Universidad Nacional Autónoma de Nicaragua

UNAN-LEÓN

Facultad de Ciencias y Tecnología

Departamento de Computación

Instalación y Configuración de un Servidor de Correo Electrónico con Open-Xchange Server y sus protocolos con seguridad

(Propuesta para implementarse en el Departamento de Computación de la Unan-León.)

Tesis previa a optar al título de Ingeniero en Telemática

Presentado por

Br. Walter Francisco González Hernández.

Br. Roberto Leonel Martínez Báez.

Br. Róger Antonio Arteaga Sandoval.

Tutor

M.Sc. Valeria Mercedes Medina

León – Nicaragua 2012

DEDICATORIA

Br. Walter Francisco González Hernández.

Dedico este trabajo monográfico primeramente a Dios que me ha dado la vida y me permitido finalizarlo.

A mis padres Isabel Hernández y Francisco González por haberme brindado su confianza y su apoyo incondicional durante todas las etapas de mi vida, a mi esposa Ana Cano y a mi hijo Johan González que son Mí razón de Ser y a mis hermanos que me han apoyado siempre.

Br. Roberto Leonel Martínez Báez.

Mi tesis la dedico con todo mi amor y cariño a Dios, porque me dio la fe, 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 mis padres Leonel Martínez y Lisseth Báez quienes me dieron la vida y han estado con migo en todo momento a mis hermanos que han sido sostén y apoyo en mis esfuerzos de superación profesional a todas las personas que han creído en mí.

Br. Róger Antonio Arteaga Sandoval.

La presente tesis la dedico primeramente a Dios quien me ha dado la vida y sabiduría para finalizar este proyecto monográfico en esta etapa tan importante de mi vida encaminándome siempre por la senda del bien y en su infinito amor.

A mis padres Napoleón Arteaga y Marina Sandoval y a todos mis hermanos quienes han sido la motivación en mi vida brindándome su apoyo y aliento incondicional en todo momento para lograr cumplir mis metas y objetivos.

AGRADECIMIENTOS

Estamos profundamente agradecidos con Dios que nos a brindado la fuerza y conocimiento para llegar hasta el final de nuestro trabajo monográfico.

Estamos agradecidos por el gran apoyo incondicional, paciencia y dedicación que nos ha dado el Msc. Valeria Medina Rodríguez.

A todos los maestros del área de Ingeniería en Telemática del Departamento de Computación les agradecemos infinitamente por sus apoyo educativo donde nos formaron como futuros profesionales.

A nuestros padres por el apoyo incondicional que nos han brindado durante toda las etapas de nuestras vidas.

INDICE

ÍNDICE DE FIGURA

INDICE DE TABLA

I. INTRODUCCIÓN

En esta tesis se presentan los resultados obtenidos de la implementación de una Autoridad Certificadora auto-firmada que firme electrónicamente los certificados de los servicios que ofrecerán una comunicación segura en un servidor de correo electrónico

La ejecución de dicha implementación se realizara utilizando el sistema operativo Univention Corporate Server. La utilización del sistema nos permite definir sus características, ventajas, desventajas y otros aspectos importantes con respecto a la gestión del correo electrónico.

El desarrollo de la tesis proporciona un sistema de correo electrónico totalmente funcional y de alto rendimiento que use un completo abanico de modernas tecnologías y protocolos que mejoren su eficiencia, robustez, flexibilidad y seguridad. Así mismo se proporciona muchas facilidades de uso para los usuarios de este servicio.

II. ANTECEDENTES

El correo electrónico es una de las aplicaciones de internet más ampliamente utilizadas para el intercambio de información entre personas, empresas u organismos.

A partir del año actual (2012) en el departamento de computación se utiliza el servidor de correo electrónico facilitado por la UNAN-León que cumple con los aspectos de seguridad bajo una plataforma de software privado por lo cual debe ajustarse a políticas de servicio, para obtener el servicio la debilidad está en que la información se almacena en dispositivos que no son totalmente administrados por la UNAN-León lo cual da lugar a que la información pueda ser tratada por otras partes y genera un gasto monetario.

