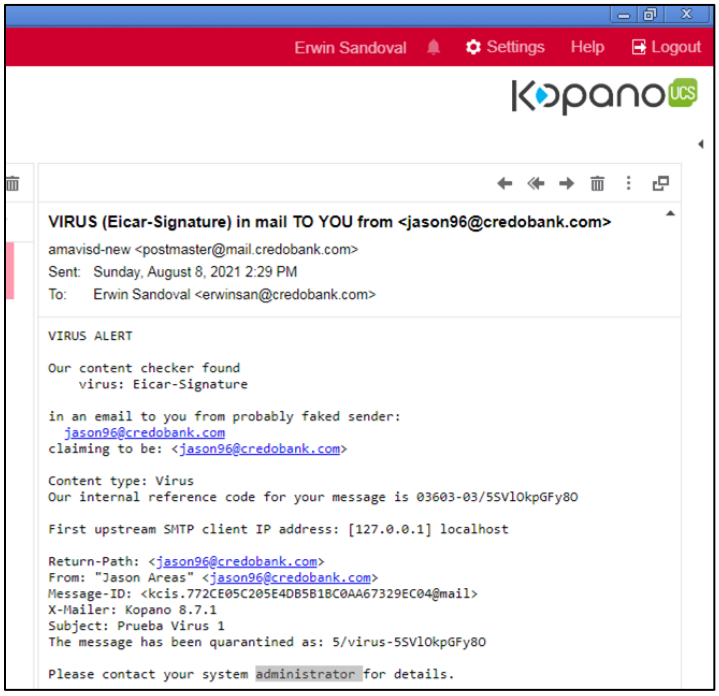

Figura 71. Mensaje de Antivirus en KOPANO

Ahora bien, intentar desactivar el antivirus para saltar los controles de seguridad supone la suspensión del servicio de correo, porque esta predefinido que todos los correos deben ser analizados previamente para su posterior envío o recepción.

5.4.5. Prueba de Envío de correo

Desde el Usuario jason96@credobank.com se intentó enviar correo al usuario erwinsan@credobank.com y según el log fue identificado como Virus y el remitente recibo un correo de notificación que se ha intentado mandar un correo con contenido malicioso, el archivo lo que enviamos fue un .exe que es activador, tipo troyano.

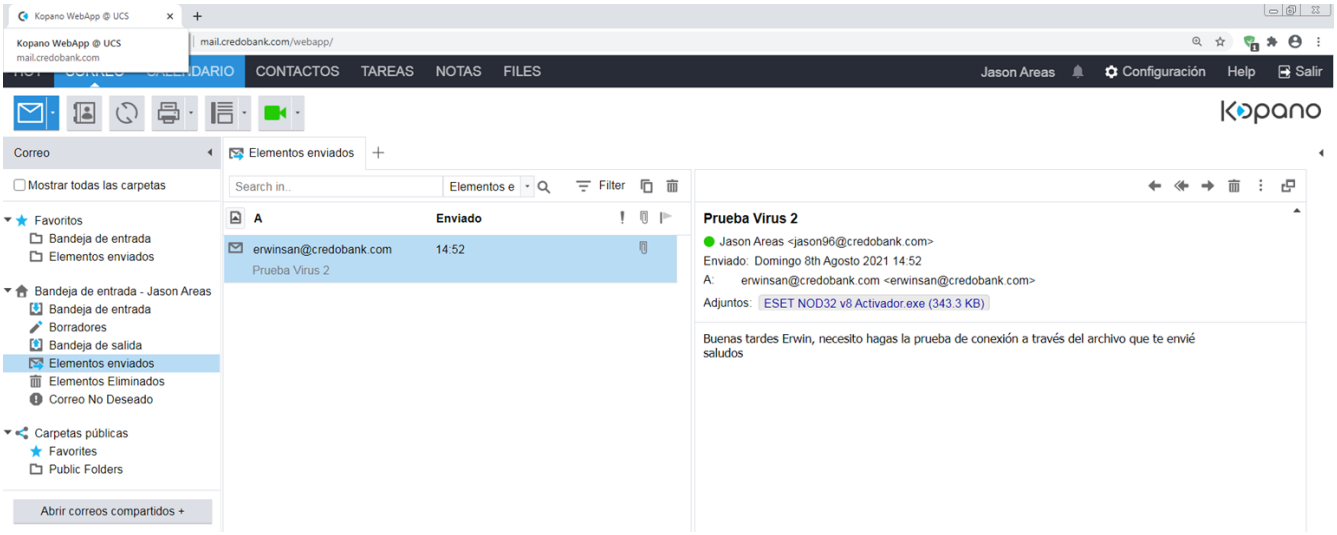

Figura 72. Envío de Virus en Correo KOPANO

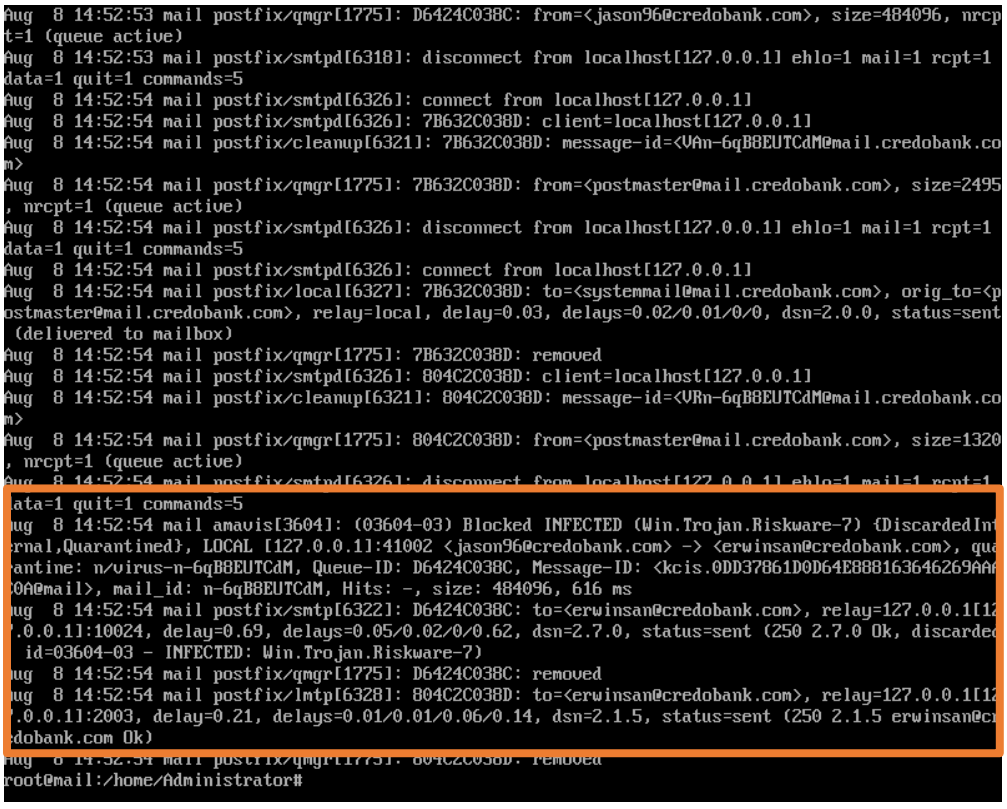

Figura 73. Log de Envío de Correo en KOPANO

Según nuestro Log, nos brinda los datos generales del correo, fechas, hora, dirección de remitente y destinatario. Y principalmente nos brinda una notificación de Amavis que descarga un correo por haber detectado un archivo de tipo troyano. Según el peso del archivo, tardara en analizar el correo.

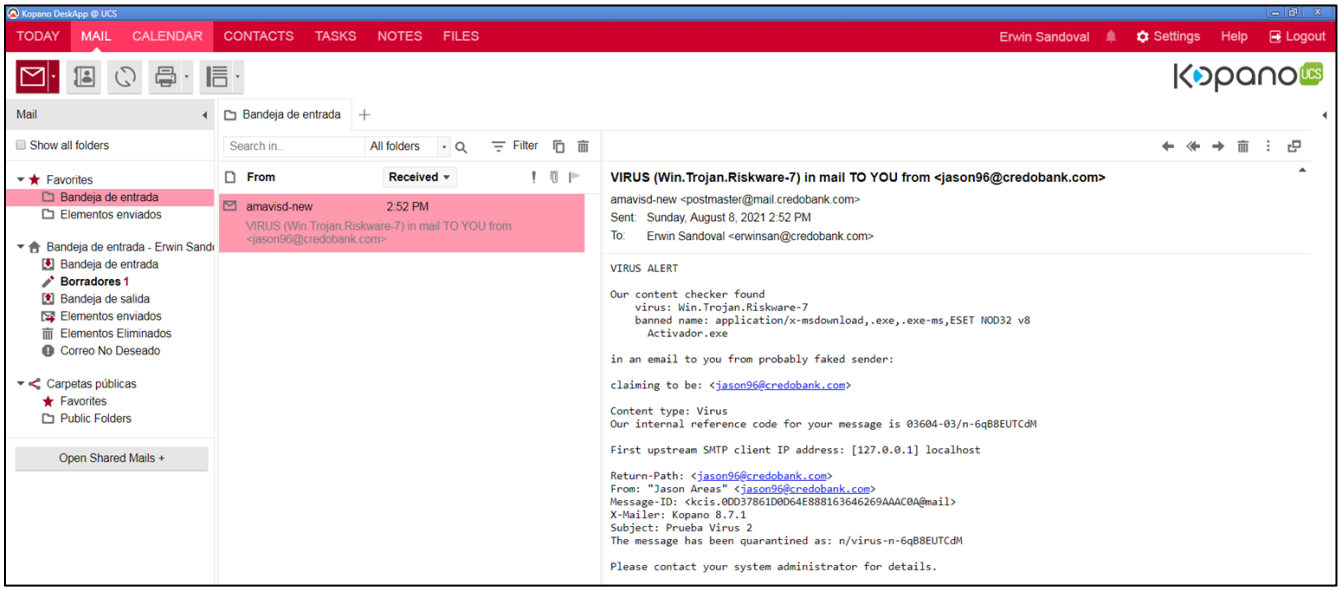

Figura 74. Mensaje de Alerta de Virus en KOPANO

El sistema envía el correo de notificación al destinatario informando la situación.

5.4.6. Recepción de Correo de OpenXchange de origen desconocido a jason96@credobank.com

desde el Correo fabian@teknova.com, se procedió a desactivar servicio de antivirus para analizar el comportamiento de Kopano frente a las amenazas que pueda recibir de otros servidores de correo en el log se observa que fue detectado por el servicio de Amavis en Kopano

```
Aug  8 15:02:32 mail postfix/qmgr[1775]: 272CBC038C: from=<fabian@teknova.com>, size=2289, nrcpt=1 (
queue active)
Aug  8 15:02:32 mail postfix/smtpd[6557]: disconnect from unknown[192.168.1.4] ehlo=1 mail=1 rcpt=1
data=1 quit=1 commands=5
Aug  8 15:02:32 mail postfix/smtpd[6567]: connect from localhost[127.0.0.1]
Aug  8 15:02:32 mail postfix/smtpd[6567]: 661EFC038D: client=localhost[127.0.0.1]
Aug  8 15:02:32 mail postfix/cleanup[6561]: 661EFC038D: message-id=<VA21EXU5sHENfa@mail.credobank.co
m>
Aug  8 15:02:32 mail postfix/smtpd[6567]: disconnect from localhost[127.0.0.1] ehlo=1 mail=1 rcpt=1
data=1 quit=1 commands=5
Aug  8 15:02:32 mail postfix/qmgr[1775]: 661EFC038D: from=<postmaster@mail.credobank.com>, size=2548
, nrcpt=1 (queue active)
Aug  8 15:02:32 mail postfix/smtpd[6567]: connect from localhost[127.0.0.1]
Aug  8 15:02:32 mail postfix/local[6568]: 661EFC038D: to=<systemmail@mail.credobank.com>, orig_to=<p
ostmaster@mail.credobank.com>, relay=local, delay=0.03, delays=0.02/0.01/0/0, dsn=2.0.0, status=sent
 (delivered to mailbox)
Aug  8 15:02:32 mail postfix/smtpd[6567]: 6AC4BC038E: client=localhost[127.0.0.1]
Aug  8 15:02:32 mail postfix/qmgr[1775]: 661EFC038D: removed
Aug  8 15:02:32 mail postfix/cleanup[6561]: 6AC4BC038E: message-id=<VR21EXU5sHENfa@mail.credobank.co
m>
Aug  8 15:02:32 mail postfix/smtpd[6567]: disconnect from localhost[127.0.0.1] ehlo=1 mail=1 rcpt=1
data=1 quit=1 commands=5
, nrcpt=1 (queue active)
Aug  8 15:02:32 mail amavis[3604]: (03604-04) Blocked INFECTED (Win.Test.EICAR_HDB-1) {DiscardedInte
rnal,Quarantined}, LOCAL [192.168.1.4]:39736 <fabian@teknova.com> -> <jason96@credobank.com>, quaran
tine: 2/virus-21EXU5sHENfa, Queue-ID: 272CBC038C, Message-ID: <1016855085.114.1628456557755@10.100.0
.14>, mail_id: 21EXU5sHENfa, Hits: -, size: 2289, 200 ms
Aug  8 15:02:32 mail postfix/smtp[6562]: 272CBC038C: to=<jason96@credobank.com>, relay=127.0.0.1[127
.0.0.1]:10024, delay=0.31, delays=0.1/0.01/0/0.2, dsn=2.7.0, status=sent (250 2.7.0 Ok, discarded, i
d=03604-04 - INFECTED: Win.Test.EICAR_HDB-1)
Aug  8 15:02:32 mail postfix/qmgr[1775]: 272CBC038C: removed
Aug  8 15:02:32 mail postfix/lmtp[6569]: 6AC4BC038E: to=<jason96@credobank.com>, relay=127.0.0.1[127
.0.0.1]:2003, delay=0.23, delays=0.01/0.01/0.05/0.16, dsn=2.1.5, status=sent (250 2.1.5 jason96@cred
obank.com Ok)
Aug  8 15:02:32 mail postfix/qmgr[1775]: 6AC4BC038E: removed
root@mail:/home/Administrator# _
```

Figura 75. Log Recepción de Correo KOPANO

Y nuestro antivirus nos envía un correo, notificando que se nos ha intentado enviar un correo con contenido malicioso, así como sus datos Generales.

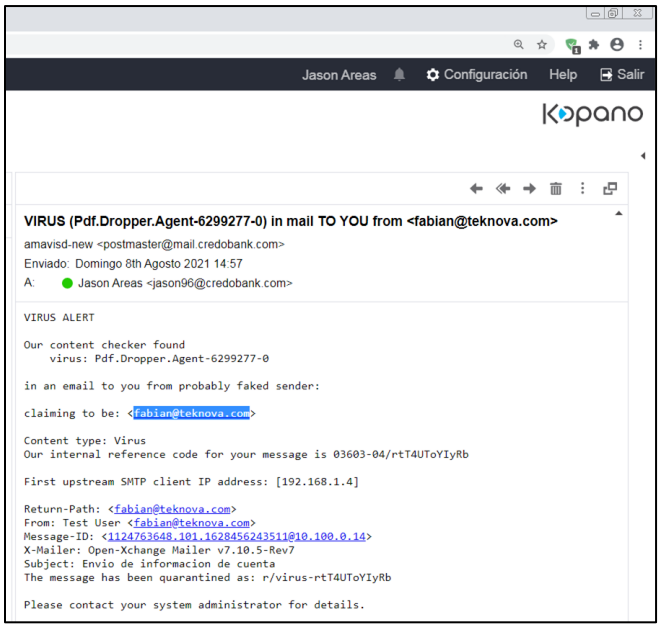

Figura 76. Mensajes de Virus en KOPANO

Nuestro remitente hace de nuevo un envío de correo de Tipo ZIP para intentar vulnerar o burlar nuestro detector de Virus

Lo curioso es que envía un correo de notificación de la detección de un correo malicioso pero esta vez lo envía a la carpeta de SPAM

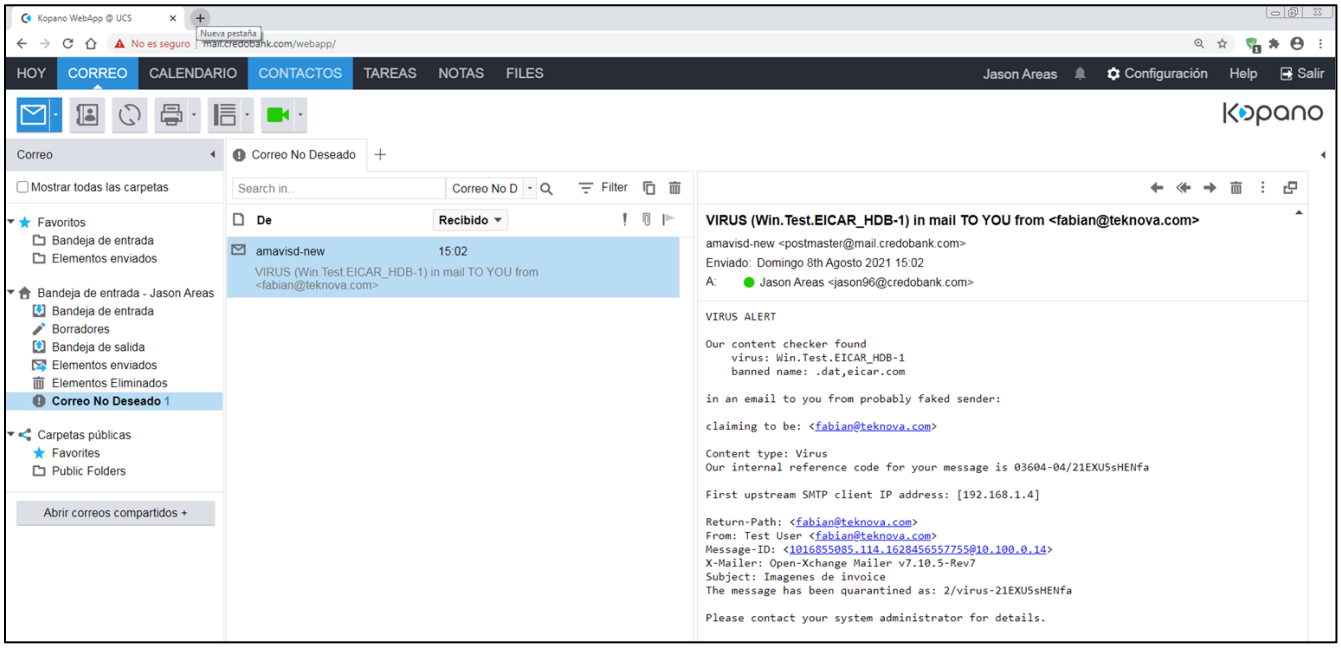

Figura 77. Mensaje de Virus en SPAM en KOPANO

en el último intento nos tratarán enviar un archivo Excel para ver que comportamiento o notificación se presenta

```
Aug  8 15:08:50 mail postfix/qmgr[1775]: 2B76CC038C: from=<fabian@teknova.com>, size=2048, nrcpt=1 (
queue active)
Aug  8 15:08:50 mail postfix/smtpd[6667]: disconnect from unknown[192.168.1.4] ehlo=1 mail=1 rcpt=1
data=1 quit=1 commands=5
Aug  8 15:08:50 mail postfix/smtpd[6675]: connect from localhost[127.0.0.1]
Aug  8 15:08:50 mail postfix/smtpd[6675]: 68F6DC038D: client=localhost[127.0.0.1]
Aug  8 15:08:50 mail postfix/cleanup[6671]: 68F6DC038D: message-id=<VAHfZONwQ2cp3S@mail.credobank.co
m>
Aug  8 15:08:50 mail postfix/smtpd[6675]: disconnect from localhost[127.0.0.1] ehlo=1 mail=1 rcpt=1
data=1 quit=1 commands=5
Aug  8 15:08:50 mail postfix/qmgr[1775]: 68F6DC038D: from=<postmaster@mail.credobank.com>, size=2579
, nrcpt=1 (queue active)
Aug  8 15:08:50 mail postfix/smtpd[6675]: connect from localhost[127.0.0.1]
Aug  8 15:08:50 mail postfix/smtpd[6675]: 6CF59C038E: client=localhost[127.0.0.1]
Aug  8 15:08:50 mail postfix/cleanup[6671]: 6CF59C038E: message-id=<VRHfZONwQ2cp3S@mail.credobank.co
m>
Aug  8 15:08:50 mail postfix/qmgr[1775]: 6CF59C038E: from=<postmaster@mail.credobank.com>, size=1273
, nrcpt=1 (queue active)
Aug  8 15:08:50 mail postfix/smtpd[6675]: disconnect from localhost[127.0.0.1] ehlo=1 mail=1 rcpt=1
ug  8 15:08:50 mail amavis[3603]: (03603-05) Blocked INFECTED (Win.Test.EICAR_HDB-1) {DiscardedInt
nal,Quarantined}, LOCAL [192.168.1.4]:39738 <fabian@teknova.com> -> <jason96@credobank.com>, quara
ine: H/virus-HfZONwQ2cp3S, Queue-ID: 2B76CC038C, Message-ID: <1913691977.127.1628456935532@10.100.
14>, mail_id: HfZONwQ2cp3S, Hits: -, size: 2048, 156 ms
ug  8 15:08:50 mail postfix/smtp[6672]: 2B76CC038C: to=<jason96@credobank.com>, relay=127.0.0.1[12
0.0.1]:10024, delay=0.31, delays=0.14/0.01/0/0.16, dsn=2.7.0, status=sent (250 2.7.0 Ok, discarded
id=03603-05 - INFECTED: Win.Test.EICAR_HDB-1)
ug  8 15:08:50 mail postfix/qmgr[1775]: 2B76CC038C: removed
ug  8 15:08:50 mail postfix/local[6676]: 68F6DC038D: to=<systemmail@mail.credobank.com>, orig_to=<
stmaster@mail.credobank.com>, relay=local, delay=0.05, delays=0.03/0.02/0/0.01, dsn=2.0.0, status=
nt (delivered to mailbox)
ug  8 15:08:50 mail postfix/qmgr[1775]: 68F6DC038D: removed
ug  8 15:08:50 mail postfix/lmtp[6677]: 6CF59C038E: to=<jason96@credobank.com>, relay=127.0.0.1[12
0.0.1]:2003, delay=0.27, delays=0.01/0.01/0.08/0.17, dsn=2.1.5, status=sent (250 2.1.5 jason96@cre
bank.com Ok)
root@mail:/home/Administrator# _
```

Figura 78. Log de Correo infectado en KOPANO

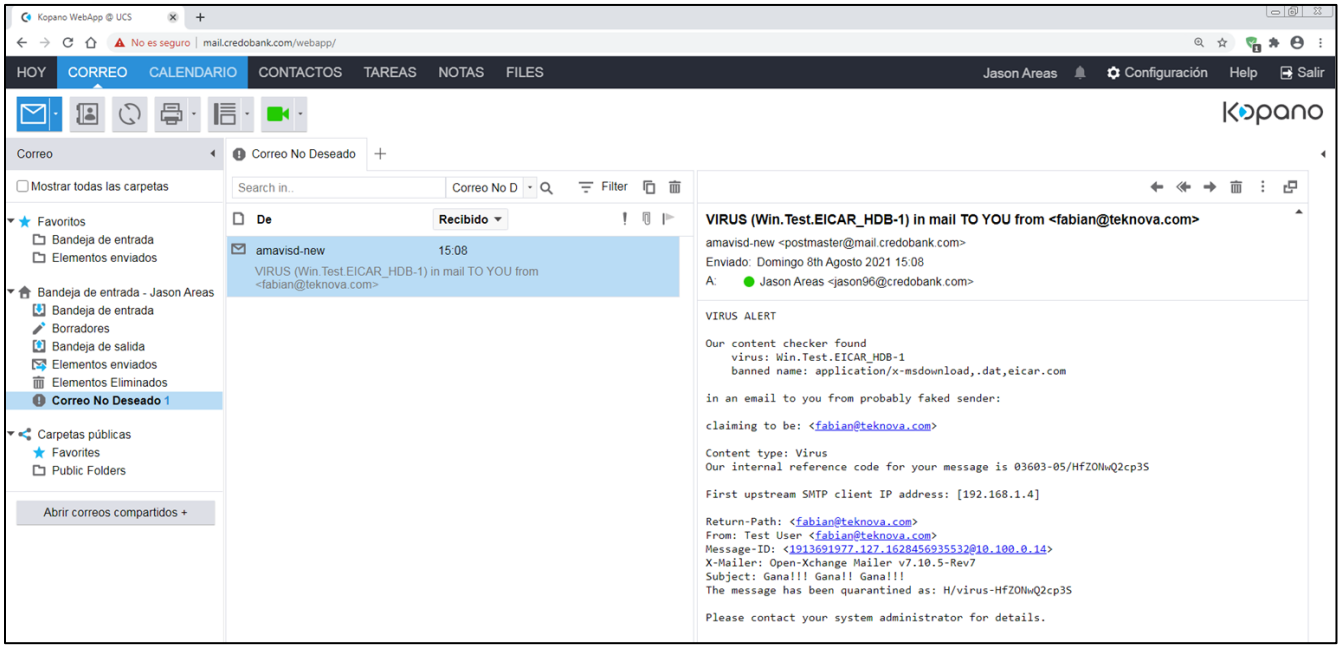

Figura 79. Mensaje de Virus en Correo KOPANO

Estas pruebas se realizaron, asumiendo las diversas formas que algunas personas malas intenciones envían correo malicioso para ocasionar daño o robar información importante por ello nuestras suites de correo deben hacer frente con apoyo de herramientas complementarias para así la recepción y envío de correo sea lo segura posible.