En el Departamento de computación de la UNAN-León existen dos trabajos investigativos relacionados con la instalación y configuración de un servidor de correo electrónico los cuales son:

- ✓ Configuración e instalación de un completo servidor de correo con postfix y cyrus (2006).
- ✓ Configuración de un servidor web y de correo electrónico en Red-Hat (2007).

Cabe destacar que estos trabajos se centran en la funcionalidad básica de un servidor de correo electrónico, sin tomar en cuenta aspectos básicos de la seguridad en este tipo de servicio.

III. JUSTIFICACIÓN

En la actualidad gran parte de las actividades de muchas entidades educativas se facilitan mediante el uso del correo electrónico permitiendo los siguientes propósitos:

- ✓ Distribución de información interna o externa.
- ✓ Comunicación entre directores, profesores y alumnos.
- ✓ Correspondencia con las diferentes áreas que forman parte de las entidades educativas.

La seguridad es otro aspecto fundamental del servicio de correo electrónico ya que a través de esta se garantiza la integridad, confidencialidad y autenticidad del mensaje cifrado en un canal de comunicación seguro.

Por esta razón la presente investigación tiene como finalidad la implementación de este servicio de una manera confiable utilizando protocolos seguros e implementando mecanismos y herramientas que nos proporcionen esta seguridad como son:

- ✓ Privacidad,
- ✓ Autenticidad,
- ✓ Integridad,
- ✓ Confidencialidad,
- ✓ Compresión,
- ✓ Fragmentación

Lo que garantizara la comunicación segura y eficiente entre las partes involucradas.

El presente proyecto de tesis se presenta como propuesta de implementación para el Departamento de Computación de la UNAN-León el cual será de mucha utilidad para el aprovechamiento de los recursos tecnológicos con que cuenta, ofreciendo integridad de los datos, autenticación de los miembros, la implantación de herramientas que nos permitan denegar los Spam y virus, además la implementación de este servicio con herramientas de software libre tendrá un bajo coste económico.

IV. OBJETIVOS

OBJETIVO GENERAL

- Instalar y Configurar un servidor de correo electrónico seguro con Open-Xchange Server, como propuesta de implementación en el departamento de computación de la Unan-León.

OBJETIVOS ESPECIFICOS

- Utilizar la herramienta o plataforma de Univention Corporate Server para la implementación del servidor de correo electrónico y sus protocolos con seguridad

- Aplicar herramientas de seguridad asociados a la configuración de un correo electrónico y sus protocolos con seguridad.

- Implementar mecanismos para rechazar los Spam y Virus en el servidor de correo electrónico.

V. MARCO TEORICO

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.

1.1. 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 envió 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.

1.2. Agente

Fig. 1 Agentes en una comunicación de correo electrónico.

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 (MS Outlook, Lotus Notes, Thunderbird, etc.).

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

1.3. Elementos del servicio de correo electrónico

1.3.1. 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.

1.3.2. Agente de Transferencia del correo (MTA)

Un Agente de Transporte de Correo (MTA) transfiere mensajes de correo electrónico entre hosts usando SMTP. Un mensaje puede involucrar varios MTAs a medida que este se mueve hasta llegar a su destino.

Aunque la entrega de mensajes entre máquinas puede parecer bien simple, el proceso completo de decidir si un MTA particular puede o debería aceptar un mensaje para ser repartido, es más bien complicado. Además, debido a los problemas de spam, el uso de un MTA particular está usualmente restringido por la configuración del MTA o por la configuración de acceso a la red en la que reside el MTA.

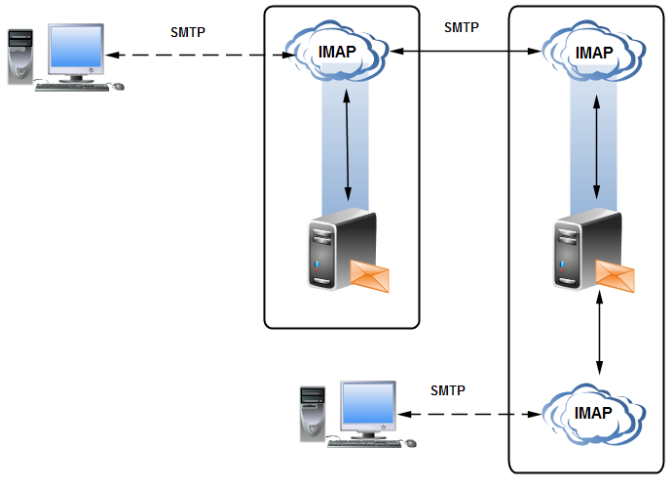


Fig. 2 Agente MTA.

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.

1.3.3. Agente de Entrega de Correo (MDA)

Un MTA invoca a un Agente de entrega de correos (MDA) para archivar el correo entrante en el buzón de correo del usuario. En muchos casos, el MDA es en realidad un Agente de entregas local (LDA), tal como mail o Procmail. Cualquier programa que maneje la entrega de mensajes hasta el punto en que puede ser leído por una aplicación cliente de correos se puede considerar un MDA. Por esta razón, algunos MTAs (tales como Sendmail y Postfix) pueden tener el papel de un MDA cuando ellos anexan nuevos mensajes de correo al archivo spool de correo del usuario.

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.

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.

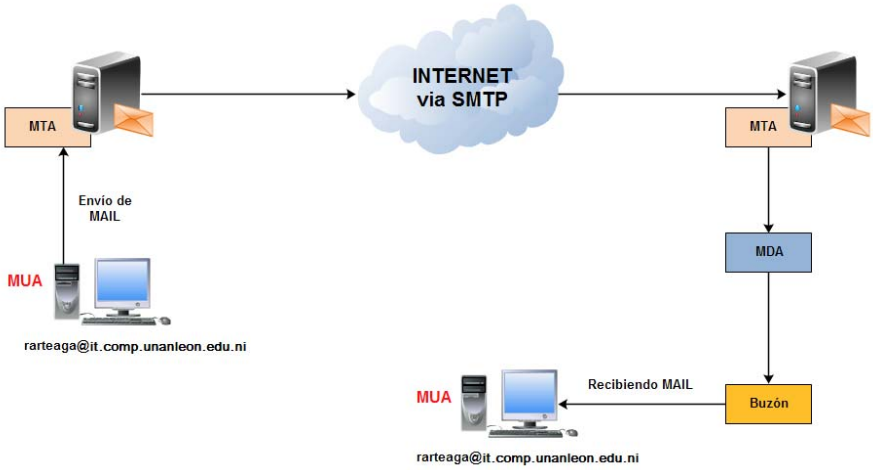


Fig. 3 Agente MDA

1.3.4. Agente de Usuario de Correo (MUA)

Un agente de usuario de correo (MUA) es sinónimo con una aplicación cliente de correo. Un MUA es un programa que, al menos les permite a los usuarios leer y redactar mensajes de correo. Muchos MUAs son capaces de recuperar mensajes a través de los protocolos POP o IMAP, configurando los buzones de correo para almacenar mensajes y enviando los mensajes salientes a un MTA.

Características.

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

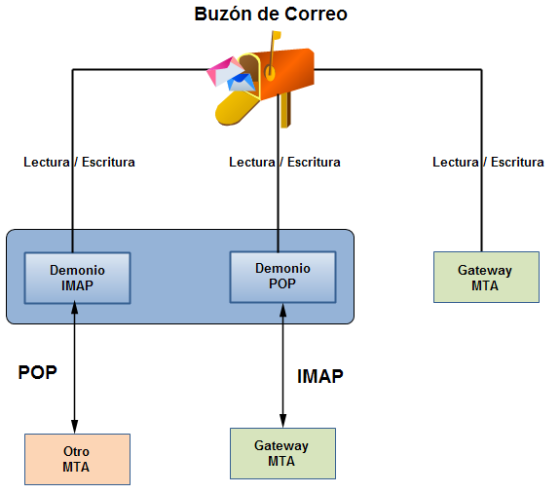


Fig. 4 ***Agenta MUA***

1.3.5. 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.