5.4.7. Videollamadas y mensajes.

Una de las virtudes de Kopano es que aparte de tener servicio de Correo Electrónico, podemos realizar chats, llamadas y videollamadas, ya sea a través su sitio especifico o desde la interfaz de correo electrónico.

Como detalle principal es que cada usuario debe poseer sus credenciales de acceso y poseer un navegador web, ya sea Chrome, Opera o Firefox (Internet Explorer no es compatible).

1. Debemos acceder a la IP de nuestro servidor Kopano o su dominio: https://mail.kopano.com/webapp o https://mail.credobank.com/webmeetings/

a través de webapp:

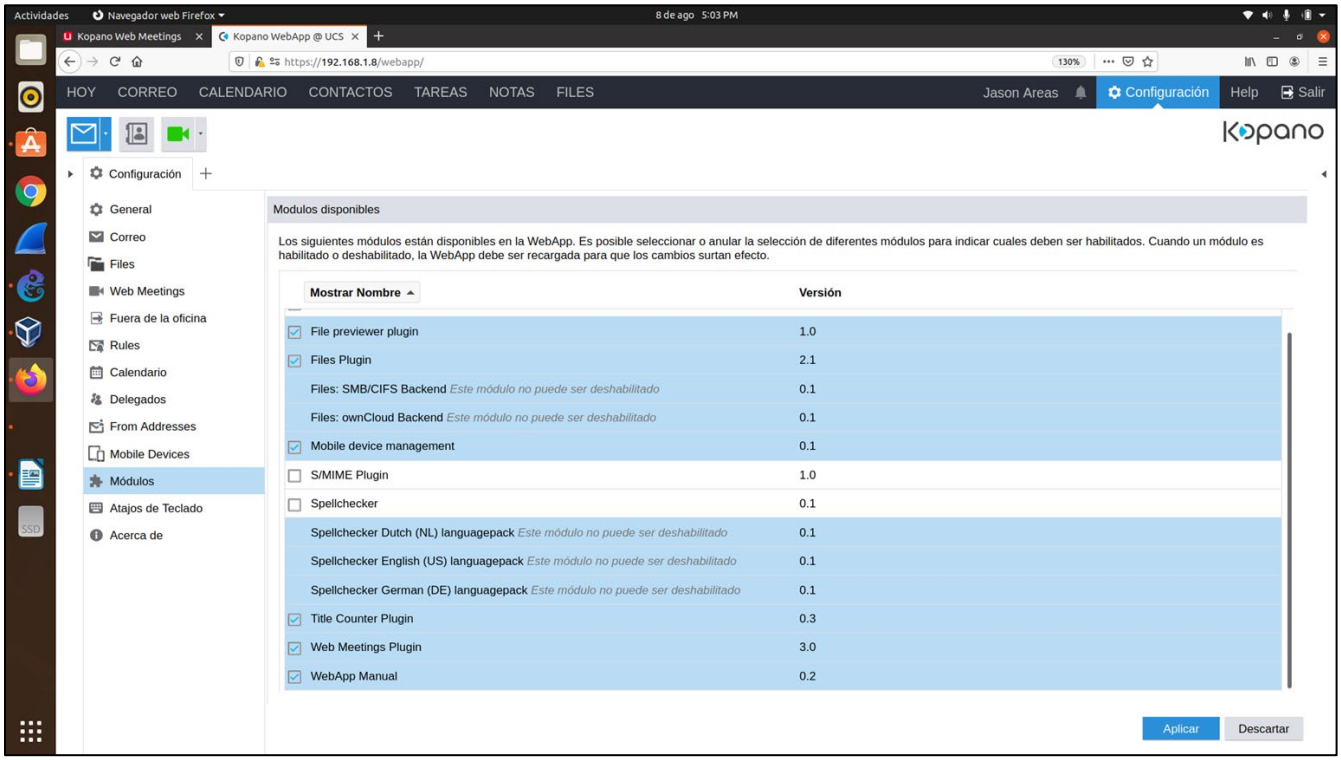

Figura 80. Ajustes para Videollamadas en KOPANO

ingresamos nuestras credenciales en caso el usuario es jason96 y la password: 123

ingresamos a la interfaz con todos nuestros correos y nos dirigimos a la parte de configuraciones y buscamos la sección de Módulos.

Habilitamos la opcion de WebMeetings y clicleamos en aplicar.

Para ellos nos pedirá reiniciar el navegador o recargar la página de nuestra interfaz

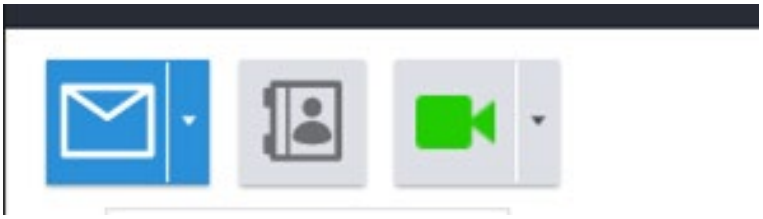

Figura 81. Icono de Videollamadas en KOPANO

Nos aparece el logo de WebMeetings disponible y presiona en ese icono para iniciar una llamada o video llamada.

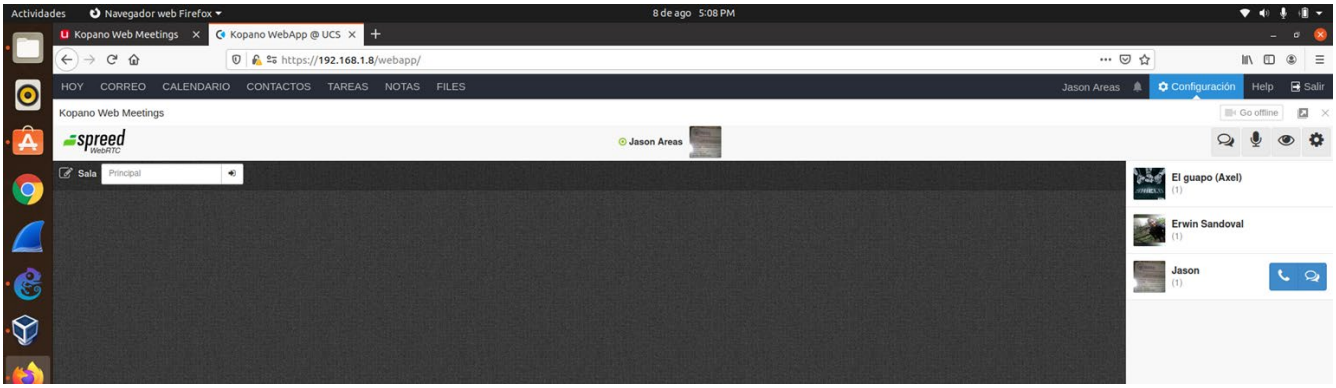

Figura 82. Interfaz de Videollamadas en KOPANO

Tenemos en línea, a dos usuarios más: Axel y Erwin. Iniciaremos una llamada o video llamada.

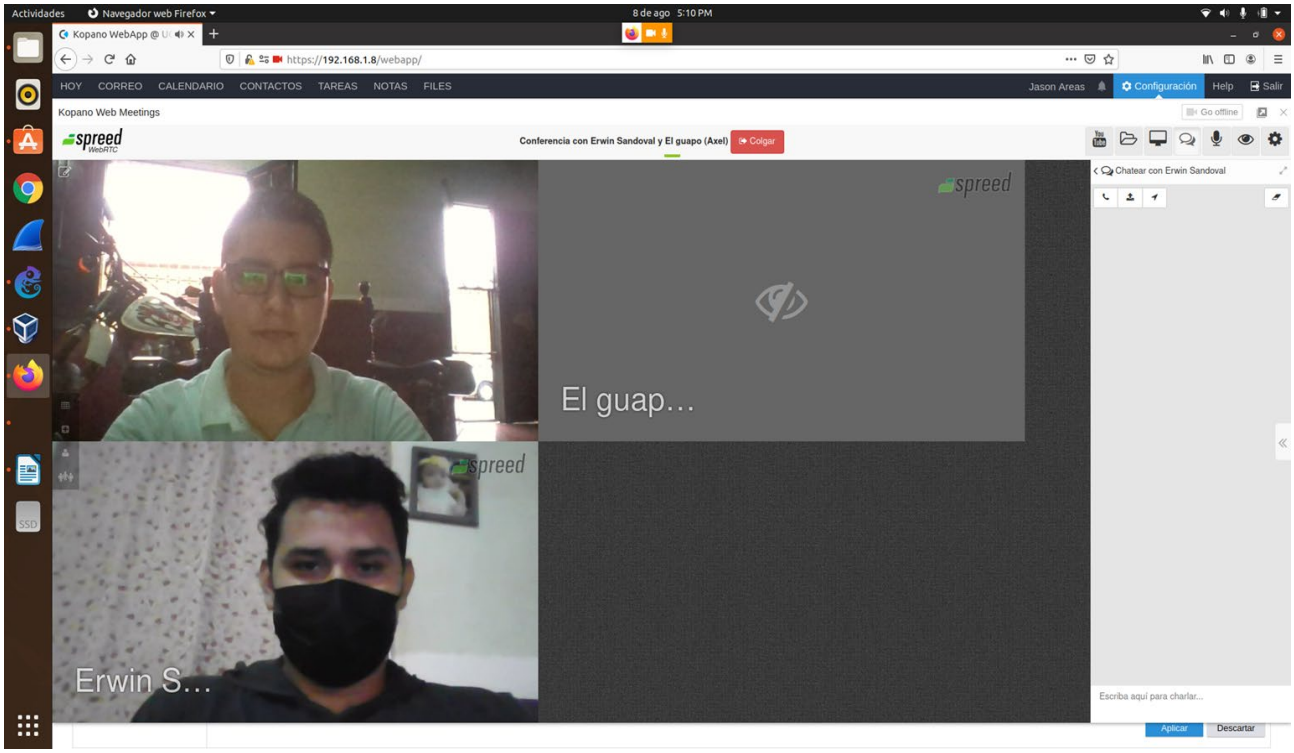

Figura 83. Interfaz de Videollamadas en KOPANO

Nos enviamos mensajes de prueba, incluso tiene una funcionalidad que podemos enviar nuestra ubicación a nuestros amigos del chat.

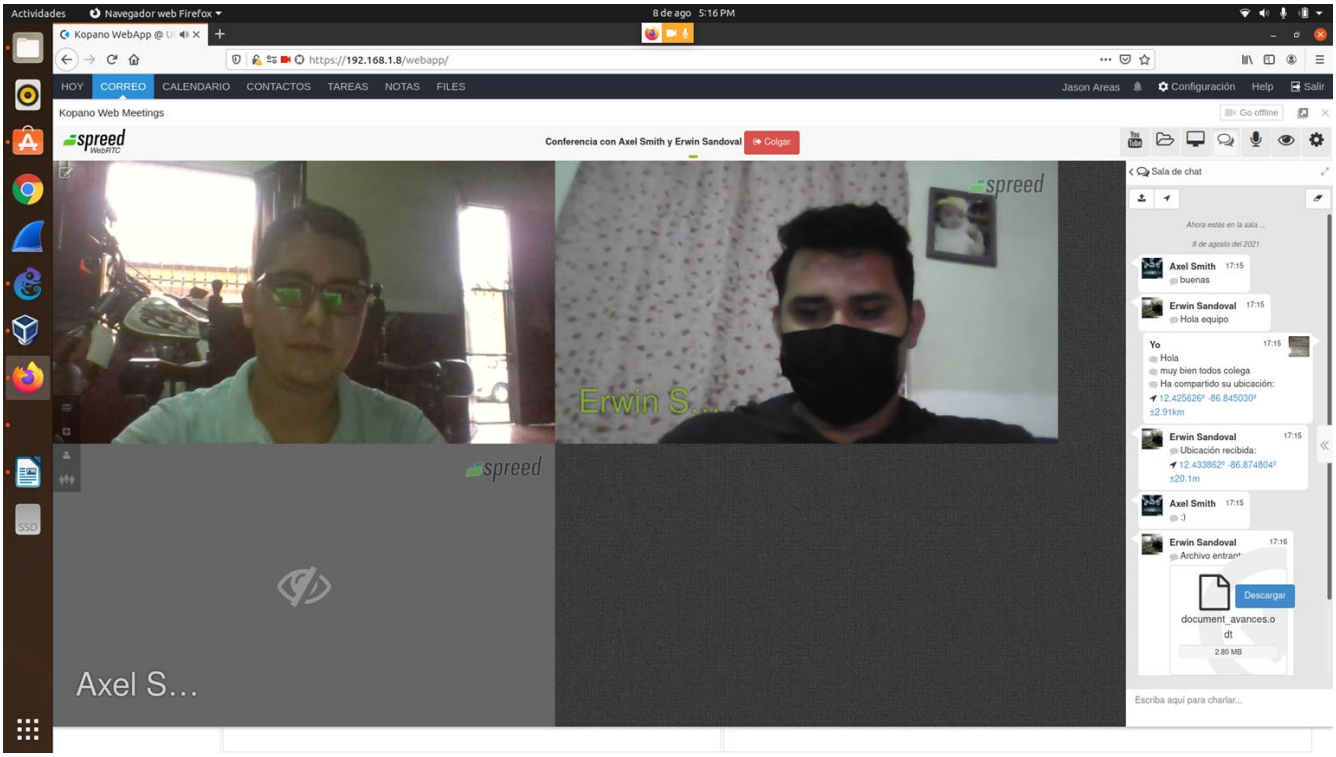

Figura 84. Interfaz de Videollamadas en KOPANO

a través de esta plataforma, podemos hacer una llamada grupal, y compartimos mensajes, archivos, y la ubicación de donde nos encontramos

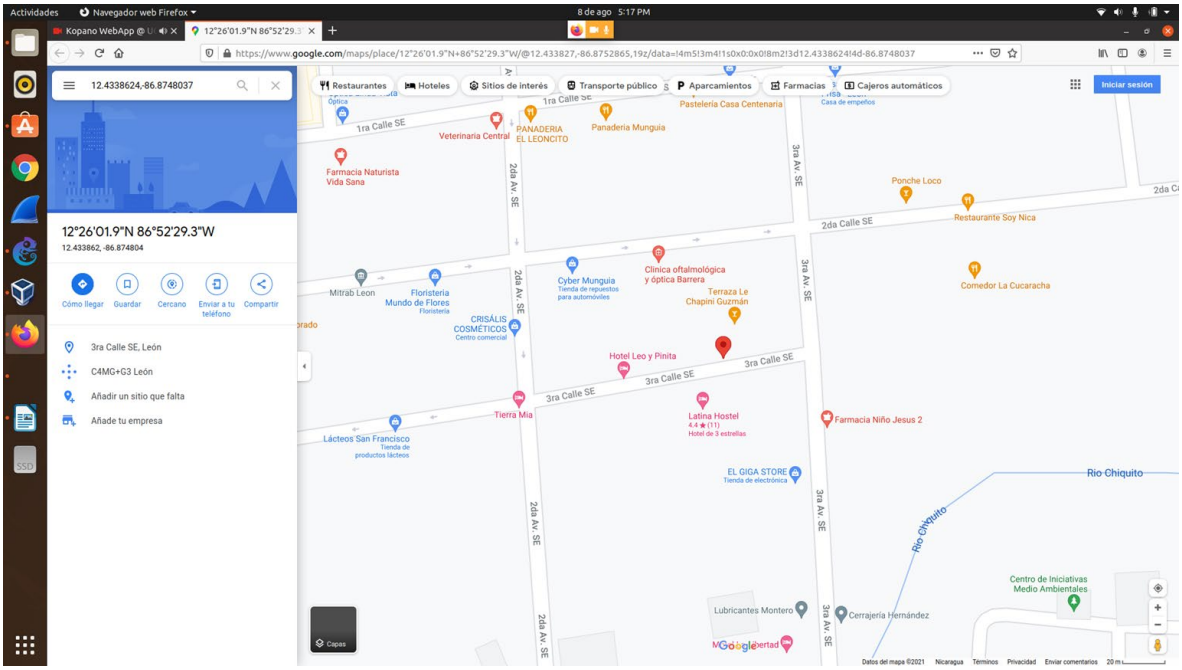

Figura 85. Compartiendo ubicación en Videollamada de KOPANO

Otra funcionalidad muy útil hoy en día para nuestras reuniones es compartir nuestras pantallas con los integrantes del grupo de chat.

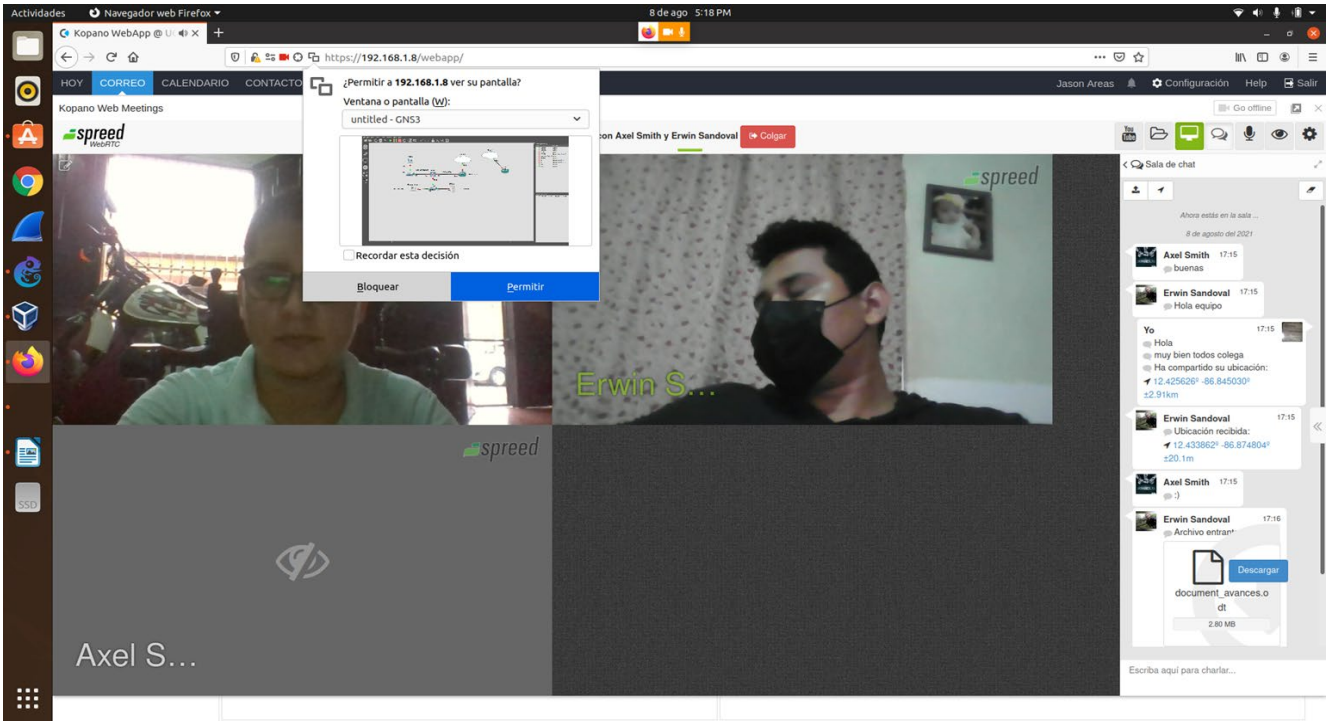

Figura 86. Chat grupal en Videollamada en KOPANO

Incluso si necesitamos mostrar videos de YouTube para brindar alguna demostración de algún video en particular como parte de nuestra reunión, tenemos la opcion de cargar links de YouTube.

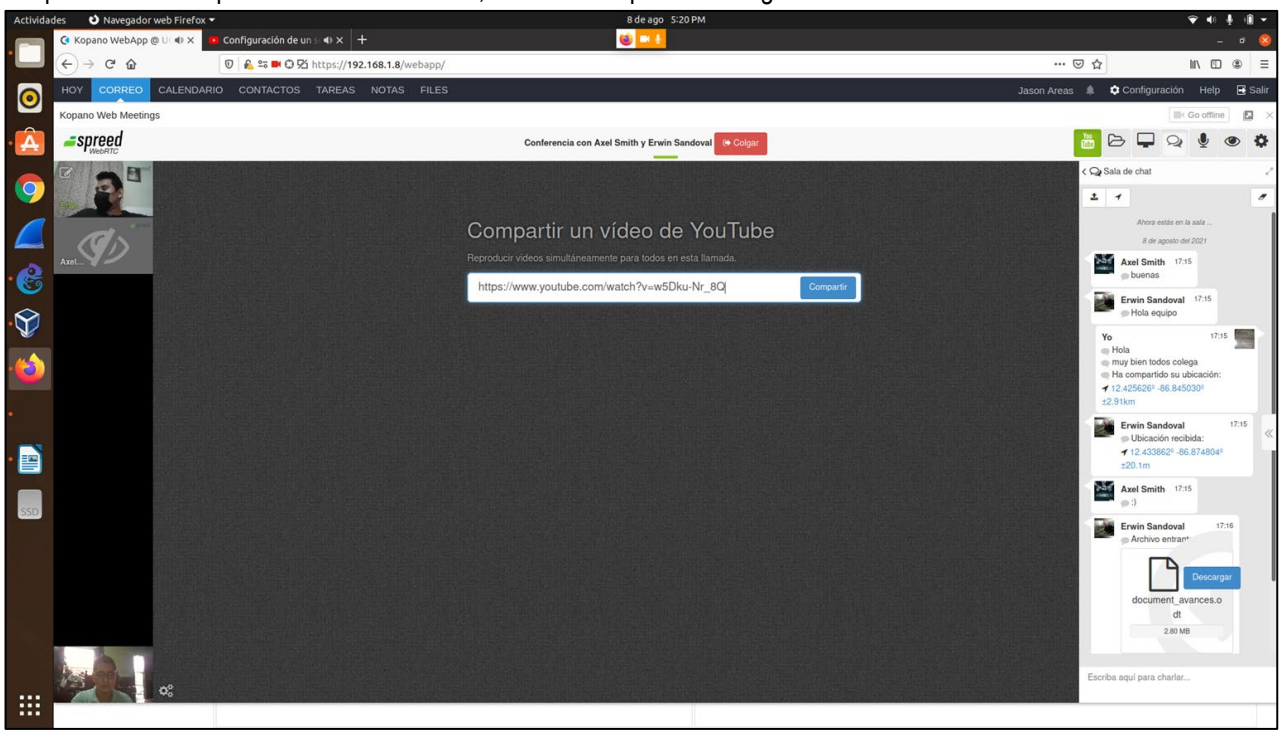

Figura 87. Compartiendo Link YouTube en Videollamada KOPANO

Figura 88. Muestra de Video de YouTube en Videollamada KOPANO

5.5. Pruebas Suite Zimbra

5.5.1. Prueba de envío de correo

Envío de texto plano desde Zimbra a Open-Xchange y Kopano

De: Smith@redone.com A: Jason96@credobank.com Fabian@teknova.com

En la primera prueba hemos enviado un correo de texto plano a las diferentes suites para demostrar su funcionamiento por interfaz y por consola.

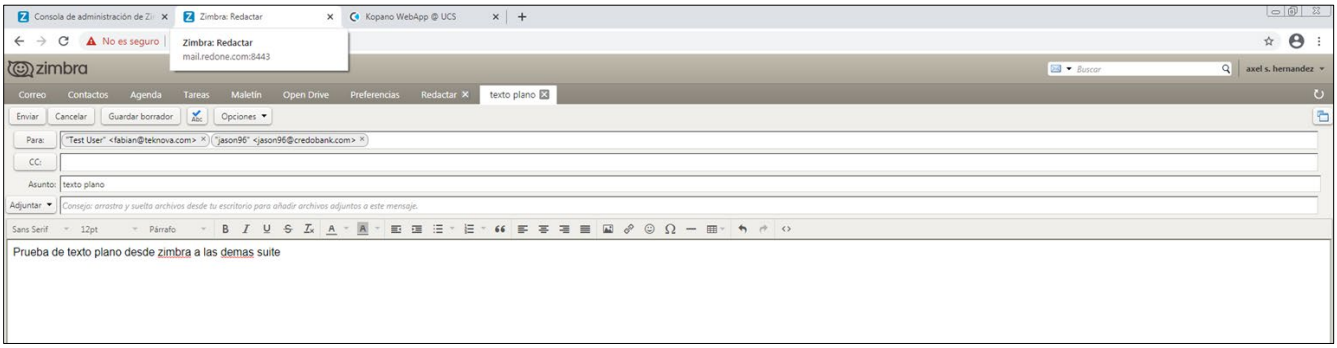

Figura 89. Envío de texto plano desde Zimbra a Open-Xchange y Kopano

En la imagen de arriba mostramos lo fácil y rápido que es crear un correo mediante la interfaz de zimbra.

```
Jul 25 17:28:29 mail postfix/dkimmilter/smtpd[26349]: F24043C3894: client=localhost[127.0.0.1]
Jul 25 17:28:29 mail postfix/cleanup[26345]: F24043C3894: message-id=<401848534.744.1627255708538.Ja
vaMail.zimbra@redone.com>
Jul 25 17:28:29 mail postfix/dkimmilter/smtpd[26349]: disconnect from localhost[127.0.0.1] ehlo=1 ma
il=1 rcpt=2 data=1 quit=1 commands=6
Jul 25 17:28:29 mail postfix/qmgr[5376]: F24043C3894: from=<smith@redone.com>, size=1648, nrcpt=2 (q
ueue active)
Jul 25 17:28:29 mail postfix/smtp[26347]: C9DBD3C379A: to=<jason96@credobank.com>, relay=127.0.0.1[
27.0.0.1]:10026, delay=0.24, delays=0.03/0.03/0/0.18, dsn=2.0.0, status=sent (250 2.0.0 from MTA(sm
p:[127.0.0.1]:10030): 250 2.0.0 Ok: queued as F24043C3894)
Jul 25 17:28:29 mail postfix/smtp[26347]: C9DBD3C379A: to=<fabian@teknova.com>, relay=127.0.0.1[127
0.0.1]:10026, delay=0.24, delays=0.03/0.03/0/0.18, dsn=2.0.0, status=sent (250 2.0.0 from MTA(smtp:
127.0.0.1]:10030): 250 2.0.0 Ok: queued as F24043C3894)
Jul 25 17:28:29 mail postfix/qmgr[5376]: C9DBD3C379A: removed
Jul 25 17:28:39 mail postfix/amavisd/smtpd[26357]: connect from localhost[127.0.0.1]
Jul 25 17:28:39 mail postfix/amavisd/smtpd[26357]: 2726F3C379A: client=localhost[127.0.0.1]
Jul 25 17:28:39 mail postfix/cleanup[26345]: 2726F3C379A: message-id=<401848534.744.1627255708538.J
vaMail.zimbra@redone.com>
Jul 25 17:28:39 mail postfix/qmgr[5376]: 2726F3C379A: from=<smith@redone.com>, size=1947, nrcpt=2 (
ueue active)
Jul 25 17:28:39 mail postfix/amavisd/smtpd[26357]: disconnect from localhost[127.0.0.1] ehlo=1 mail
1 rcpt=2 data=1 quit=1 commands=6
Jul 25 17:28:39 mail postfix/smtp[26351]: F24043C3894: to=<jason96@credobank.com>, relay=127.0.0.1[
27.0.0.1]:10032, delay=10, delays=0.05/0.01/0/10, dsn=2.0.0, status=sent (250 2.0.0 from MTA(smtp:[
27.0.0.1]:10025): 250 2.0.0 Ok: queued as 2726F3C379A)
Jul 25 17:28:39 mail postfix/smtp[26351]: F24043C3894: to=<fabian@teknova.com>, relay=127.0.0.1[127
0.0.1]:10032, delay=10, delays=0.05/0.01/0/10, dsn=2.0.0, status=sent (250 2.0.0 from MTA(smtp:[127
0.0.1]:10025): 250 2.0.0 Ok: queued as 2726F3C379A)
Jul 25 17:28:39 mail postfix/qmgr[5376]: F24043C3894: removed
Jul 25 17:28:40 mail postfix/smtp[26358]: 2726F3C379A: to=<jason96@credobank.com>, relay=smtp.credo
ank.com[192.168.1.9]:25, delay=0.9, delays=0.03/0.01/0.58/0.27, dsn=2.0.0, status=sent (250 2.0.0 O
: queued as C970CC0B3F)
Jul 25 17:28:40 mail postfix/smtp[26359]: 2726F3C379A: to=<fabian@teknova.com>, relay=smtp.teknova.
om[192.168.1.4]:25, delay=0.96, delays=0.03/0.02/0.64/0.26, dsn=2.0.0, status=sent (250 2.0.0 Ok: q
eued as 87CFE73E36B)
Jul 25 17:28:40 mail postfix/qmgr[5376]: 2726F3C379A: removed
root@mail:~#
```

Figura 90. Log Envío de texto plano desde Zimbra a Open-Xchange y Kopano

Como se puede observar hay 6 notificaciones, las 2 primera nos notifica que han sido enviados correctamente, los otros 2 restantes son notificaciones del servidor de correo de Kopano y open-xchange que nos indica que han sido encolados, las ultimas 2 nos indica que los mensajes han sido enviados y recibidos exitosamente por el usuario.

Envío de archivo Zip desde Zimbra a Open-Xchange y Kopano

Se ha realizado una segunda prueba para ver el comportamiento de la suite zimbra, enviando un archivo Zip a las demás instituciones.

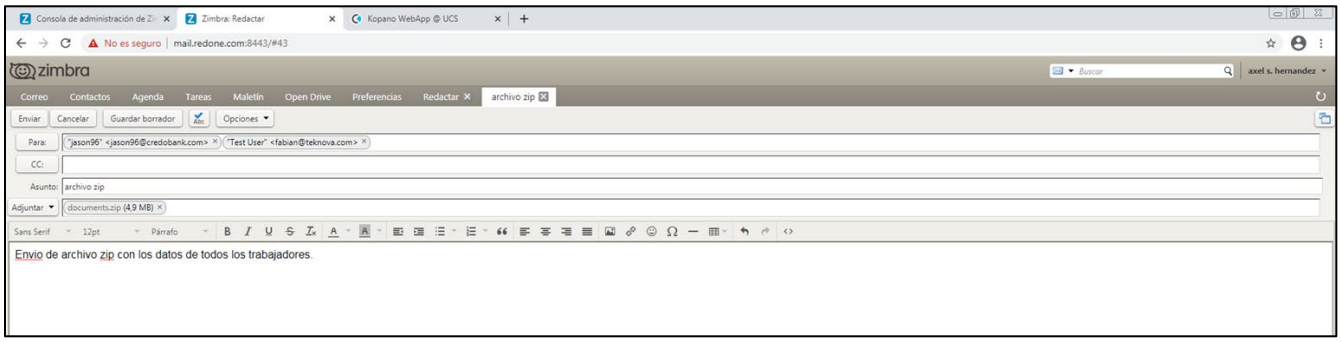

Figura 91. Envío de archivo Zip desde Zimbra a Open-Xchange y Kopano

Como pueden ver hemos cargado un archivo zip de tamaño de (4.9 mb) para realizar nuestra segunda prueba

```
Jul 25 17:35:53 mail postfix/qmgr[5376]: 52B563C3894: removed
Jul 25 17:36:04 mail postfix/amavisd/smtpd[30757]: connect from localhost[127.0.0.1]
Jul 25 17:36:04 mail postfix/amavisd/smtpd[30757]: 6005B3C3905: client=localhost[127.0.0.1]
Jul 25 17:36:04 mail postfix/cleanup[30557]: 6005B3C3905: message-id=<1173502688.812.1627256149660.J
Jul 25 17:36:04 mail postfix/qmgr[5376]: 6005B3C3905: from=<smith@redone.com>, size=6989672, nrcpt=2
 (queue active)
Jul 25 17:36:04 mail postfix/smtp[30562]: 7A7DC3C379A: to=<jason96@credobank.com>, relay=127.0.0.1[1
27.0.0.1]:10032, delay=11, delays=0.31/0.01/0.01/11, dsn=2.0.0, status=sent (250 2.0.0 from MTA(smtp
:[127.0.0.11:10025): 250 2.0.0 Ok: queued as 6005B3C3905)
Jul 25 17:36:04 mail postfix/smtp[30562]: 7A7DC3C379A: to=<fabian@teknova.com>, relay=127.0.0.1[127.
0.0.1]:10032, delay=11, delays=0.31/0.01/0.01/11, dsn=2.0.0, status=sent (250 2.0.0 from MTA(smtp:[1
27.0.0.1]:10025): 250 2.0.0 Ok: queued as 6005B3C3905)
Jul 25 17:36:04 mail postfix/qmgr[5376]: 7A7DC3C379A: removed
Jul 25 17:36:07 mail /postfix-script[30887]: the Postfix mail system is running: PID: 5950
Jul 25 17:36:14 mail /postfix-script[31298]: the Postfix mail system is running: PID: 5950
Jul 25 17:37:20 mail /postfix-script[31735]: the Postfix mail system is running: PID: 5950
Jul 25 17:38:07 mail /postfix-script[32219]: the Postfix mail system is running: PID: 5950
Jul 25 17:38:26 mail /postfix-script[32631]: the Postfix mail system is running: PID: 5950
Jul 25 17:39:31 mail /postfix-script[616]: the Postfix mail system is running: PID: 5950
Jul 25 17:40:21 mail /postfix-script[1277]: the Postfix mail system is running: PID: 5950
Jul 25 17:40:40 mail /postfix-script[1692]: the Postfix mail system is running: PID: 5950
Jul 25 17:41:04 mail postfix/amavisd/smtpd[30757]: timeout after END-OF-MESSAGE from localhost[127.0
.0.1]
Jul 25 17:41:04 mail postfix/amavisd/smtpd[30757]: disconnect from localhost[127.0.0.1] ehlo=1 mail=
1 rcpt=2 data=1 commands=5
Jul 25 17:41:46 mail /postfix-script[2128]: the Postfix mail system is running: PID: 5950
Jul 25 17:42:09 mail /postfix-script[2608]: the Postfix mail system is running: PID: 5950
Jul 25 17:42:52 mail /postfix-script[3076]: the Postfix mail system is running: PID: 5950
Jul 25 17:43:06 mail postfix/smtp[30759]: 6005B3C3905: to=<fabian@teknova.com>, relay=smtp.teknova.c
om[192.168.1.4]:25, delay=422, delays=0.31/0.03/1.1/420, dsn=2.0.0, status=sent (250 2.0.0 Ok: queue
d as 8C43B73E36B)
Jul 25 17:43:17 mail postfix/smtp[30758]: 6005B3C3905: to=<jason96@credobank.com>, relay=smtp.credob
ank.com[192.168.1.9]:25, delay=433, delays=0.31/0.02/1.1/432, dsn=2.0.0, status=sent (250 2.0.0 Ok:
queued as CF72FC0B3F)
Jul 25 17:43:17 mail postfix/qmgr[5376]: 6005B3C3905: removed
root@mail:~#
```

Figura 92. Log Envío de archivo Zip desde Zimbra a Open-Xchange y Kopano

Como se puede observar hay 4 notificaciones 2 de ellas nos muestra que el mensaje se envió correctamente y las otras 2 notificaciones que son de Kopano y open-Xchange, que nos indica que están siendo atendidas por dichos servidores, lo cual esas notificaciones nos brindara una pequeña información donde, nos muestra los usuarios a quienes le queremos mandar un correo, muestra un status que nos indica que el mensaje ha sido enviado exitosamente, también nos muestra un delay que es el tiempo de retardo.

5.5.2. Prueba de envió de archivos

Envió de archivo Excel desde Zimbra a Open-Xchange y Kopano

Se ha realizado una prueba para ver el comportamiento de la suite zimbra, enviando un archivo Excel a las demás instituciones

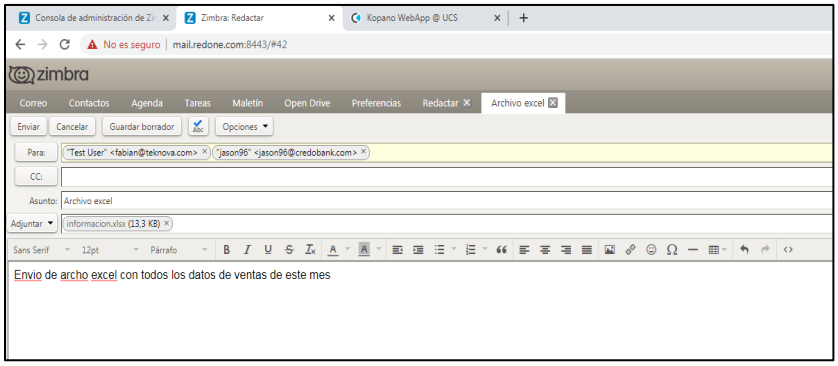

Figura 93. Envió de archivo Excel desde Zimbra a Open-Xchange y Kopano

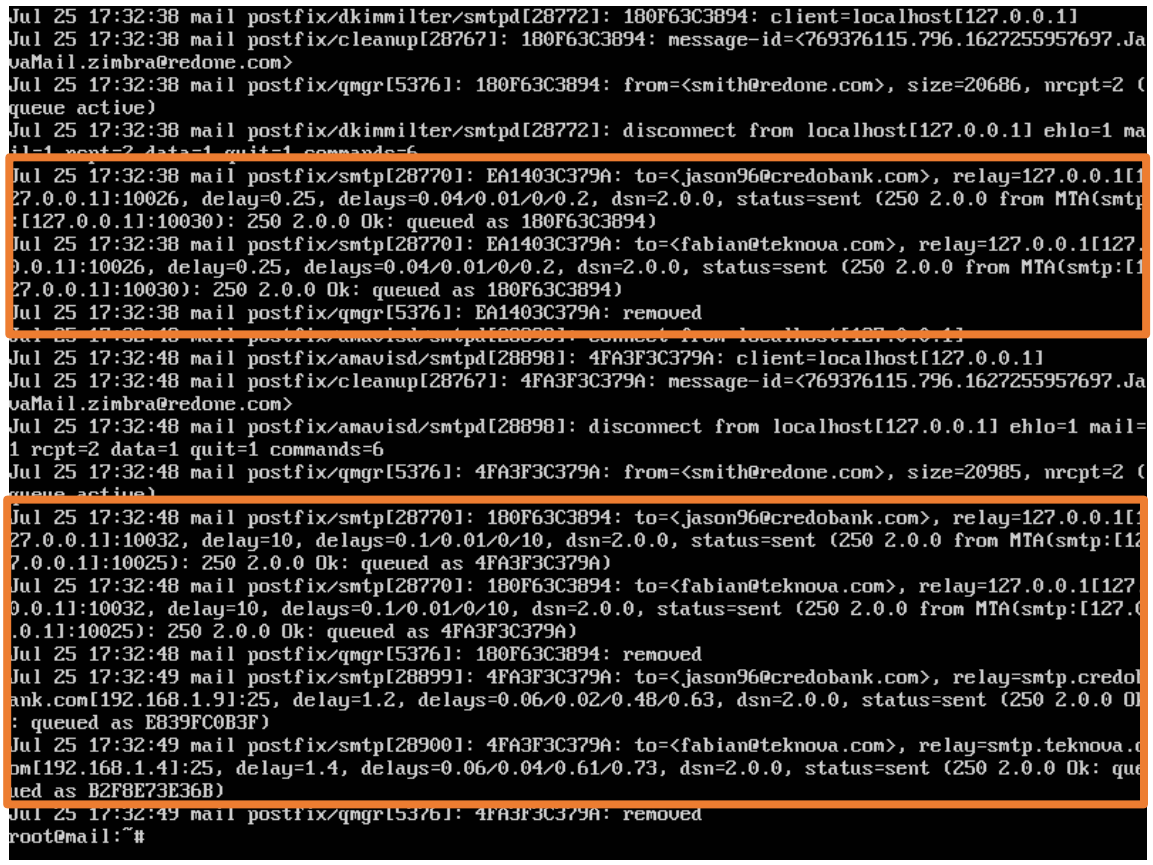

Figura 94. Log Envió de archivo Excel desde Zimbra a Open-Xchange y Kopano

Como podemos observar cuando se envía un correo de menor tamaño es mucho más rápido lo cual el destinatario recibe los mensajes casi instantánea, se muestran 6 notificaciones 2 nos indican de que dirección de correo se están enviando los archivos, el tamaño del mensaje y que está en cola activa y 2 notificaciones que nos indica a quienes se los estamos enviando, además que nos muestra que los correos están siendo analizados y encolados y las 2 últimas que los mensajes ya fueron recibidos con éxito.

5.5.3. Prueba de spam

Se ha realizado una prueba para ver el comportamiento de la suite zimbra, configurando y creando reglas antispam con palabras claves para identificar los mensajes entrantes.

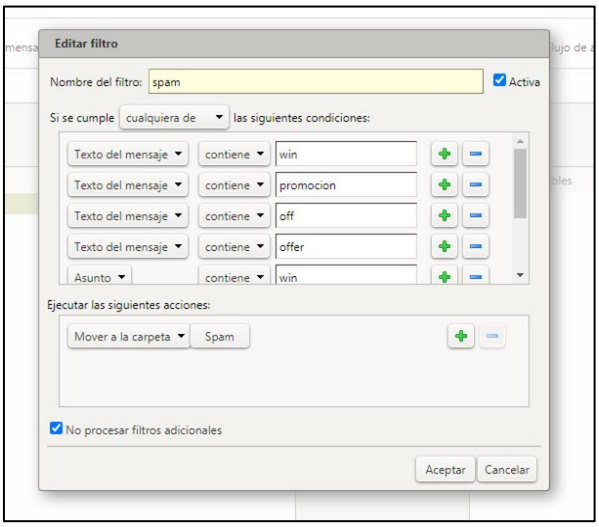

Figura 95. Ajustes SPAM

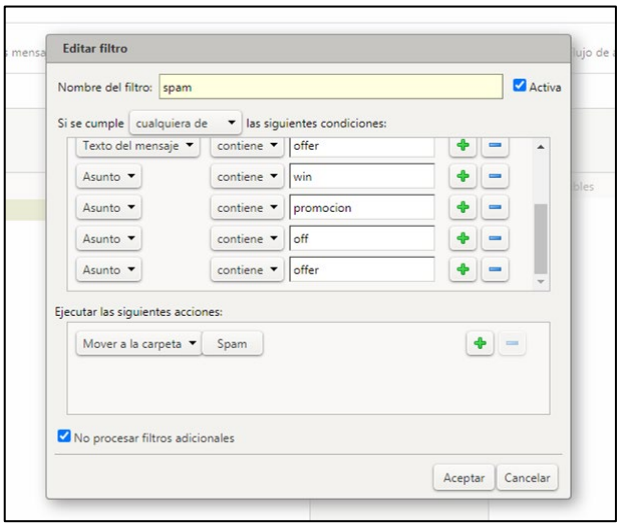

Figura 96. Ajustes SPAM

Como se puede observar se han creado palabras claves que nos ayudaran a identificar mensajes como spam, hemos creado un filtro con condiciones que se deben cumplir para identificar mensajes con spam si algunas de las condiciones que hemos creado se cumple el mensaje puede ser descartado o movido directamente a la carpeta que le hemos indicado en la regla ya se a la papelera o a la carpeta de spam.

Mensaje detectado como spam

cómo podemos ver Zimbra ha detectado un mensaje de spam, que se envió desde la suite (open-Xchange) teknova.com, lo cual lo ha identificado, analizado y enviado a la carpeta spam como el filtro y regla lo indica.

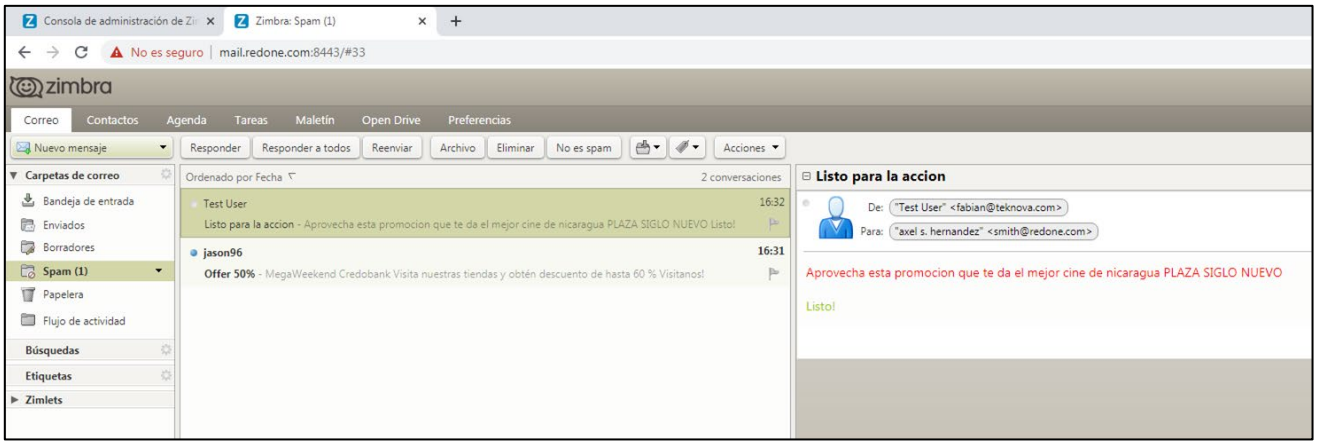

Figura 97. Bandeja de SPAM Zimbra

Mensaje detectado como spam

Igual mente zimbra ha detectado otro mensaje como spam, la suite que ha enviado el mensaje spam es Kopano y ha sido analizado e identificado como spam lo cual la regla también se cumple y es enviado a la carpeta spam directamente.

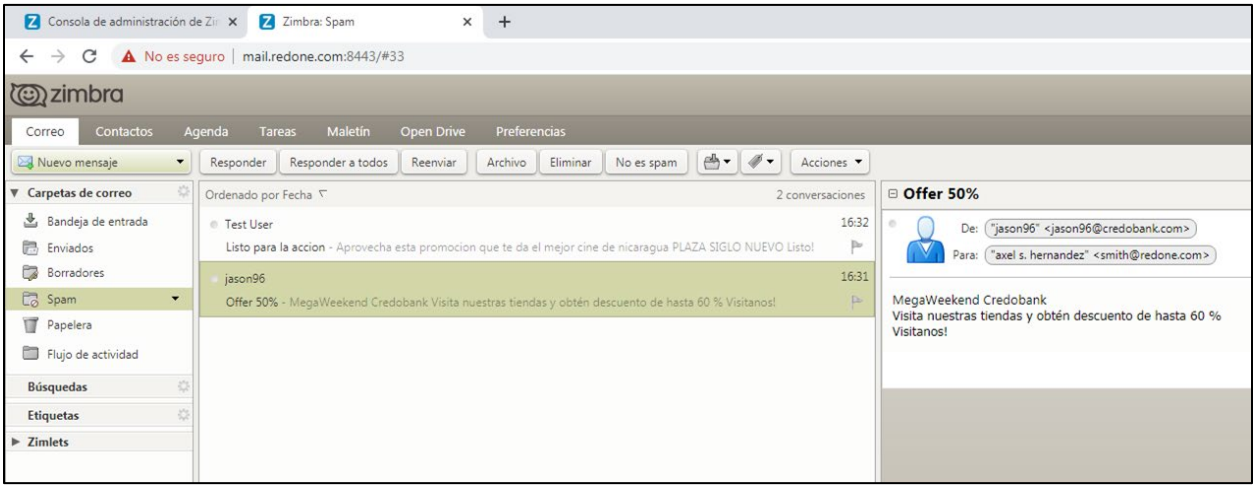

Figura 98. Bandeja de SPAM Zimbra

5.5.4. Prueba de spam de tamaño mayor de 3 mb

Se ha realizado una segunda prueba para ver el comportamiento de la suite zimbra, creando reglas antispam con un filtro de tamaño mínimo de 3mb si la regla se no se cumple el mensaje será descartado a la carpeta spam.