1.4. 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).

1.4.1. Protocolo Simple de Transferencia de Correo (SMTP)

El servidor SMTP de email no se ejecuta como un demonio de ejecución permanente. Un programa auxiliar, como por ejemplo inetd, xinetd, o tcpserver se ejecuta como demonio. Cuando recibe una conexión TCP en el puerto 25, el puerto SMTP, ejecuta una copia de qmail-smtpd.

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

1. Acepta un mensaje entrante.
2. Comprueba las direcciones del mensaje.
3. Si son direcciones locales, almacena el mensaje para recuperarlo.
4. Si son direcciones remotas, envía el mensaje.
5. 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 5 se muestra como trabaja el protocolo IMAP en combinación con el SMTP, para la gestión del correo.

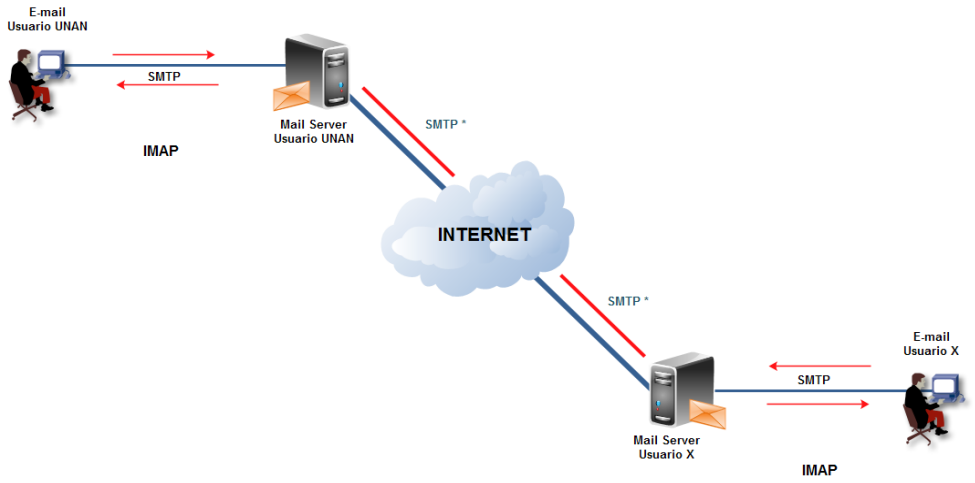


Fig. 5 ***SMTP trabajando con el IMAP.***

1.4.2. 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 Proveedor*) 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 a como se muestra en la figura 6.

Fig. 6 ISPs del mail Server.

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 conjuntamente 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 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.

1.4.3. 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.

Ventajas IMAP

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

1.4.4. X.400

Es un estándar conforme al Modelo de interconexión de sistemas abiertos OSI, para el intercambio de correo electrónico (por entonces se llamaban Mensajes Interpersonales o IPMs) desarrollado por el ITU-T (por entonces llamado CCITT) con el beneplácito del ISO desde el año 1984.

Como le pasó a la mayor parte de los estándares OSI del Nivel de aplicación no soportó la competencia con el protocolo similar Internet, en este caso el SMTP. El correo X.400 llegó a tener una base de usuarios relativamente amplia, especialmente en Europa, sobre todo en entornos corporativos y de investigación. El modelo de correo era más robusto y completo que el equivalente de Internet. Su sistema de direcciones de correo, basado en X.500, era demasiado complicado para la época, aunque muchísimo más potente. Como

todos los estándares OSI, este era el recomendado/soportado por las compañías telefónicas (por la época y en Europa casi todas eran monopolios estatales) que ofertaban unas tarifas de conexión excesivas. Un poco por todo ello el estándar OSI no tuvo gran aceptación. No obstante aún se usa el correo X.400 en algunas aplicaciones sectoriales que requieran mayor seguridad e integridad (como aplicaciones militares).