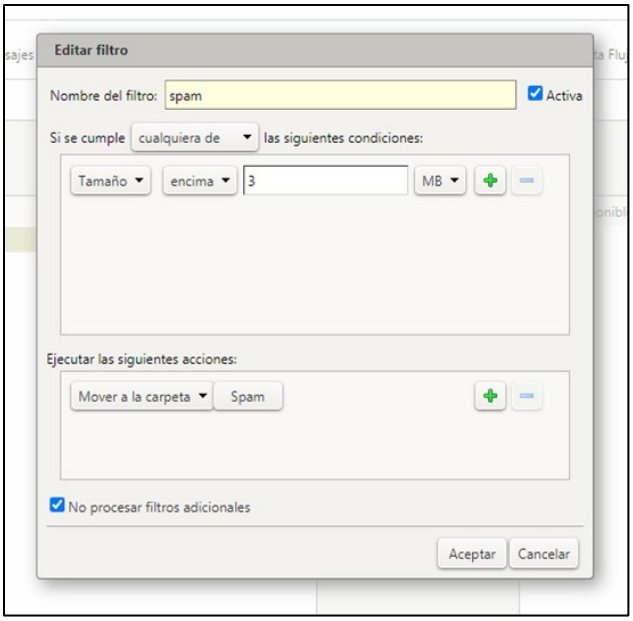

Figura 99. Ajuste SPAM de tamaño mayor de 3 mb

Para esta prueba la regla de spam por tamaño es simple ya que solo necesitamos una sola regla, si quieres ingresar otra regla necesitas eliminar la que se está ejecutando para no tener inconvenientes.

El filtro funciona de la siguiente manera si una suite envía un correo mayor de 3 megas lo descarta y lo identifica como spam.

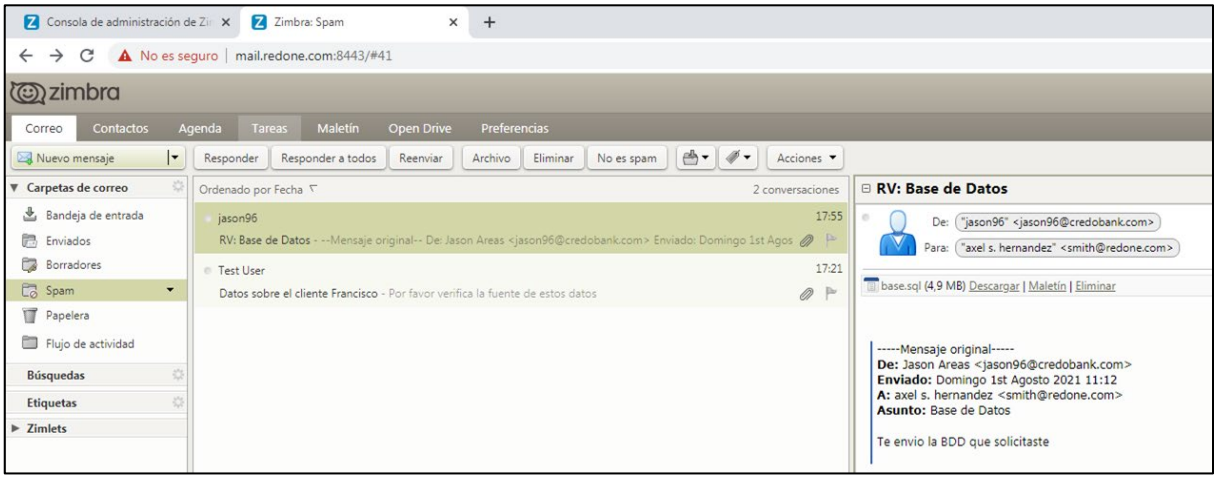

Figura 100. Bandeja de SPAM Zimbra

Hemos recibido un archivo desde la suite Kopano que sobrepasa el tamaño indicado de regla establecida en la configuración por lo que el correo será descartado directamente a la carpeta de spam.

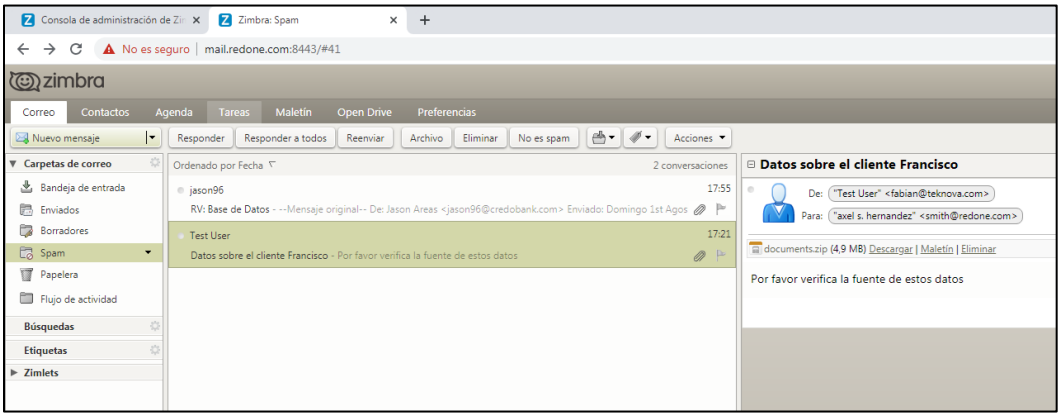

Figura 101. Bandeja de SPAM Zimbra

También se ha recibido otro archivo desde la suite Open-Xchange que sobrepasa el tamaño lo cual vemos que la regla de zimbra está funcionando como corresponde.

Prueba de hipervínculo zimbra

Se ha realizado una tercera prueba para ver el comportamiento de la suite zimbra, creando reglas antispam con un filtro de hipervínculo si la regla se no se cumple el mensaje será descartado a la carpeta spam.

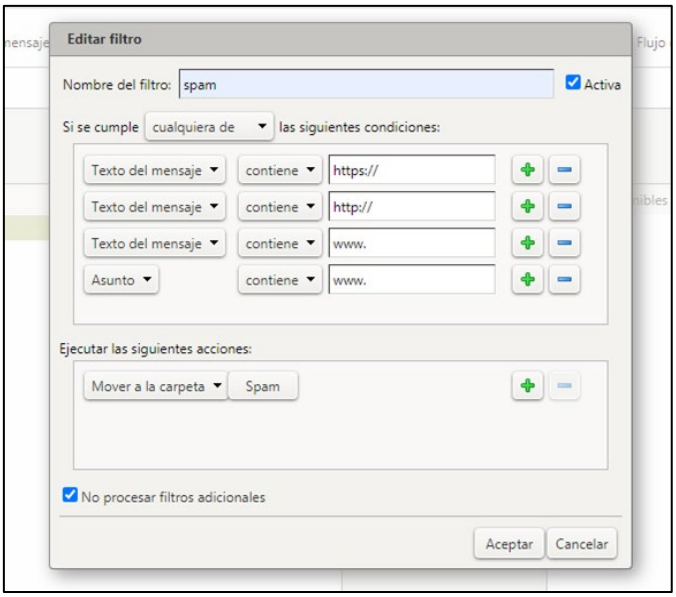

Figura 102. Ajuste hipervínculo Zimbra para SPAM

En la configuración realizada para crear un filtro de hipervínculo, solo es necesario bloquear los protocolos necesarios https, http, www (Protocolo de transferencia de hipertexto) protocolo de comunicación de Internet, si la regla se cumple y el mensaje recibido contiene un hipervínculo a una página web será descartado como spam.

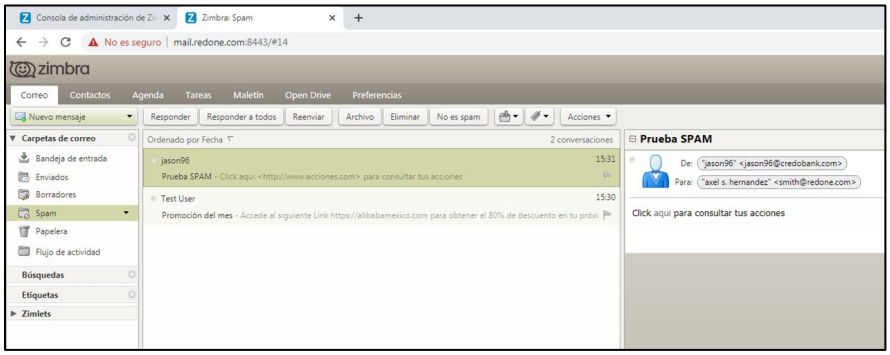

Figura 103. Ajuste hipervínculo Zimbra para SPAM

Se ha enviado un mensaje desde Kopano y Open-Xchange para hacer las pruebas de hipervínculo, para percatarnos que la regla funciona correctamente, se ha recibido un mensaje que contiene un hipervínculo dentro de una palabra, por lo cual Amavis que es nuestro servidor de antispam analizo correctamente el mensaje y ejecuto la regla anteriormente configurada y traslado el mensaje directamente a la carpeta spam

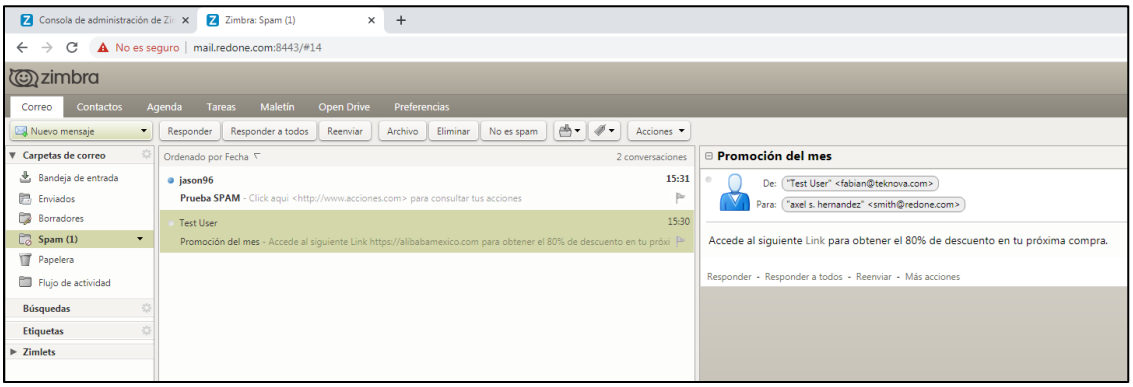

Figura 104. Bandeja SPAM en Zimbra

5.5.5. Prueba de antivirus dentro la suite zimbra

AS/AV (AntiSpam, Antivirus)

Zimbra viene configurado por defecto con Amavis; si lo mantenemos como filtro de contenido, ajustamos los valores de AntiSpam; en donde mientras mayor sea el Score es más probable que sea Spam.

Valores por defecto Porcentaje eliminado: 75 (75 x 0.2 = 15.0) Porcentaje etiquetado: 33 (33 x 0.2 = 6.6) Valores recomendados Porcentaje eliminado: 35 (35 x 0.2 = 7.0) ---> Los correos con score >= 7.0 no llegarán al usuario porque son muy alto Porcentaje etiquetado: 18 (18 x 0.2 = 3.6) ---> Los correos con score >= 3.6 llegarán a la carpeta Spam del usuario

Nota: Si instalamos MailScanner y MailWatch estos valores ya no tendrán efecto. Lo cual el admin tiene la decisión si usar el default u otros de los mencionados.

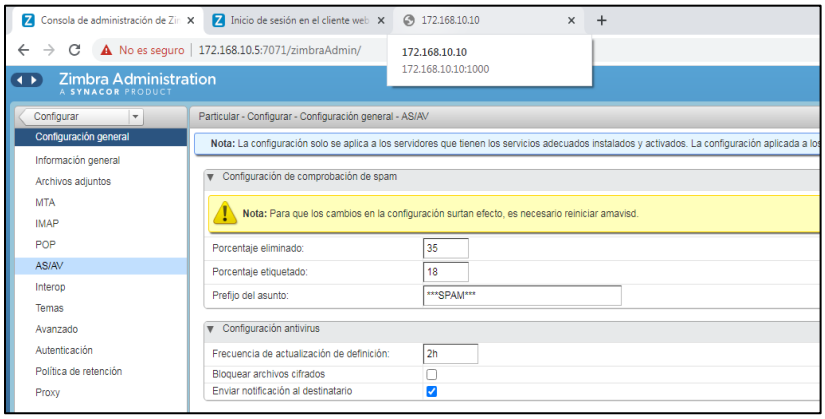

Figura 105. Ajuste Antivirus Zimbra

Menú Administrar

Cuentas y Recursos son buzones de correo (1 licencia por buzón en el Network Edition) Alias y

Listas de correo son alias

Crear cuentas

Click en la rueda y Nuevo

Nombre de Cuenta: javi@redobe.com Nombre: javi Apellido: caballero Nombre Común:

dejar en auto

Estado: Activo Clase de Servicio: por defecto es default

Contraseña: 123456789. (por seguridad habilitar fortaleza de contraseña en el COS) Longitud 8, 1

número, una mayúscula, un signo de puntuación

Finalizar

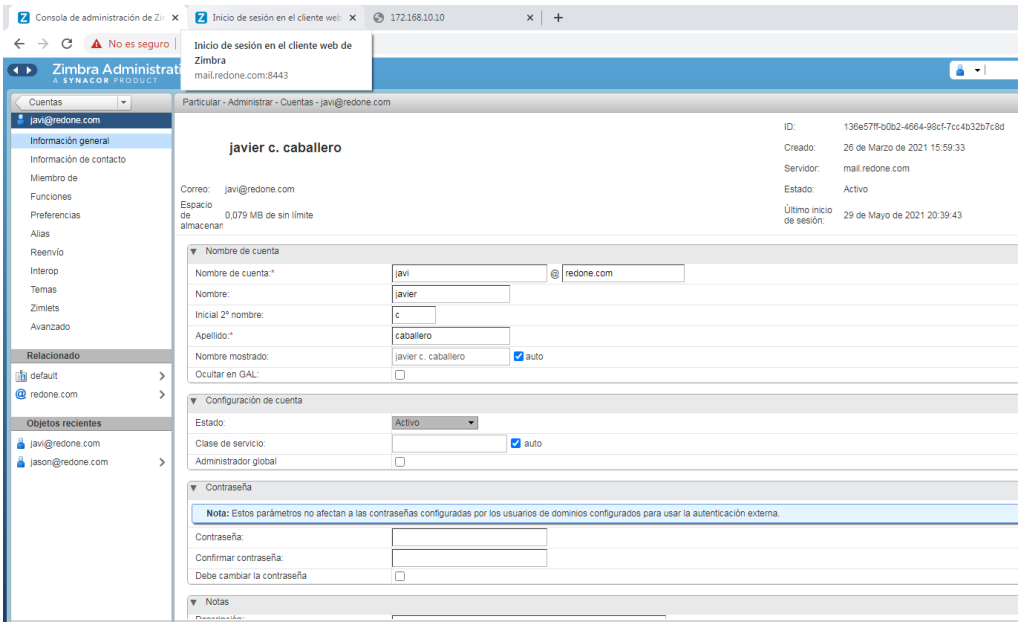

Figura 106. Ajuste Antivirus Zimbra

Para comenzar se realizarán 2 pruebas una de envío y recepción de virus, lo primero será enviar correos con virus a los diferentes usuarios para ver cómo se comporta el servidor de antivirus (ClamAV (antivirus), así mismo veremos la información que nos muestran los logs.

Envió de virus dentro un archivo zip

Se les ha enviado un correo malicioso a unos de nuestros usuarios dentro de la institución redone.com

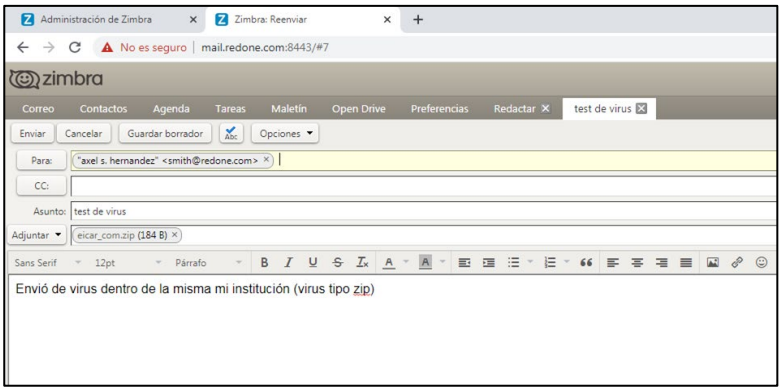

Figura 107. Envío de Virus en Archivo .ZIP en Zimbra

Como se puede observar las notificaciones de los logs, nos muestra que un mensaje enviado por el usuario smith@redone.com no pudo salir del servidor ya que fue analizado por (ClamAV antivirus) y lo descarto como correo malicioso lo cual lo ha metido directamente a cuarentena, luego de ello el servidor de zimbra envía una notificación al usuario que iba a recibir dicho virus alertando de que el usuario smith@redone.com le envió un archivo malicioso. Como puede observar en la imagen nos muestra toda la información de dicho correo y también información que (ClamAV antivirus) recopilo del usuario que ha enviado dicho correo malicioso

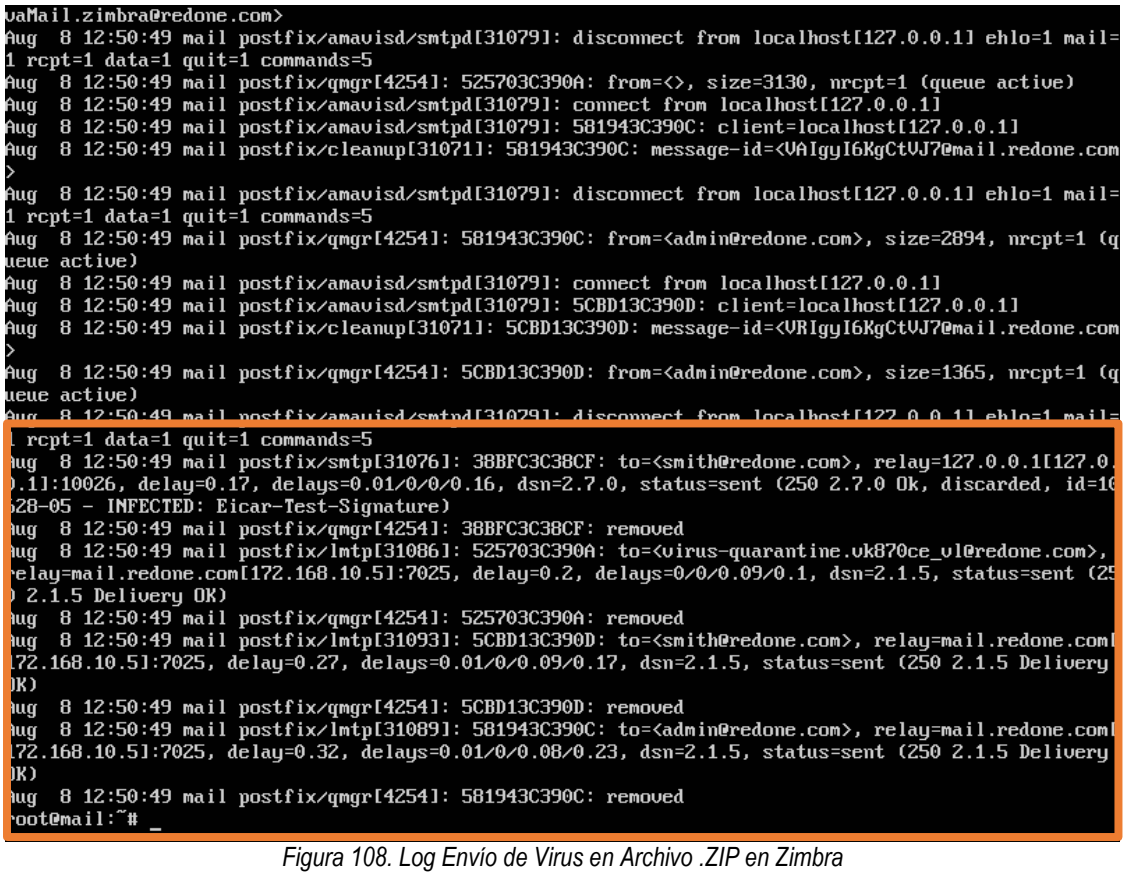

Figura 108. Log Envío de Virus en Archivo .ZIP en Zimbra

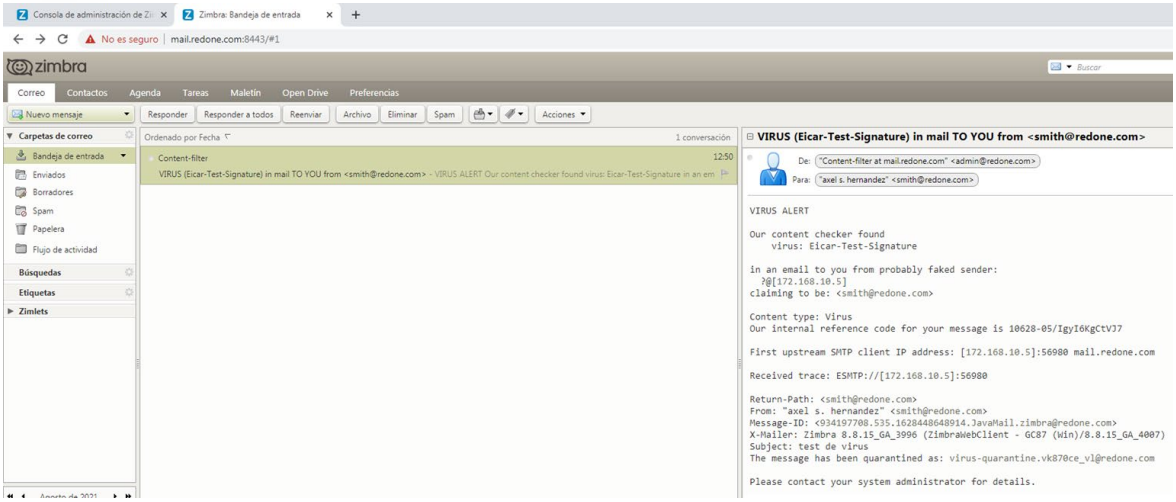

Figura 109. Alerta de Virus en Zimbra

5.5.6. Envío de virus dentro la institución redone.com suite zimbra

Se ha enviado otro tipo de archivo malicioso al usuario smith@redone.com en este caso hemos insertado un virus dentro un pdf, de esta forma estaremos probando si (ClamAV antivirus) puede detectar dicha amenaza.

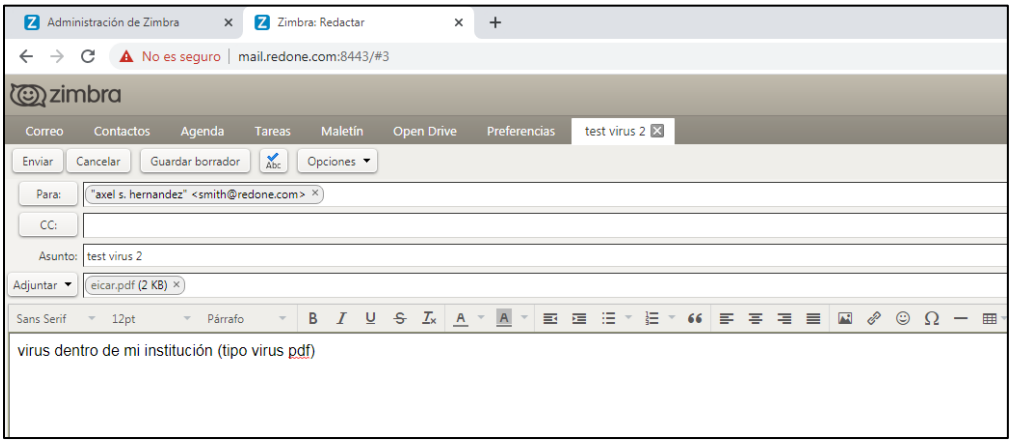

Figura 110. Envío de Virus en Archivo PDF en Zimbra

A continuación, tenemos los logs correspondientes al mensaje enviado como podemos ver las notificaciones nos indica que el mensaje no se pudo enviar y fue analizado por (ClamAV antivirus) y está en estado de cuarentena, donde nos indica el tipo de virus fue enviado el destino y quien lo ha enviado.

Por último, nos muestra que se le ha enviado un correo al usuario

```
Aug  8 12:49:30 mail postfix/amavisd/smtpd[31079]: disconnect from localhost[127.0.0.1] ehlo=1 mail=
1 rcpt=1 data=1 quit=1 commands=5
Aug  8 12:49:30 mail postfix/qmgr[4254]: 3F4913C390A: from=<>, size=5596, nrcpt=1 (queue active)
Aug  8 12:49:30 mail postfix/amavisd/smtpd[31079]: connect from localhost[127.0.0.1]
Aug  8 12:49:30 mail postfix/amavisd/smtpd[31079]: 4D6643C390C: client=localhost[127.0.0.1]
Aug  8 12:49:30 mail postfix/cleanup[31071]: 4D6643C390C: message-id=<VADxjjUyEhY0IR@mail.redone.com
>
Aug  8 12:49:30 mail postfix/amavisd/smtpd[31079]: disconnect from localhost[127.0.0.1] ehlo=1 mail=
1 rcpt=1 data=1 quit=1 commands=5
Aug  8 12:49:30 mail postfix/qmgr[4254]: 4D6643C390C: from=<admin@redone.com>, size=2902, nrcpt=1 (q
ueue active)
Aug  8 12:49:30 mail postfix/amavisd/smtpd[31079]: connect from localhost[127.0.0.1]
Aug  8 12:49:30 mail postfix/amavisd/smtpd[31079]: 5ACE33C390D: client=localhost[127.0.0.1]
Aug  8 12:49:30 mail postfix/cleanup[31071]: 5ACE33C390D: message-id=<VRDxjjUyEhY0IR@mail.redone.com
>
Aug  8 12:49:30 mail postfix/qmgr[4254]: 5ACE33C390D: from=<admin@redone.com>, size=1396, nrcpt=1 (q
ueue active)
Aug  8 12:49:30 mail postfix/amavisd/smtpd[31079]: disconnect from localhost[127.0.0.1] ehlo=1 mail=
1 rcpt=1 data=1 quit=1 commands=5
Aug  8 12:49:30 mail postfix/smtp[31076]: 0E0A63C38CF: to=<smith@redone.com>, relay=127.0.0.1[127.0.
0.1]:10026, delay=0.36, delays=0.02/0.02/0/0.32, dsn=2.7.0, status=sent (250 2.7.0 Ok, discarded, id
=10621-04 - INFECTED: Heuristics.PDF.ObfuscatedNameObject)
Aug  8 12:49:30 mail postfix/qmgr[4254]: 0E0A63C38CF: removed
Aug  8 12:49:30 mail postfix/lmtp[31086]: 3F4913C390A: to=<virus-quarantine.vk870ce_vl@redone.com>,
relay=mail.redone.com[172.168.10.5]:7025, delay=0.29, delays=0.02/0.04/0.1/0.13, dsn=2.1.5, status=s
ent (250 2.1.5 Delivery OK)
Aug  8 12:49:30 mail postfix/qmgr[4254]: 3F4913C390A: removed
Aug  8 12:49:30 mail postfix/lmtp[31089]: 4D6643C390C: to=<admin@redone.com>, relay=mail.redone.com[
172.168.10.5]:7025, delay=0.24, delays=0.02/0.04/0.09/0.09, dsn=2.1.5, status=sent (250 2.1.5 Delive
ry OK)
Aug  8 12:49:30 mail postfix/qmgr[4254]: 4D6643C390C: removed
Aug  8 12:49:30 mail postfix/lmtp[31093]: 5ACE33C390D: to=<smith@redone.com>, relay=mail.redone.com[
172.168.10.5]:7025, delay=0.22, delays=0.01/0.03/0.09/0.1, dsn=2.1.5, status=sent (250 2.1.5 Deliver
y OK)
Aug  8 12:49:30 mail postfix/qmgr[4254]: 5ACE33C390D: removed
Aug  8 12:49:31 mail /postfix-script[31186]: the Postfix mail system is running: PID: 4252
root@mail:~# _
```

Figura 111. Log Envío de Virus en Archivo PDF en Zimbra

Como nos muestra la imagen a continuación, el administrador nos manda una notificación con información recopilada por (ClamAV antivirus) donde nos muestra la procedencia, así como la información del emisor.

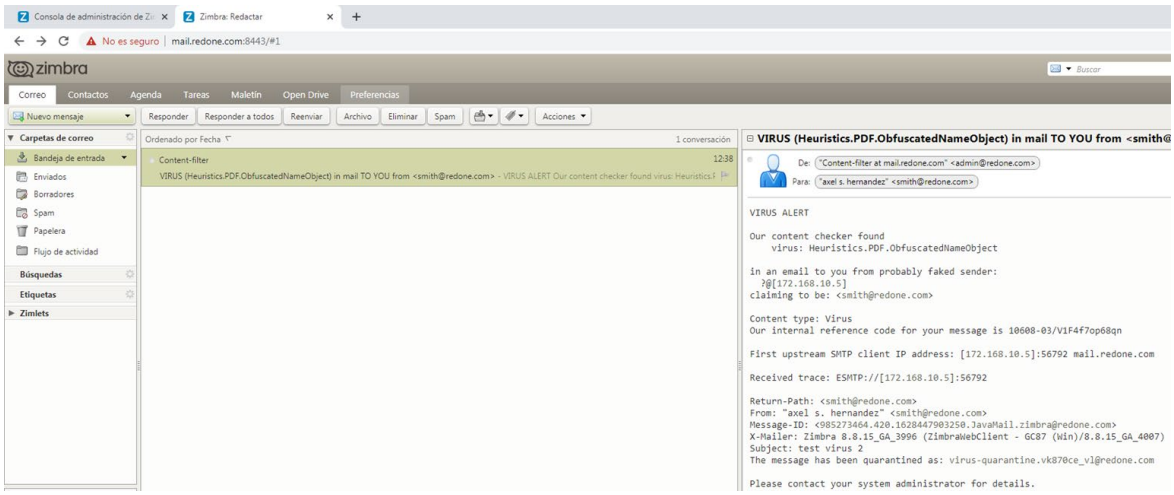

Figura 112. Alerta de Virus en Zimbra

Envío de virus dentro la institución redone.com suite zimbra con un programa .exe

Hemos ingresado un virus dentro un programa .exe, como última prueba interna para asegurarnos que nuestro antivirus (ClamAV antivirus) funciona correctamente

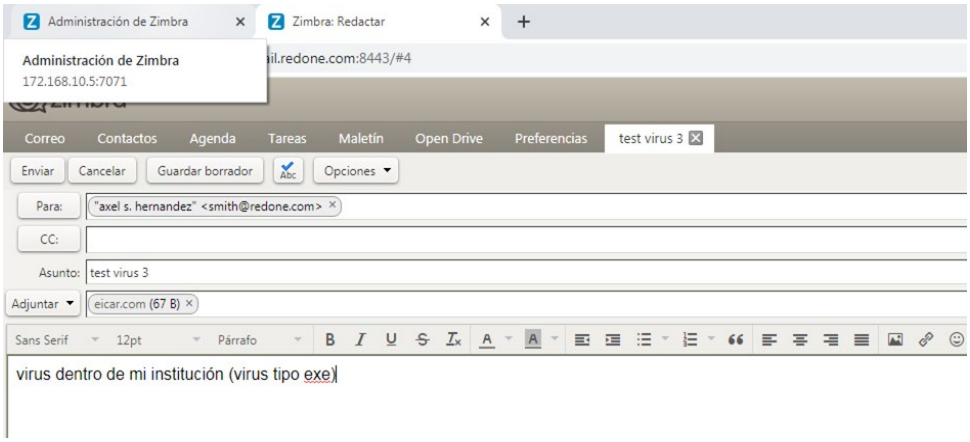

Figura 113. Envío de Archivo .EXE en Zimbra

```
Aug  8 12:52:42 mail postfix/amavisd/smtpd[851]: 48ACA3C390A: client=localhost[127.0.0.1]
Aug  8 12:52:42 mail postfix/cleanup[846]: 48ACA3C390A: message-id=<748744317.564.1628448762004.Java
Mail.zimbra@redone.com>
Aug  8 12:52:42 mail postfix/qmgr[4254]: 48ACA3C390A: from=<>, size=2720, nrcpt=1 (queue active)
Aug  8 12:52:42 mail postfix/amavisd/smtpd[851]: disconnect from localhost[127.0.0.1] ehlo=1 mail=1
rcpt=1 data=1 quit=1 commands=5
Aug  8 12:52:42 mail postfix/amavisd/smtpd[851]: connect from localhost[127.0.0.1]
Aug  8 12:52:42 mail postfix/amavisd/smtpd[851]: 4EBC33C390C: client=localhost[127.0.0.1]
Aug  8 12:52:42 mail postfix/cleanup[846]: 4EBC33C390C: message-id=<VApJp2zJx1dYOO@mail.redone.com>
Aug  8 12:52:42 mail postfix/qmgr[4254]: 4EBC33C390C: from=<admin@redone.com>, size=2694, nrcpt=1 (q
ueue active)
Aug  8 12:52:42 mail postfix/amavisd/smtpd[851]: disconnect from localhost[127.0.0.1] ehlo=1 mail=1
rcpt=1 data=1 quit=1 commands=5
Aug  8 12:52:42 mail postfix/amavisd/smtpd[851]: connect from localhost[127.0.0.1]
Aug  8 12:52:42 mail postfix/amavisd/smtpd[851]: 5650F3C390D: client=localhost[127.0.0.1]
Aug  8 12:52:42 mail postfix/cleanup[846]: 5650F3C390D: message-id=<VRpJp2zJx1dYOO@mail.redone.com>
Aug  8 12:52:42 mail postfix/qmgr[4254]: 5650F3C390D: from=<admin@redone.com>, size=1364, nrcpt=1 (q
ueue active)
Aug  8 12:52:42 mail postfix/amavisd/smtpd[851]: disconnect from localhost[127.0.0.1] ehlo=1 mail=1
 rcpt=1 data=1 quit=1 commands=5
ug  8 12:52:42 mail postfix/smtp[847]: 21C333C38CF: to=<smith@redone.com>, relay=127.0.0.1[127.0.0.
 ]:10026, delay=0.24, delays=0.01/0.02/0.01/0.21, dsn=2.7.0, status=sent (250 2.7.0 Ok, discarded, i
 =10621-05 - INFECTED: Eicar-Test-Signature)
ug  8 12:52:42 mail postfix/qmgr[4254]: 21C333C38CF: removed
ug  8 12:52:42 mail postfix/lmtp[853]: 48ACA3C390A: to=<virus-quarantine.vk870ce_vl@redone.com>, re
ay=mail.redone.com[172.168.10.5]:7025, delay=0.22, delays=0.01/0.01/0.11/0.09, dsn=2.1.5, status=se
t (250 2.1.5 Delivery OK)
ug  8 12:52:42 mail postfix/qmgr[4254]: 48ACA3C390A: removed
ug  8 12:52:42 mail postfix/lmtp[854]: 4EBC33C390C: to=<admin@redone.com>, relay=mail.redone.com[17
.168.10.5]:7025, delay=0.2, delays=0.01/0.02/0.09/0.09, dsn=2.1.5, status=sent (250 2.1.5 Delivery
K)
ug  8 12:52:42 mail postfix/qmgr[4254]: 4EBC33C390C: removed
ug  8 12:52:42 mail postfix/lmtp[855]: 5650F3C390D: to=<smith@redone.com>, relay=mail.redone.com[17
.168.10.5]:7025, delay=0.19, delays=0.01/0.01/0.09/0.07, dsn=2.1.5, status=sent (250 2.1.5 Delivery
OK)
ug  8 12:52:42 mail postfix/qmgr[4254]: 5650F3C390D: removed
root@mail:~# _
```

Figura 114. Log Envío de Archivo .EXE en Zimbra

Como se muestra en los log tenemos toda la información necesaria para demostrar que nuestro antivirus está funcionando correctamente.

El mensaje enviado con el programa malicioso fue detectado por el antivirus y fue enviado a cuarentena directamente, también nos muestra la información de hora, tamaño y correo con su dominio.

También nos muestra un (Delivery OK) en la notificación 3 del log que es un mensaje enviado por el administrador que muestra una pequeña información de dicho atacante o usuario que quiso enviar un virus

Como nos muestra la siguiente imagen tenemos la pequeña información que el administrador nos ha proporcionado después de analizar el virus como el tipo, correo especifico y dominio, ip del atacante y un pequeño mensaje de advertencia.

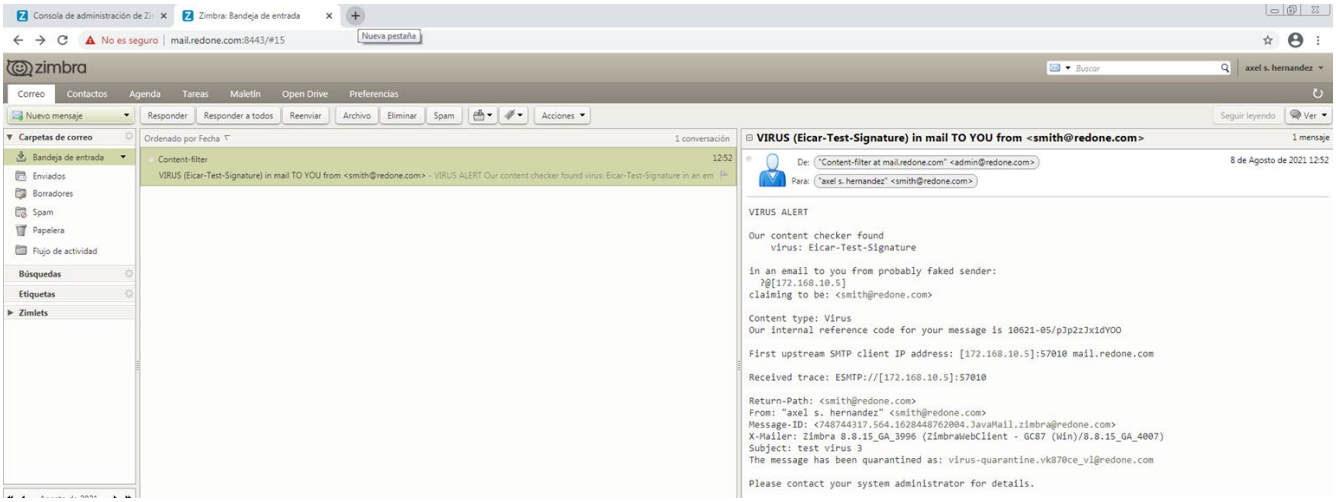

Figura 115. Alerta de Virus en Zimbra

5.6. Pruebas Suite Open-Xchange

5.6.1. Pruebas envíos de correo desde open-xchange a zimbra y Kopano

De: Fabian@teknova.com A: Jason96@credobank.com smith@redone.com

Prueba de envío de texto plano desde open-xchange a zimbra y Kopano

En esta sección se harán las pruebas respectivas del envío de texto plano en correo a las suites zimbra y Kopano, se hará un pequeño análisis de que es lo que nos muestran los archivos logs del servidor que es donde llega todo tipo de notificación del sistema

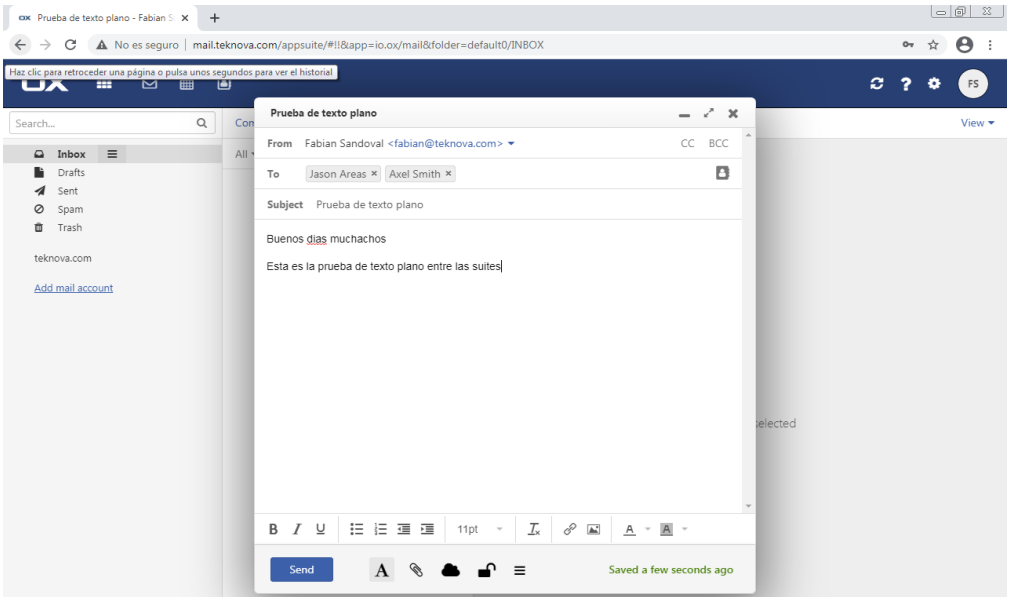

Figura 116. Envío de correo desde OpenXchange a Zimbra y Kopano

En la figura anterior se observa la interfaz para enviar un nuevo correo en open-xchange, en esta ocasión se estará enviando dos correos simultáneos a las demás suites con sus respectivos dominios para este ejemplo tenemos las siguientes direcciones de correo y a que suite pertenecen:

- jason96@credobank.com (Kopano)
- smith@redone.com (Zimbra)

Luego procederemos a analizar los logs resultantes del envío de estos correos

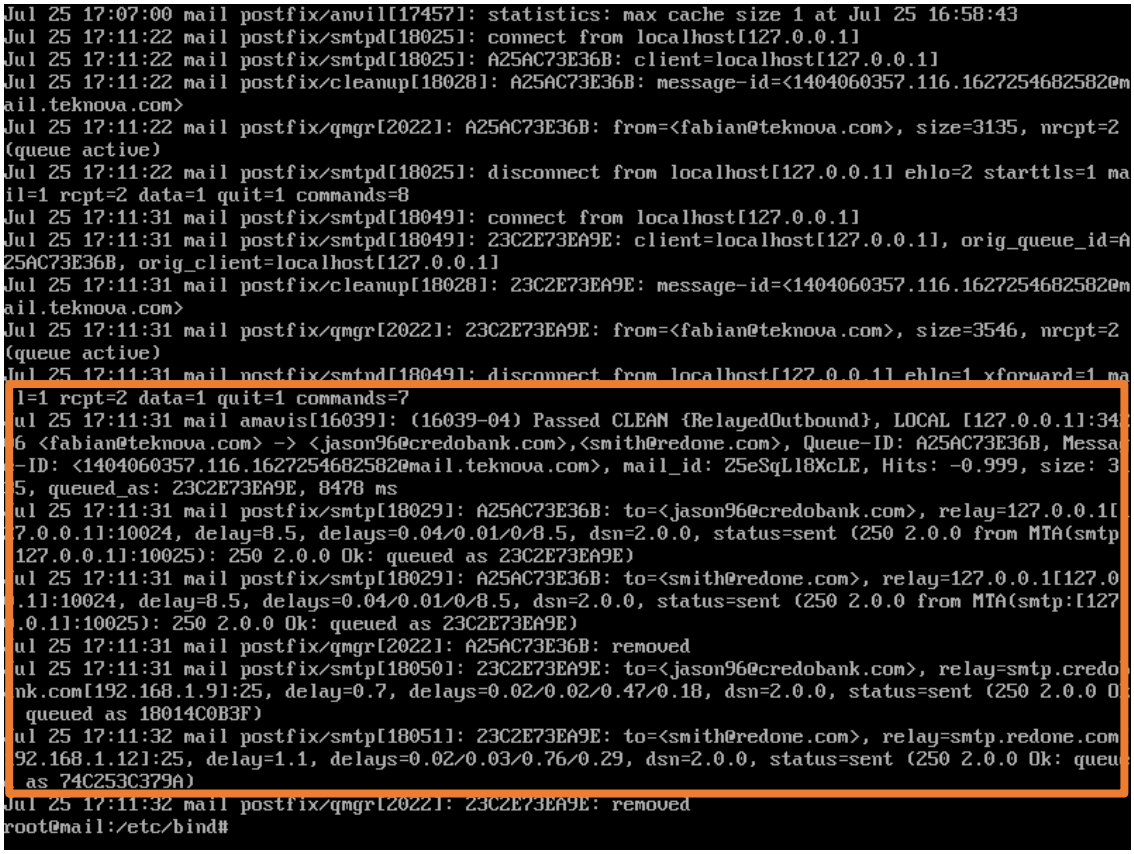

Figura 117. Log Envío de correo desde OpenXchange a Zimbra y Kopano

En primera instancia se hace un análisis de los correos con el antivirus instalado en el sistema en este caso es el antivirus ClamAV con interfaz Amavisd-new entre nuestro servidor de correo y el antivirus, luego de haber pasado el análisis se procede a hacer el envío y nuestro servidor SMTP nos confirma que el envío se ha hecho correctamente, luego de ellos nos llegan dos notificaciones más estas provenientes de los servidores vecinos confirmándonos que el correo fue recibido y pasado a ser encolado para su dicha entrega al cliente.

5.6.2. Prueba de envío de archivo Excel desde open-xchange a zimbra y Kopano.

En esta prueba se hará el envío de un archivo Excel a través de correo a los respectivos usuarios de las demás suites, se hará un pequeño análisis de que es lo que nos muestran los archivos logs del servidor que es donde llega todo tipo de notificación del sistema.

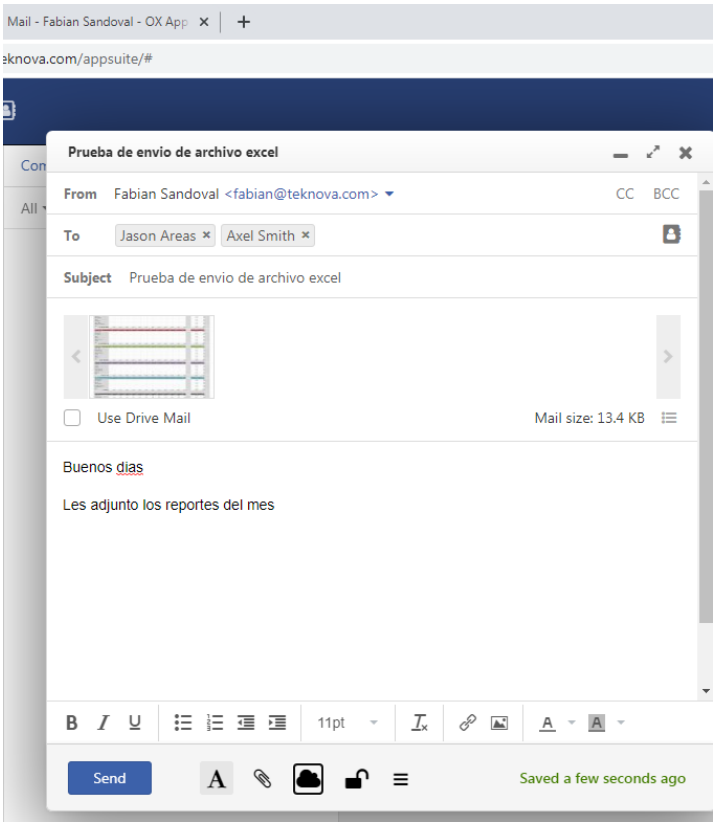

Figura 118. Envío de archivo Excel desde OpenXchange a Zimbra y Kopano.

Como podemos apreciar OpenXchange nos permite también adjuntar archivos, por defecto OpenXchange solo nos permite subir archivos no mayores a 10Mb siendo esta opción configurable para implementaciones avanzadas.

La opción "Use Drive Mail" es útil si solo se desea que la persona tenga acceso al archivo sin ser enviado una copia de este, lo que se enviara será un enlace a una sección de la nube de open-xchange administrada por el usuario que envió el correo teniendo permisos también el usuario receptor del correo

Se estará utilizando también los mismos dominios para este ejemplo, tenemos las siguientes direcciones de correo y a que suite pertenecen:

- jason96@credobank.com (Kopano)
- smith@redone.com (Zimbra)

Luego procederemos a analizar los logs resultantes del envío de estos correos.

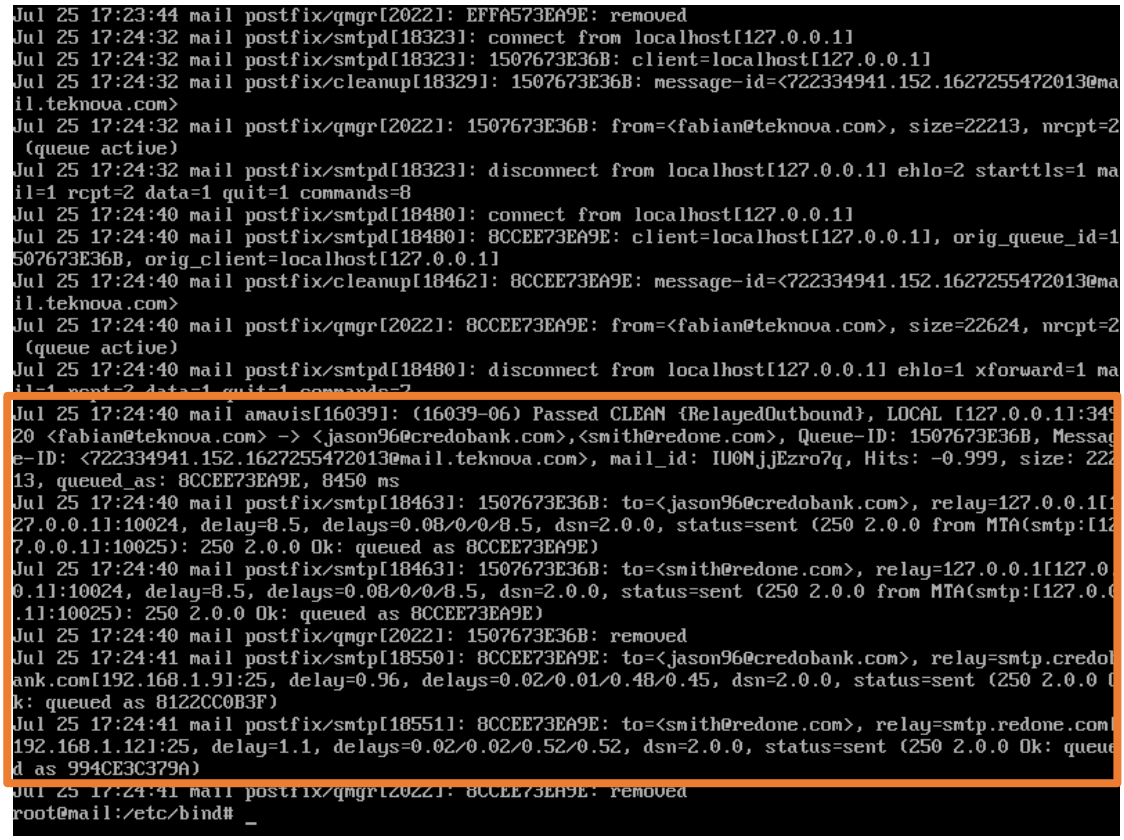

Figura 119. Envío de archivo Excel desde OpenXchange a Zimbra y Kopano.

Al igual que la prueba anterior todo ocurre con normalidad y se reciben 2 confirmaciones de los servidores vecinos anunciando que los correos fueron recibidos además de ser analizado por el antivirus en busca de amenazas.

5.6.3. Prueba de envío de archivo ZIP desde open-xchange a zimbra y Kopano.

Lo que se pretende lograr con esta prueba es que open-xchange. No tiene problema alguno con el envío de este tipo de archivo.

Las direcciones usadas para esta prueba serán las siguientes:

- jason96@credobank.com (Kopano)
- smith@redone.com (Zimbra)

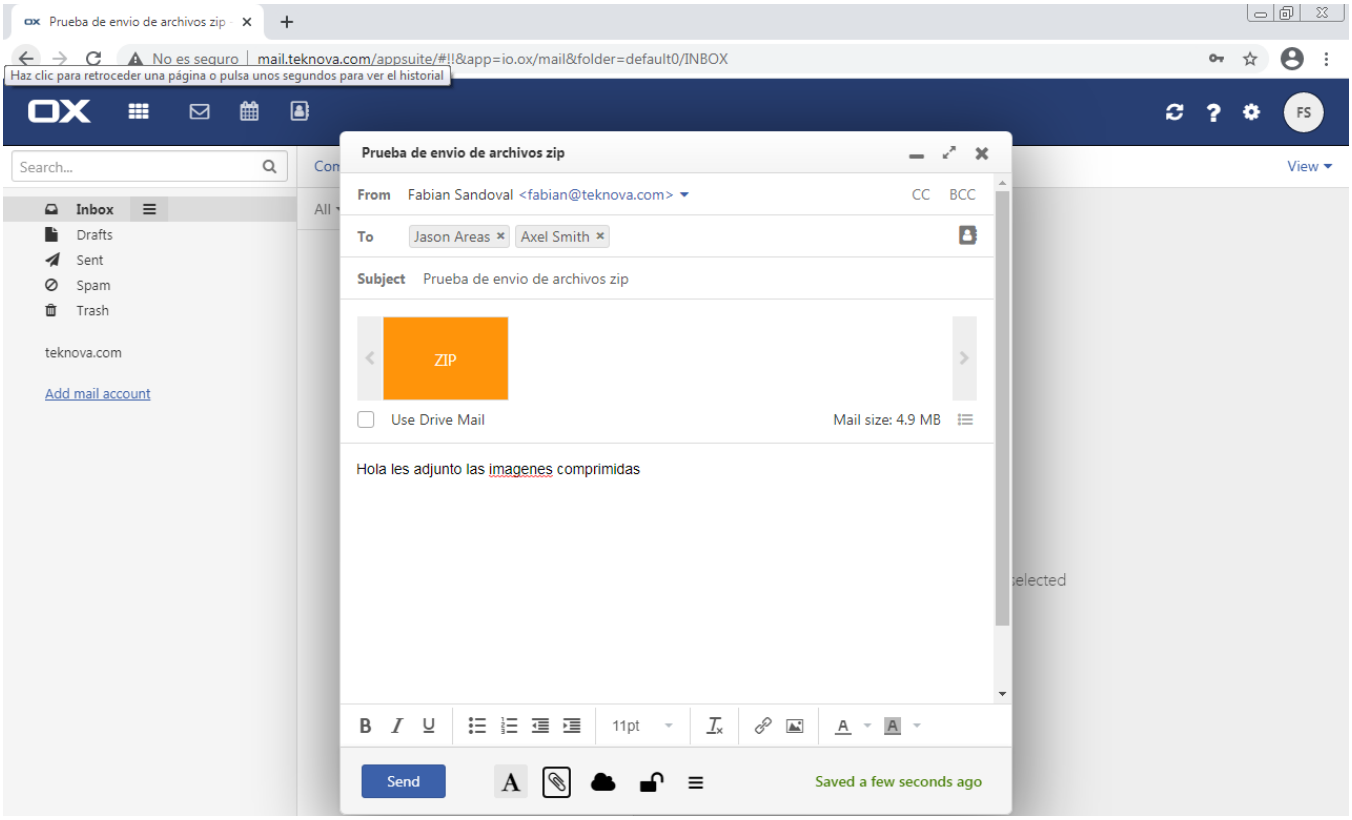

Figura 120. Envío de archivo ZIP desde OpenXchange a Zimbra y Kopano

OpenXchange realiza el envío con normalidad a ambos destinatarios como si fuera con cualquier otro archivo. Pasaremos a inspeccionar que nos indican el archivo log sobre la pasada acción.

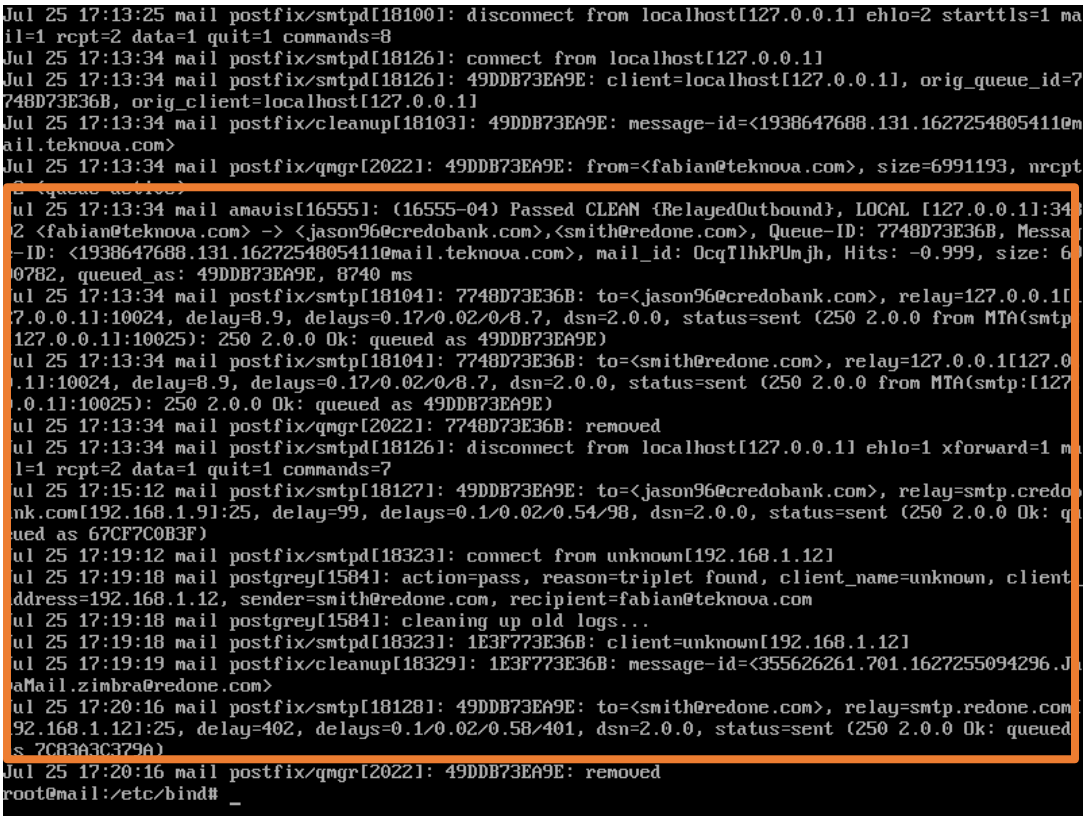

Figura 121. Envío de archivo ZIP desde OpenXchange a Zimbra y Kopano.

Se sigue el mismo procedimiento como en las pruebas anteriores solo que notamos un ligero retardo en el análisis del contenido del correo esto debido a que es un archivo de 4.9Mb por lo tanto el antivirus suele demorarse unos milisegundos más que con las pruebas anteriormente hechas.

5.6.4. Pruebas configuración antispam en OpenXchange.

Filtro de palabras claves en los correos.

En esta prueba se configurará un filtro con la suite OpenXchange para que mueva de lugar los correos que contengan cierto patrón de texto.

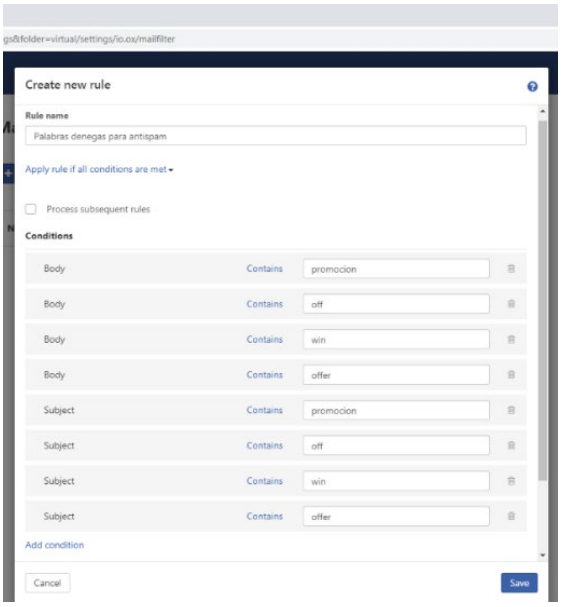

Figura 122. Configuración Antispam en OpenXchange

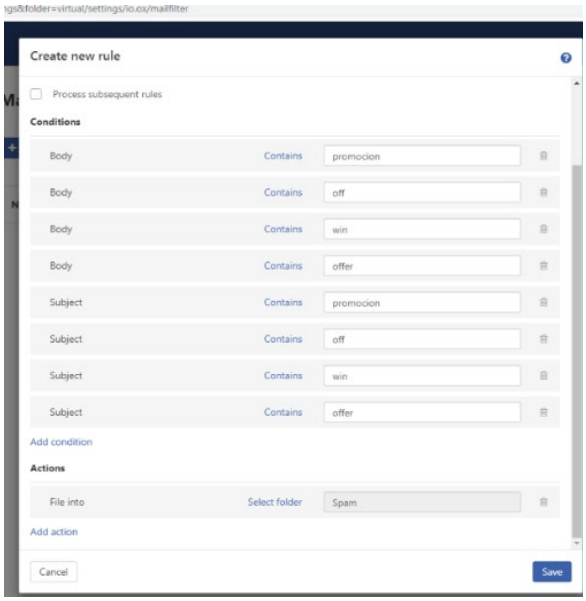

Figura 123. Configuración Antispam en OpenXchange

En la figura anterior se observa la interfaz para agregar un filtro antispam en open-xchange, el filtro consta de 10 líneas y cada una es un filtro que realiza una búsqueda de las palabras agregadas en cada línea. Este filtro es llamado “Contains” porque realiza una comparativa si el punto específico del correo contiene la palabra indicada en el campo de texto, para este ejemplo usaremos como puntos específicos el cuerpo y el asunto de los correos.

La sección de “Actions” es donde especificamos que queremos que haga la suite si las condiciones anteriores se cumplen, nosotros elegiremos mandar todos los correos con este patrón a la carpeta de spam de usuario.

Nos estarán enviando dos correos que contengan este patrón para que open-xchange se encargue de hacer la redirección a la carpeta de spam.

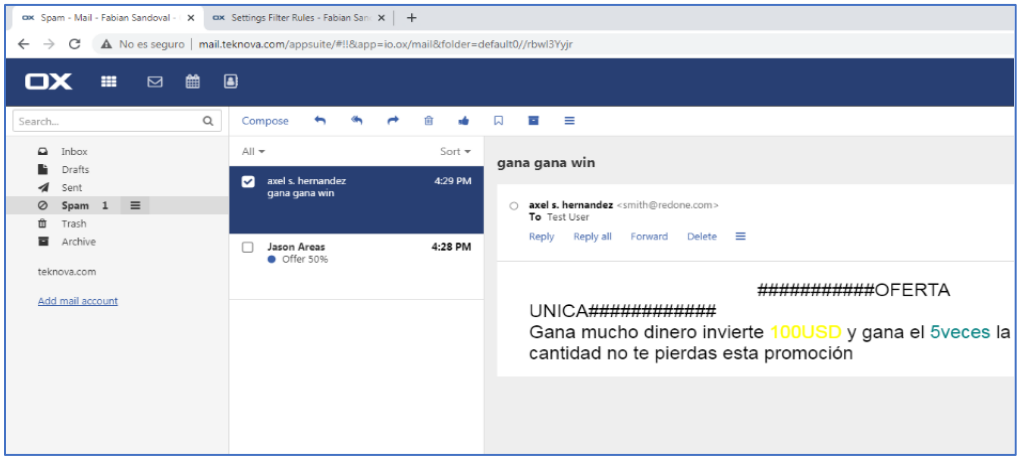

Figura 124. Bandeja de Correo SPAM.

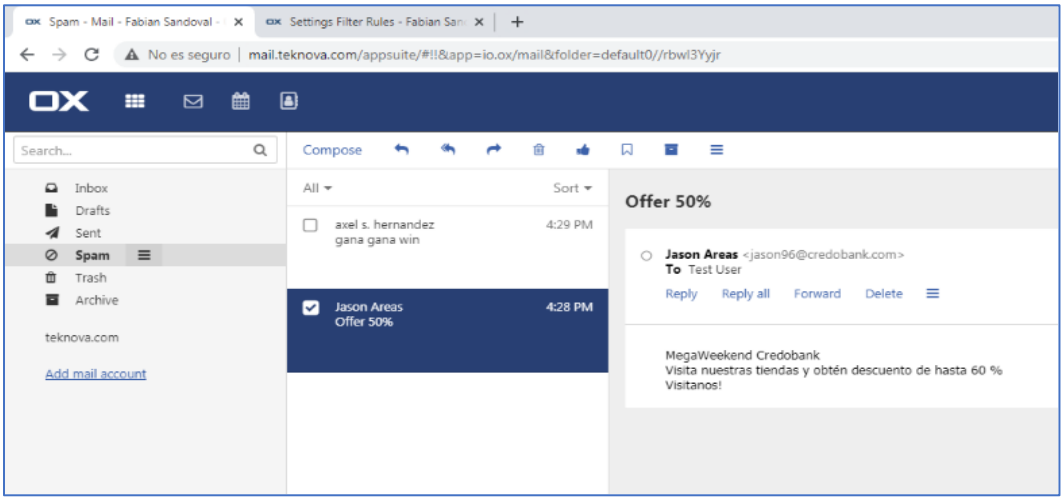

Figura 125. Bandeja de Correo SPAM.

Con las pasadas imagen nos aseguramos de que los correos llegaron donde corresponden y cumplen con el patrón descrito en la regla, existen muchas más opciones de configuración que estaremos viendo en apartados más adelante.

Filtro de palabras enlaces a sitios externos en los correos.

Para esta sección se configurará un filtro con la suite OpenXchange para que mueva de lugar los correos que contengan enlaces a sitios exteriores y potencialmente dañinos.

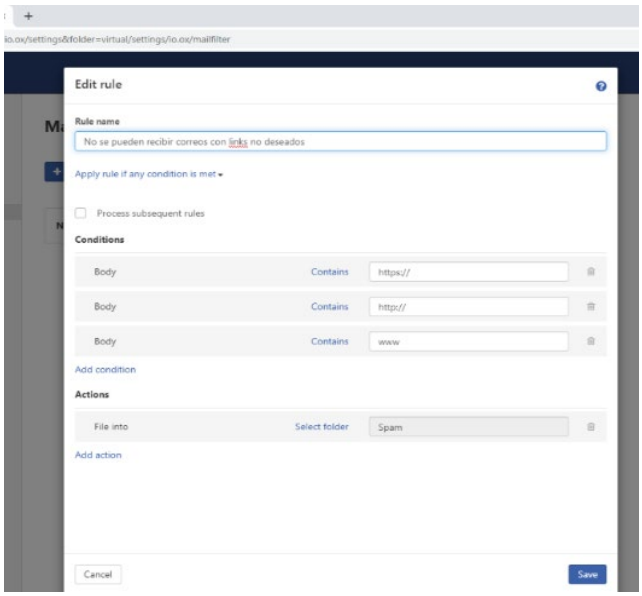

Figura 126. Ajuste de SPAM en OpenXchange

Para aplicar este filtro solo se necesita aplicar los mismos pasos de la prueba anterior pero esta vez estaremos buscando las palabras “https://”, “http://” y “www”.

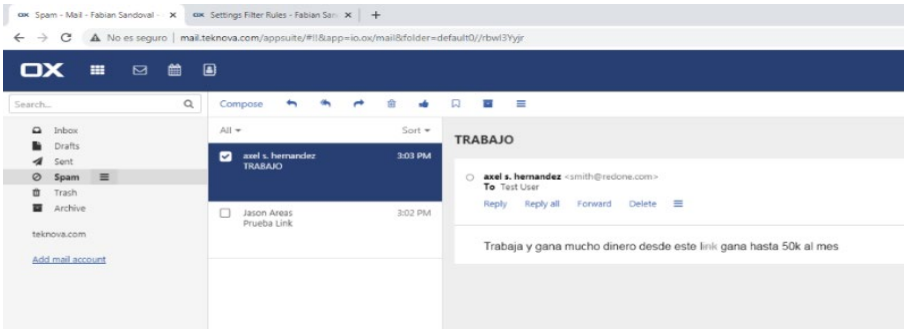

Figura 127. Ajuste de SPAM en OpenXchange Filtro de palabras.

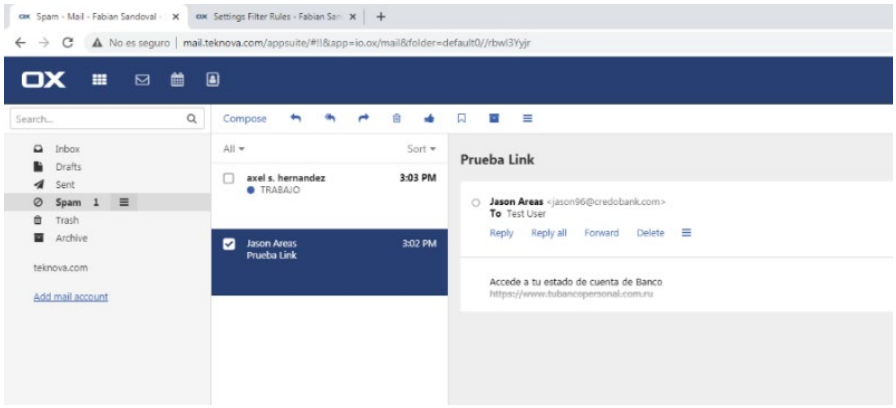

Figura 128. Bandeja de SPAM en OpenXchange.

La regla tuvo éxito en su análisis ya que detecta los enlaces en el cuerpo de los correos, aunque estos estén compactados como palabras y además de eso open-xchange nos indica la palabra que contiene el link y lo tacha de gris para poder ser diferenciado del resto del contenido.

Gracias a este filtro el usuario no tendrá las molestias de leer correos y por accidente acceder a sitios indeseados o con algún método para dañar su integridad.

Filtro de archivos pesados en los correos.

Para esta prueba se establecerá un filtro con la suite open-xchange que nos permitirá mover a la carpeta de spam todos los correos que contengan archivos mayores a 4Mb ya que algunas instituciones no suelen compartir archivos muy pesados a través de correos sino solo se comparten el enlace para acceder a dicho recurso.

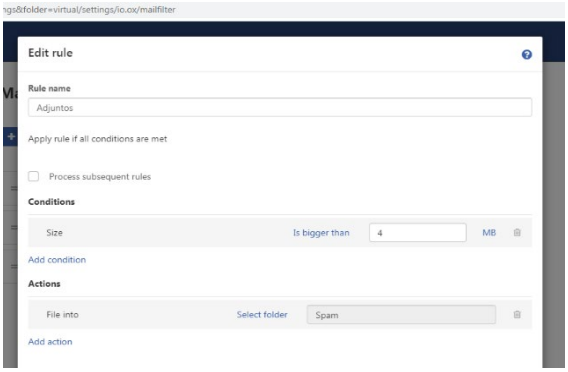

Figura 129. Ajuste de SPAM en OpenXchange.

Para este filtro se utilizará la condición “Size” con la secuencia “In bigger than” que tiene disponible con el filtro de spam de open-xchange, esta condición nos dará los parámetros necesarios para aplicar el filtro solo introducimos la cantidad y damos guardar para aplicar el filtro.

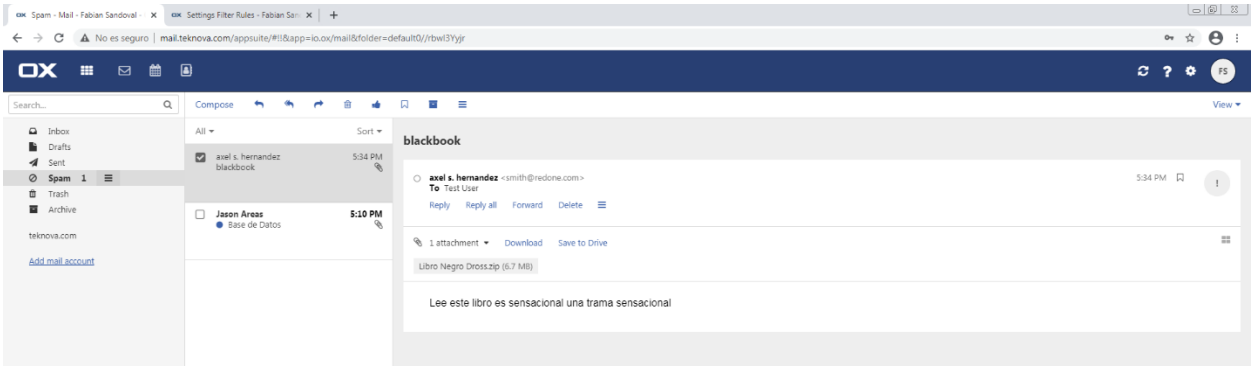

Figura 130. Bandeja SPAM en OpenXchange

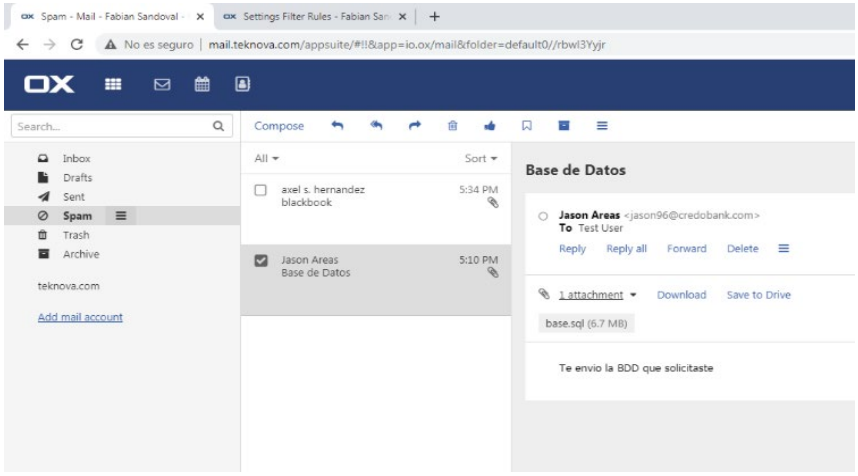

Figura 131. Bandeja de SPAM en OpenXchange.

Nuestras pruebas se ejecutaron correctamente y podemos observar que la condición se cumplió y todos los correos con archivos mayores a 4Mb han sido movidos a la carpeta spam del usuario.

Este filtro puede ser muy útil ya que se puede dar la situación de que se trate de enviar algún archivo malicioso en los correos o un archivo comprimido que al abrirlo pueda duplicar o triplicar su tamaño.

Existe múltiples condiciones y acciones que nos ofrece el filtro antispam de open-xchange para configurar un filtro más robusto y que se acople a las necesidades de la empresa para el cuido de los usuarios y su uso sea el correcto, para estas pruebas se han realizados los filtros básicos que un usuario normal podría ocupar en su día a día.

5.6.5. Pruebas de antivirus en open-xchange.

En esta sección estaremos realizando pruebas al filtrador de contenido ClamAV a través de Amavisd-new que viene instalado por defecto en el software univention, open-xchange como tal no cuenta con un antivirus elaborado por su equipo de desarrollo si cuenta con el servicio de Ox Guard pero este no es un antivirus como tal más bien es una forma de controlar el acceso a los correos de cada usuario.

Para que open-xchange pueda analizar los correos en busca de posibles amenazas se debe de instalar un antivirus de tercero en este caso ClamAV viene por defecto integrado con el software Univention.

La prueba EICAR (nombre oficial: EICAR Standard Anti-Virus Test File) es una prueba, desarrollada por el European Institute for Computer Antivirus Research (en español Instituto Europeo para la Investigación de los Antivirus Informáticos) y por Computer Antivirus Research Organization (en español Organización de Investigación de los Antivirus Informáticos), para probar la respuesta de los programas antivirus en el equipo. La razón detrás de esto es permitir a las personas, empresas y programadores de antivirus, probar su software sin tener que utilizar un verdadero virus informático que pudiera causar daño real al no responder el antivirus correctamente. El Instituto Europeo para la Investigación de los Antivirus Informáticos, compara el uso de un

virus vivo para probar el software antivirus como el establecimiento de un fuego en un cubo de basura para poner a prueba una alarma de incendio, y promueve el archivo de prueba EICAR como una alternativa segura.

Se estará probando la efectividad del filtrador de contenido Amavisd-new tanto en el envío como la recepción de diferentes archivos potencialmente dañinos para esto se realizará el envío y recepción de 3 tipos de archivos infectados con el archivo de prueba antes descrito llamado Eicar los archivos serán:

- Archivo .exe o ejecutable
- Archivo .pdf o archivo de texto
- Archivo zip que contiene un archivo infectado.

Con estos 3 tipos de archivos se pretende medir la efectividad del antivirus ClamAV y como Amavisd-new se encarga de realizar la comunicación entre el servidor de correo y el antivirus instalado en el sistema además estaremos viendo que nos pueden mostrar los archivos logs con respecto a cada prueba.

de archivo .exe o ejecutable desde OpenXchange.

En esta prueba se intentará enviar un correo con un archivo ejecutable al usuario jason96@credobank.com veremos que nos muestran los logs y de qué forma reacciona el ClamAV ante tal amenaza.

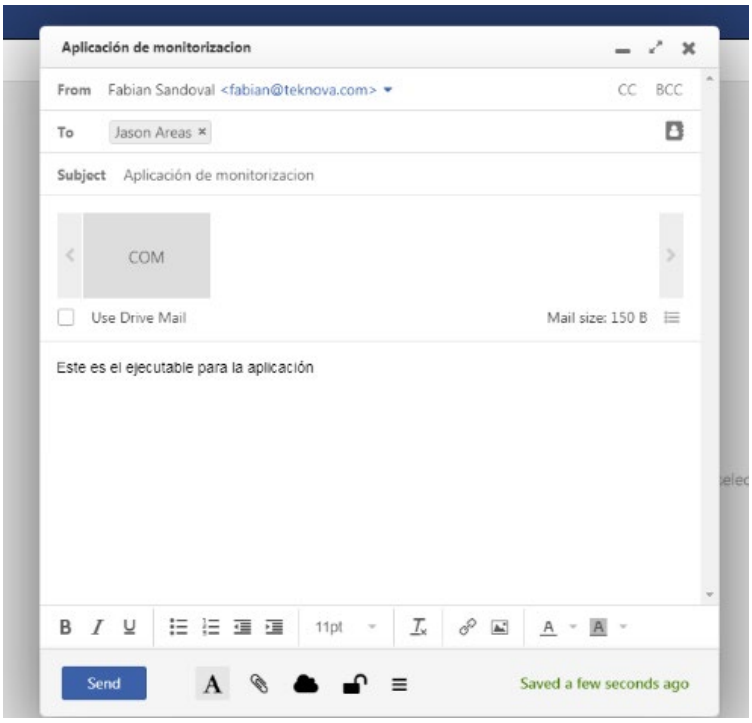

Figura 132. Virus en Archivo .EXE en OpenXchange

Antes de enviar el correo la vista ´para enviar el archivo ejecutable no nos muestran si hay una amenaza o no, simplemente todo fluye con normalidad, los archivos logs son los que nos mostraran más detalle acerca de esto.

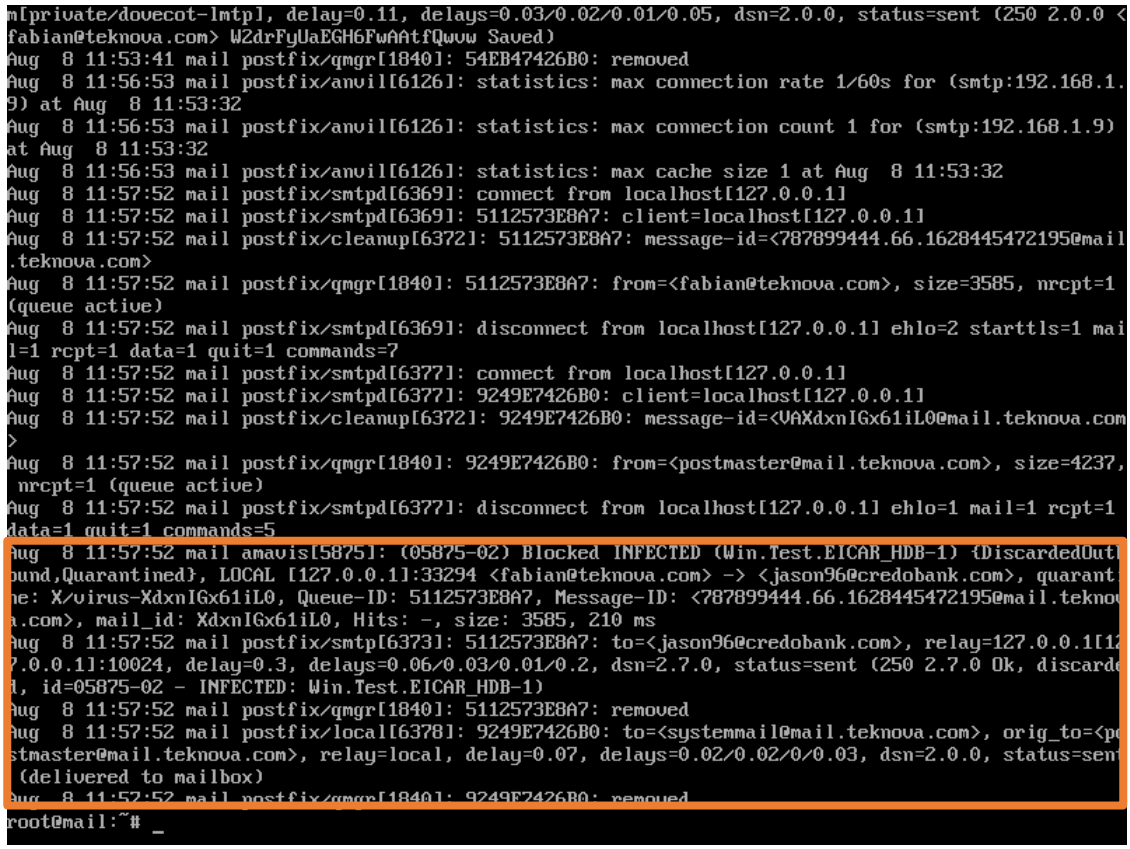

Figura 133. Log Virus en Archivo .EXE en OpenXchange

En la figura anterior podemos notar que la amenaza fue detectada ya que el antivirus detecta la amenaza como Win.Test. EICAR_HDB-1 esto nos demuestra que no solo fue detectado, sino que también nos regresa el nombre de la amenaza con esto podemos saber que las licencias de virus tienen en sus bases de datos información acerca del archivo de prueba EICAR.

También podemos observar información como el tiempo que demoro el antivirus en analizar el archivo la dirección IP del usuario que intento hacer el envío además que fue descartado el correo y puesto en cuarentena, por esta razón no fue enviado al destinatario.

Envió de archivo pdf o texto desde open-xchange.

Para esta ocasión se intentará enviar un correo con un archivo pdf al usuario jason96@credobank.com para ser analizado y veremos si ClamAV es capaz de detectar el código malicioso dentro de un archivo pdf.

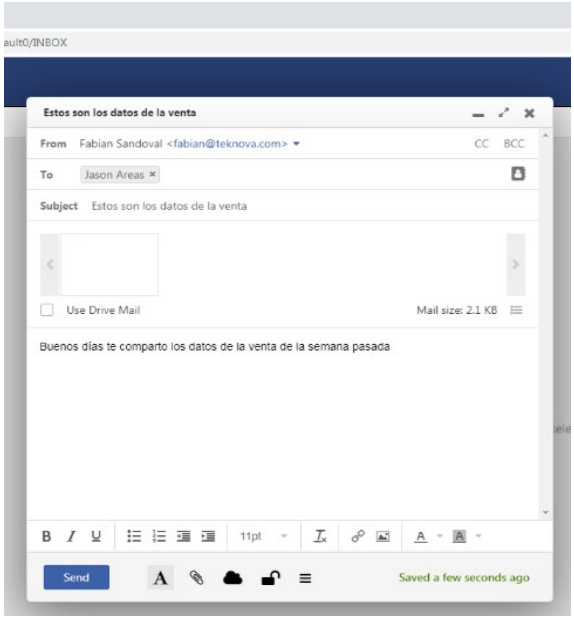

Figura 134. Virus en Archivo .PDF en OpenXchange

Al igual que en pruebas anteriores todo fluye con normalidad y la interfaz no muestra señales de que haga un análisis al contenido del correo

```
Aug  8 11:23:06 mail postfix/anvil[4817]: statistics: max connection rate 1/60s for (smtp:192.168.1.
9) at Aug  8 11:19:45
Aug  8 11:23:06 mail postfix/anvil[4817]: statistics: max connection count 1 for (smtp:192.168.1.9)
at Aug  8 11:19:45
Aug  8 11:23:06 mail postfix/anvil[4817]: statistics: max cache size 1 at Aug  8 11:19:45
Aug  8 11:37:14 mail postfix/smtpd[5349]: connect from localhost[127.0.0.1]
Aug  8 11:37:14 mail postfix/smtpd[5349]: disconnect from localhost[127.0.0.1] ehlo=1 quit=1 command
s=2
Aug  8 11:37:14 mail postfix/smtpd[5349]: connect from localhost[127.0.0.1]
Aug  8 11:37:14 mail postfix/smtpd[5349]: E10F473F1B3: client=localhost[127.0.0.1]
Aug  8 11:37:14 mail postfix/cleanup[5352]: E10F473F1B3: message-id=<1066723939.16.1628444234796@mai
l.teknova.com>
Aug  8 11:37:14 mail postfix/qmgr[1840]: E10F473F1B3: from=<fabian@teknova.com>, size=6338, nrcpt=1
(queue active)
Aug  8 11:37:14 mail postfix/smtpd[5349]: disconnect from localhost[127.0.0.1] ehlo=2 starttls=1 mai
l=1 rcpt=1 data=1 quit=1 commands=7
Aug  8 11:37:15 mail postfix/smtpd[5358]: connect from localhost[127.0.0.1]
Aug  8 11:37:15 mail postfix/smtpd[5358]: 49FE07426B0: client=localhost[127.0.0.1]
Aug  8 11:37:15 mail postfix/cleanup[5352]: 49FE07426B0: message-id=<VAO2znjOjW395j@mail.teknova.com
>
Aug  8 11:37:15 mail postfix/qmgr[1840]: 49FE07426B0: from=<postmaster@mail.teknova.com>, size=4184,
 nrcpt=1 (queue active)
Aug  8 11:37:15 mail postfix/smtpd[5358]: disconnect from localhost[127.0.0.1] ehlo=1 mail=1 rcpt=1
data=1 quit=1 commands=5
Aug  8 11:37:15 mail amavis[2722]: (02722-03) Blocked INFECTED (Pdf.Dropper.Agent-6299277-0) {Discar
dOutbound,Quarantined}, LOCAL [127.0.0.1]:60712 <fabian@teknova.com> -> <jason96@credobank.com>, q
uarantine: O/virus-O2znjOjW395j, Queue-ID: E10F473F1B3, Message-ID: <1066723939.16.1628444234796@mai
l.teknova.com>, mail_id: O2znjOjW395j, Hits: -, size: 6338, 373 ms
Aug  8 11:37:15 mail postfix/smtp[5354]: E10F473F1B3: to=<jason96@credobank.com>, relay=127.0.0.1[12
7.0.0.1]:10024, delay=0.43, delays=0.04/0.01/0/0.37, dsn=2.7.0, status=sent (250 2.7.0 Ok, discarded
, id=02722-03 - INFECTED: Pdf.Dropper.Agent-6299277-0)
Aug  8 11:37:15 mail postfix/qmgr[1840]: E10F473F1B3: removed
Aug  8 11:37:15 mail postfix/local[5359]: 49FE07426B0: to=<systemmail@mail.teknova.com>, orig_to=<po
stmaster@mail.teknova.com>, relay=local, delay=0.08, delays=0.04/0.02/0/0.02, dsn=2.0.0, status=sent
 (delivered to mailbox)
Aug  8 11:37:15 mail postfix/qmgr[1840]: 49FE07426B0: removed
root@mail:~# _
```

Figura 135. Log Virus en Archivo .PDF en OpenXchange

De nuevo los logs nos reportan que se detectó una amenaza esta vez con un identificador Pdf.DropperAgent-629927-0 que al igual que en la prueba anterior fue puesto en cuarentena y descartado de ser enviado. Este escaneo se ha realizado en tiempo real y de una forma rápida.

Envió de archivo zip que contiene un archivo malicioso.

Con esta prueba vamos a comprobar que, aunque enviemos un archivo malicioso dentro de un archivo zip ClamAV detectará esta amenaza y por lo tanto este correo será descartado. Esto es muy útil cuando se puede dar el escenario que alguien mal intencionado quiera enviar un correo con un virus u otra amenaza empaquetado en un archivo zip.

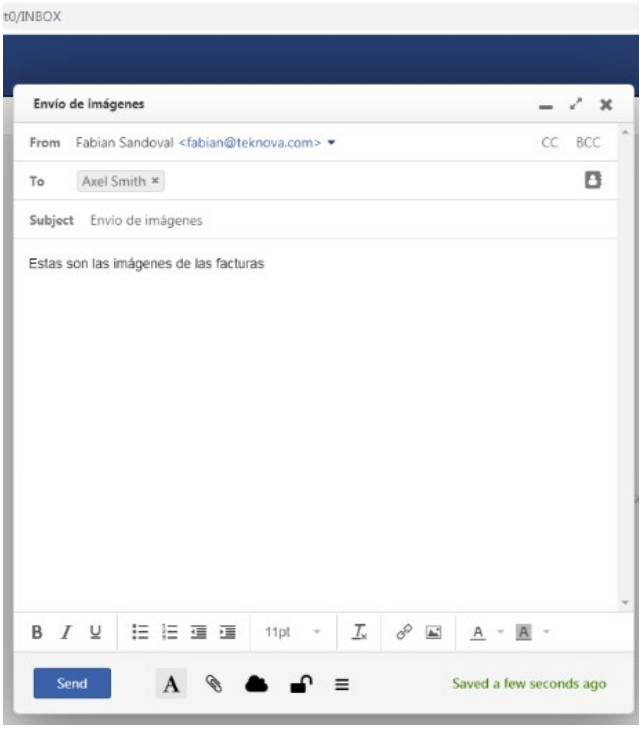

Figura 136. Virus en Archivo .RAR en OpenXchange

Con la pasada figura podemos determinar que el archivo zip se carga en open-xchange sin ningún tipo de problema o inconveniente permitiendo al usuario realizar la acción de envío.

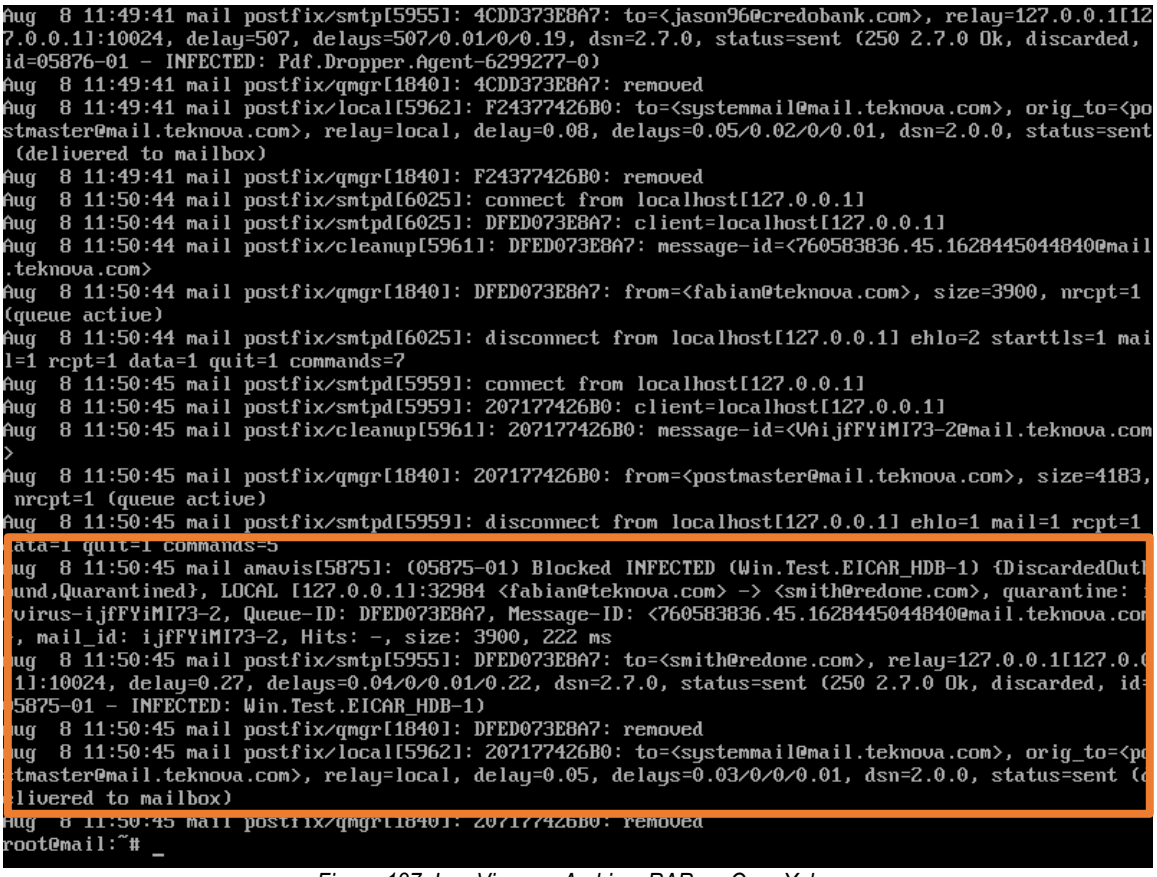

Figura 137. Log Virus en Archivo .RAR en OpenXchange

Luego de realizar el envío de nuevo ClamAV fue capaz de detectar esta amenaza con el identificador Win.Test.EICAR_HDB-1 esto nos demuestra que, aunque la amenaza vaya empaquetada dentro de otro archivo ClamAV puede analizar su contenido de forma rápida y detectar la amenaza para descartar este correo posiblemente dañino para los demás usuarios.

Podemos comprobar que estos logs pertenecen al intento anterior observando el destinatario y la hora en que se realizó el envío

Las bases de datos de firmas garantizan que ClamAV solo ejecutará definiciones de firmas confiables. Es importante recalcar que ClamAV no solo escanea archivos y archivos comprimidos, sino que también protege contra las bombas de archivos.

Comportamiento de open-xchange y ClamAV en la recepción de archivos potencialmente dañinos para los usuarios.

Con esta sección se pretende mostrar como open-xchange reacciona y procede con respecto a la recepción de archivos maliciosos. Así como se realizaron pruebas de envío desde la misma suite también es necesario mencionar como ClamAV y open-xchange cooperan cuando una fuente desconocida envío un correo hacia algún usuario en nuestra institución.

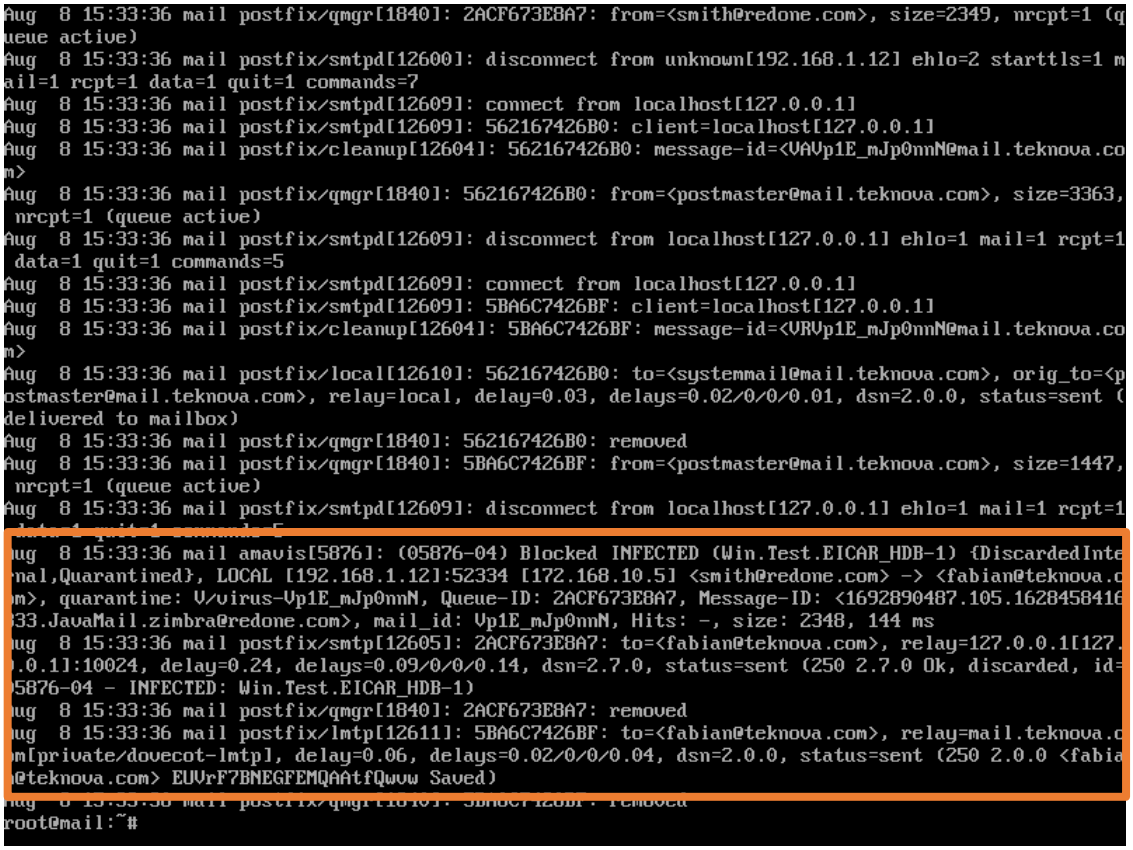

Figura 138. Log Virus en Archivo .RAR en OpenXchange

La pasada figura nos demuestra que el emisor smith@redone.com en esta ocasión nuestra fuente desconocida intento enviarnos un correo infectado con un virus (Eicar test) donde el tipo de archivo es un ejecutable ya que su identificador es Win.Test. EICAR_HDB-1.

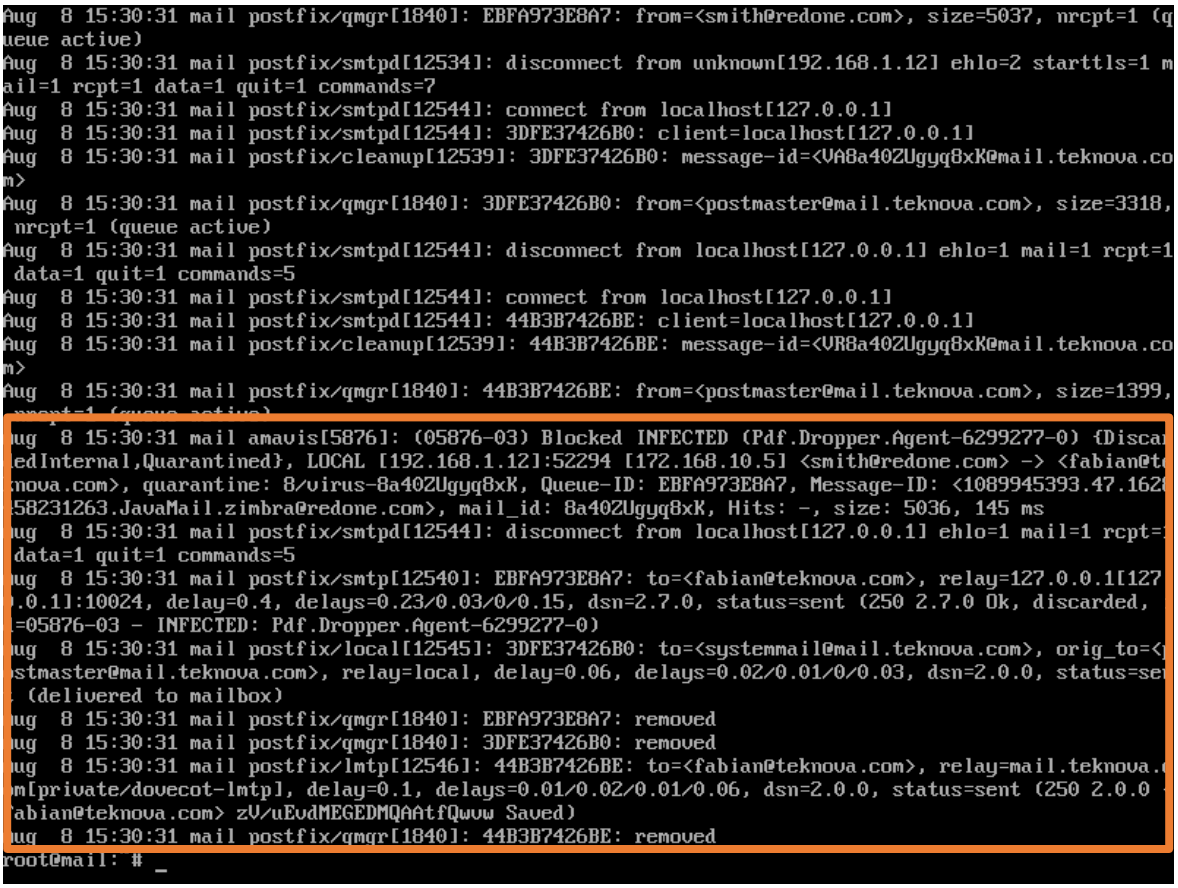

Figura 139. Virus en Archivo .PDF en OpenXchange

Luego de ello se intenta realizar la misma acción solo que esta vez es con un archivo pdf con un código malicioso (Eicar test) determinado por el siguiente identificador Pdf.DropperAgent-629927-0 que de igual manera fue detectado y descartado siendo la fuente igual que la anterior prueba.

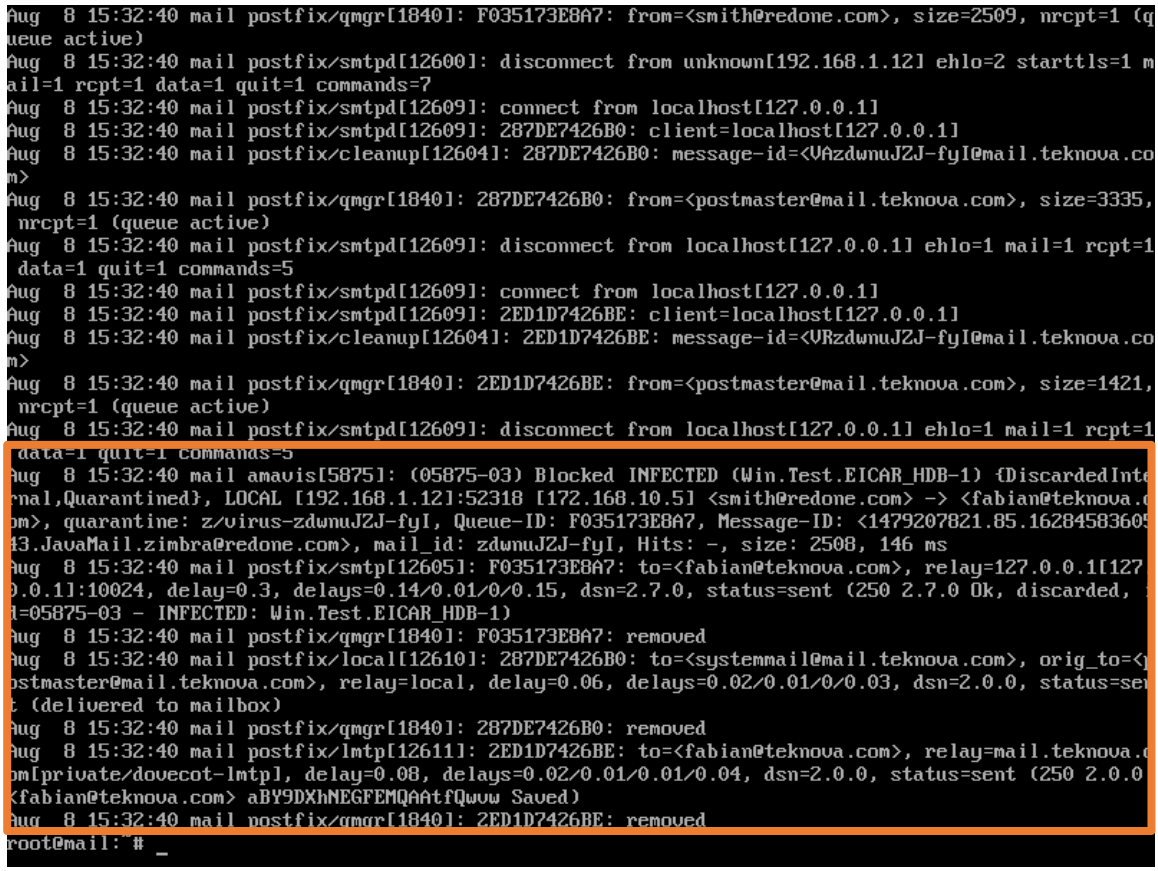

Figura 140. Virus en Archivo en OpenXchange

Por último, tenemos los registros de un intento de envío de archivo malicioso dentro de un archivo zip, aunque no se puede determinar a través de los logs si el peligro estaba en un archivo comprimido la prueba fue realizada de esa manera y nuestra fuente es la anterior smith@redone.com siendo este un servidor zimbra sin protección en pocas palabras inseguro.

La siguiente figura nos demuestra cómo actúan en cooperación open-xchange y ClamAV gracias a que Amavisd-new nos sirve como intermediario entre estos dos servicios se notifica al usuario o destinatario que una fuente insegura envió 3 correos con contenido potencialmente dañino, esta notificación es un correo que Amavisd-new elabora y con la información obtenida desde ClamAV envía a través de Postfix un correo con esta información que luego el usuario podrá leer a través de la plataforma de open-xchange.

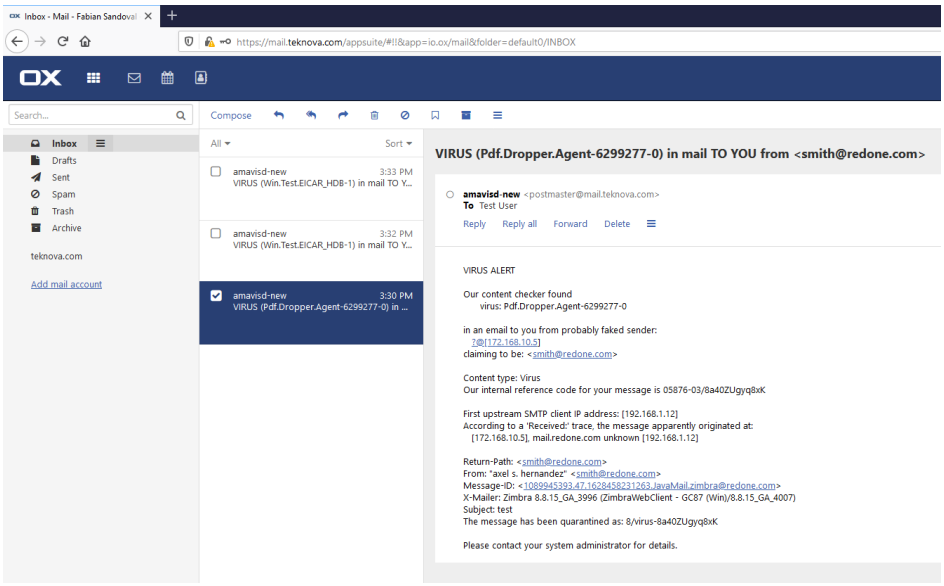

Figura 141. Mensaje de Virus en OpenXchange

Vemos reflejado en la imagen anterior que se recibieron 3 notificaciones esto debido a que fueron 3 correos que nuestra fuente desconocida envío, además de ello nos da información muy relevante para determinar el origen y contenido de esta amenaza esta información puede ser:

- IP del servidor de origen
- Identificador con el que fue reconocida la amenaza
- El tipo de contenido
- Dirección de correo de nuestra fuente
- Si el servidor está bajo red NAT podemos determinarlo en la sección que sigue después de la descripción del tipo de contenido.
- El cliente desde el cual fue enviado el correo (si fue desde uno)

Por último, nos indica que contactemos a nuestro administrador y que el mensaje ha sido puesto en cuarentena, los usuarios pueden tomar esta información y enviarla a su administrador de sistema para que se tomen las medidas pertinentes.

5.7. Características entre Suites

OS support			Protocol support						Features						Storage	License
Mail server	**Linux**	macOS	SMTP	POP3	IMAP	IDLE	SMTPS	POP3S	IPv6	SSL	DANE	Webmail	ActiveSync	Sieve	Database	
Kopano	Yes	No	postfix.	Yes	Yes	Yes	postfix	Yes	Yes	Yes	postfix	Yes	z-push	No	SQL	Yes
Open-Xchange	Yes	No	Yes	Yes	Yes	?	Yes	Yes	?	Yes	?	Yes	Yes	?	Yes	No
Zimbra	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Características	Zimbra	Open Exchange	Kopano
Disponibilidad de código abierto	Sí	Sí	Si
Único propósito	Permita que los usuarios accedan al correo electrónico, calendario, contactos, documentos y tareas desde PC, web y dispositivos móviles.	Permite a los usuarios acceder al correo electrónico, el calendario, los contactos y las tareas desde la computadora, la web y los dispositivos móviles.	Permite a los usuarios acceder al correo electrónico, el calendario, los contactos y las tareas desde la computadora, la web y los dispositivos móviles.
Correo web	El servidor Zimbra ofrece su propio cliente web Zimbra basado en Ajax.	El servidor de intercambio utiliza un protocolo de llamada de procedimiento remoto patentado: MAPI / RPC, diseñado para Open Exchange.	El servidor Zimbra ofrece su propio cliente web
Cliente de escritorio	Zimbra Desktop (ahora descontinuado)	Versión de escritorio de Open Xchange: Linux	Posee su versión de Escritorio Kopano Desktop para Windows y Mac
Capacidades de seguridad avanzadas	ClamAV, SpamAssassin y DSPAM para proteger buzones.	El filtrado antimalware y antispam protege los buzones de correo.	ClamAV, SpamAssassin
Fiabilidad	Tiempo de actividad garantizado del 99,995 % SLA	99,995 % de tiempo de actividad, SLA respaldado financieramente	N/D
Centro de administración	La consola de administración de Zimbra es la interfaz de usuario intuitiva, navegable y basada en navegador que se utiliza para administrar todos los servidores y cuentas de correo de Zimbra de forma centralizada.	Ofrece un centro de administración de Exchange basado en la web fácil de usar para administrar cuentas de Exchange, permisos y creación de usuarios.	Posee una plataforma web amigable y sencilla que desde el primer ingreso permite escoger si queremos acceder a la consola de correo o la consola de administración.
Accede desde el móvil	Configura fácilmente el correo de Zimbra en tu móvil y accede a los correos electrónicos, calendarios, contactos y otros elementos.	Sí, puede usar Open Xchange en su dispositivo móvil y trabajar en su comunicación de mensajes.	Si, Z-Push puede crear sincronización con Microsoft Outlook.
Soporte para navegador	El correo web de Zimbra es compatible con todos los principales navegadores: Chrome, Edge, Safari, Firefox, Bing.	Open Xchange es compatible con todos los navegadores importantes: Chrome, Microsoft Edge, Safari, Mozilla Firefox, Bing.	Es compatible con diversos navegadores como: Chrome, Microsoft Edge, Safari, Mozilla Firefox, Bing.
Seguridad en todos los dispositivos	No	Sí	No

fácil de mantener	El servidor Zimbra y el correo web son fáciles de administrar. Para que pueda mantenerse productivo todo el tiempo.	Es más fácil mantener el correo electrónico comercial para mantener su productividad. La aplicación automática de parches elimina el tiempo y el esfuerzo de mantener su sistema.	No requieren alta especialización para administrar el servidor.
Integración de Outlook	Sí	Sí	Si
Archivo en el lugar y eDiscovery	No	Sí	Si
Políticas de retención personalizadas	No	Sí	Si
Soporte telefónico a nivel de TI	Sí, disponible para usted las 24 horas del día, los siete días de la semana.	Sí, disponible para usted las 24 horas del día, los siete días de la semana.	Sí, disponible para usted las 24 horas del día, los siete días de la semana.
Bandeja de entrada inteligente	Un buzón personalizado con opción de búsqueda, archivador avanzado, vistas múltiples y otras funciones útiles.	Un buzón con funciones útiles como búsqueda, política, prioridad, filtro y una forma organizada de ver e interactuar con el correo electrónico.	Un buzón, con interfaz simple e interactiva que permite encontrar correo de forma sencilla.
Calendario y contacto	Sí	Sí	Si
Costo	Debe comprar el espacio de almacenamiento y crear usuarios ilimitados. Además, también está disponible el modelo para compartir Zimbra. Su costo se calcula por usuario /mes lo cual su costo oscila entre $5 a 25$ según la categoría a contratar.	Es un modelo basado en suscripción en el que debe pagar una tarifa de licencia por usuario por mes o anualmente. Entre los 5 y 55 dólares mensuales.	Suscripción Anual, los precios oscilan entre 15 a 65 euros.

6. Conclusiones

Al finalizar el presente trabajo se llegó a las siguientes conclusiones:

1. Se realizó la implementación de una topología de red en la cual se pudieron instalar y configurar las 3 suites, sin tener problemas de comunicación describiendo en cada caso, los pasos necesarios para su realización.
2. Se encontraron ventajas y desventajas en cada una de las 3 suites, y aunque todas tienen cosas en común (protocolos soportados y funcionalidades), cada una tiene un punto de vista único. Zimbra cuenta con una interfaz fácil de usar y funciones prácticas a un precio bajo. Por el contrario, Exchange ofrece un nivel extremo de seguridad y funciones avanzadas, lo que la convierte en una buena opción para empresas exigentes. Por su parte, Kopano abarca muchas funcionalidades y una interfaz muy amigable y consumo bajo de recursos.
3. Se realizaron pruebas de seguridad en tanto a la criptografía y uso de protocolos que permite que la información viaje de forma segura. Además, las tres cuentan con antivirus y antispam los cuales son obligatorios para el envío y recepción de correo electrónico.

Por lo cual podemos concluir que se realizó con éxito, una comparativa de las características y el rendimiento de las Suites de Correo Electrónico Open-Xchange, Zimbra y Kopano, ejecutadas en entornos virtuales. En nuestro país se cuentan con muchas MIPYMES que necesitan diversificar la forma como se comunican, para lo cual la suite más completa y económica sería Kopano, ya que permite tener un servicio de correo electrónico, videoconferencias y un sistema seguro con un bajo consumo de recursos.

7. Recomendaciones

1. Realizar estudios con otras suites de correo que existen en el mercado.
2. Emplear otros tipos de malware o virus para comprobar que día a día sus bases de datos de virus están actualizadas y que podrían proteger a los usuarios de las amenazas más actuales.
3. Implementar las suites en equipos físicos para obtener un mejor rendimiento en los procesos operativos.

8. Bibliografía

1. Binario, C. (12 de Julio de 2019). *Informática con corazón y bits*. Obtenido de Actualización automática de la fecha y la hora en un servidor Linux: https://corazonbinario.com/actualizacion-automatica-de-la-fecha-y-la-hora-en-un-servidor-linux/
1. BitTitan. (15 de Abril de 2021). *Resolver un problema IMAP/POP*. Obtenido de Acceso denegado: https://help-bittitan-com.translate.goog/hc/en-us/articles/115008100587-Access-Denied?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es-419&_x_tr_pto=sc
2. Castillo, J. A. (2018 de Diciembre de 10). *Profesional Review*. Obtenido de Cómo configurar servidor Telnet en Ubuntu o cualquier sistema Linux: https://www.profesionalreview.com/2018/12/10/configurar-servidor-telnet-ubuntu/
3. Herrero, H. (15 de Noviembre de 2018). *Blog Bujarra*. Obtenido de Integrando el correo en Nextcloud: https://www.bujarra.com/integrando-el-correo-en-nextcloud/
4. IBM. (2015). *WebSphere Service Registry and Repository*. Obtenido de Configuración de los valores de IMAP: https://www.ibm.com/docs/es/wsr-and-r/8.5.6?topic=notifier-configure-imap-settings
5. Kopano. (2016). *Kopano Documentation Portal*. Obtenido de Using Kopano Archiver: https://documentation.kopano.io/user_manual_kopanocore/archiver.html
6. Kopano. (2019). *Configuring Alternative Mail Clients*. Obtenido de Client configuration: https://documentation.kopano.io/user_manual_kopanocore/configure_alternative_mail_clients.html
7. Microsoft. (2020). *Soporte*. Obtenido de Configuración POP, IMAP y SMTP para Outlook.com: https://support.microsoft.com/es-es/office/configuraci%C3%B3n-pop-imap-y-smtp-para-outlook-com-d088b986-291d-42b8-9564-9c414e2aa040
8. Müehlenhoff. (21 de Agosto de 2017). *Univention*. Obtenido de Renewing the SSL certificates: https://help.univention.com/t/renewing-the-ssl-certificates/37
9. net, W. s. (2018). *Web set net*. Obtenido de Univention Corporate Server (UCS) como servidor principal: https://websetnet.net/es/using-univention-corporate-server-ucs-as-a-home-server/
10. Server, U. C. (2018). *Manual for users and administrators*. Obtenido de Manual for users and administrators: http://docs.software-univention.de/manual-4.2.html#installation:chapter
11. Severino, R. E. (14 de Abril de 2011). *Slideshre*. Obtenido de Instalar y configurar servidor de correo imap en ubuntu: https://es.slideshare.net/rqbert/instalar-y-configurar-servidor-de-correo-imap-en-ubuntu
12. Systems, O. (2019). *Collaboration services for every need*. Obtenido de https://www.omnis-systems.com/en/kopano-groupware/kopano-versions-en.

13. Timme, F. (2017). *How to forge*. Obtenido de Ubuntu/Postfix/Saslauthd - SASL authentication failure: cannot connect to saslauthd server: Permission denied: https://www.howtoforge.com/ubuntu-postfix-saslauthd-sasl-authentication-failure-cannot-connect-to-saslauthd-server-permission-denied
14. Wikipedia. (14 de Noviembre de 2021). *Kopano (software)*. Obtenido de Kopano Groupware Core: https://en.wikipedia.org/wiki/Kopano_(software)
15. Open-Xchange. (2020). Soporte. Installation and Administration Guide - Open-Xchange Software: https://www.yumpu.com/en/document/read/4935450/installation-and-administration-guide-open-xchange-software-
16. Univention Help. (2017). Soporte. Postfix smtp stopped after errata 49: https://help.univention.com/t/postfix-smtp-stopped-after-errata-49/5986
17. Open-Xchange. (2022). Soporte. Open-Xchange Installation Guide for Debian 10.0: https://oxpedia.org/wiki/index.php?title=AppSuite:OpenX-change_Installation_Guide_for_Debian_10.0

ANEXOS

Anexo 1. Configuración necesaria para el entorno

Para el correcto funcionamiento del entorno es necesario realizar las siguientes configuraciones entre el Router frontera y el Switch multicapa, el Router frontera es el que se encargara de realizar la traducción de ip publica a ip privada y viceversa implementando nat dinámico y estático, el Switch multicapa tendrá las siguientes funciones una de ellas es como servidor dhcp que será el que se encargue de asignarle ip a las distintas máquinas y servidores que estén dentro de dicha topología.

Una vez que tenemos nuestra ip publica en nuestra interfaz en el Router frontera se debe configurara la comunicación entre el Router y el Switch multicapa esto se hace configurando las ip entre las interfaces interconectadas y realizando pruebas de conexión

Ya que tengamos conexión a la puerta de enlace podremos seguir realizando las demás configuraciones para tener conexión hacia el exterior.

```
hostname R2

interface GigabitEthernet0/0

 ip address dhcp

 ip nat outside

 media-type gbic

 speed 1000

 duplex full

 negotiation auto
```

```
interface FastEthernet2/0
 ip address 10.8.0.2 255.255.255.252
 ip nat inside
 speed auto
 duplex auto

router rip
 version 2
 network 10.0.0.0
 network 195.100.40.0
 no auto-summary

ip nat inside source list 1 interface GigabitEthernet0/0 overload
ip nat inside source list 2 interface GigabitEthernet0/0 overload
ip nat inside source list 3 interface GigabitEthernet0/0 overload

access-list 1 permit 10.8.0.0 0.0.0.3
access-list 2 permit 172.100.1.0 0.0.0.255
access-list 3 permit 10.100.0.0 0.0.0.255
```

```
hostname swich-mutilayer

ip cef
no ip dhcp use vrf connected
ip dhcp excluded-address 10.100.0.1
ip dhcp excluded-address 172.100.1.1

ip dhcp pool clients1
  network 172.100.1.0 255.255.255.0
  default-router 172.100.1.1
  dns-server 10.100.0.10

ip dhcp pool mail1
  host 10.100.0.20 255.255.255.0
  hardware-address 0800.27dc.1647
  default-router 10.100.0.1
  dns-server 10.100.0.10

ip dhcp pool mail2
  host 10.100.0.10 255.255.255.0
  hardware-address 0800.2767.dfb2
  default-router 10.100.0.1

ip dhcp pool mail3
  host 10.100.0.30 255.255.255.0
  hardware-address 0800.27c4.6ad8
  default-router 10.100.0.1
```

```
interface FastEthernet0/0
 no switchport
 ip address 10.8.0.1 255.255.255.252

interface FastEthernet0/1
 no switchport
 ip address 172.100.1.1 255.255.255.0

interface FastEthernet0/2
 no switchport
 ip address 10.100.0.1 255.255.255.0
```

Anexo 2: Cronograma de actividades

Actividades	2021			
	Septiembre	Octubre	Noviembre	Diciembre
-Elección del Tema				
-Antecedentes				
-Planteamiento del problema				
-Justificación				
-Objetivos				
- Marco Teórico				
-Etapas del Proyecto				
-Anexos/Cronograma de actividades				

Actividades	2022-2023			
	Enero – Marzo	Mayo - Septiembre	Octubre - Diciembre	Agosto 2023
Análisis e Implementación de la topología.				
Organizar documento de tesis.				
Configuración de las Suites de Correo y entorno de trabajo				
Resolución de errores generales.				
Realización de primeras pruebas de conectividad y envió de correo.				
Análisis de tráfico, seguridad e integridad de los correos electrónicos				
Pruebas Finales				
Presentación de Proyecto Final.				