1.4.5. 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 a 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.

1.5. 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

1.6. 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.

Es usual que se cuente con un mecanismo de autentificación de quién origina el mensaje y privacidad para los datos. Además, de proveer un esquema de recepción firmada desde el recipiente. En núcleo de estas capacidades en el uso de la tecnología de llave pública y el uso a gran escala de llaves públicas, lo que requiere un método de certificación que dada una llave pertenece a un usuario dado. Aunque, se ofrecen servicios parecidos al usuario final, los dos protocolos tienen formatos distintos. Adicionalmente, y esto es importante a los usuarios corporativos, en este caso se cuenta con diversos formatos para los certificados. Lo que significa, que no sólo los usuarios no pueden comunicarse con los que usen otro, además, no pueden compartir los certificados de autenticación.

La diferencia entre los dos protocolos es parecida a la diferencia entre los formatos GIF y JPEG, siendo que hacen las mismas cosas, más no su formato entre ellos. 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.

1.6.1. Criptografía

La criptografía comprende toda una familia de tecnologías que incluyen las siguientes: Encriptación. Transforma la información en una forma no legible asegurando la privacidad.

Descifrar. Es el inverso de la encriptación; es decir, transforma la información encriptado 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.

1.6.2. 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.

1.6.3. 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".

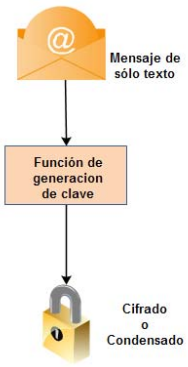


Fig. 7 ***Función Hash***

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

Los algoritmos hash más utilizados son:

MD5 (*MD* que significa *Message Digest; en castellano, Resumen de mensaje*), el MD5 crea, a partir de un texto cuyo tamaño es elegido al azar, una huella digital de 128 bits procesándola en bloques de 512 bits. Es común observar documentos descargados de Internet que vienen acompañados por archivos MD5: este es el hash del documento que hace posible verificar su integridad.

SHA (*Secure Hash Algorithm; en castellano, Algoritmo Hash Seguro*) crea una huella digital que tiene 160 bits de longitud. SHA-1 es una versión mejorada de SHA que data de 1994. Produce una huella digital de 160 bits a partir de un mensaje que tiene una longitud máxima de 2^{64} bits y los procesa en bloques de 512 bits.

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.

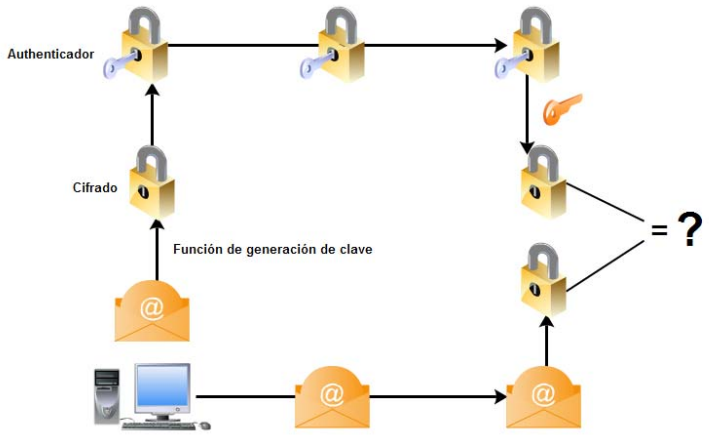


Fig. 8 Cifrado de Mensaje

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.

1.6.4. 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.

1.6.4.1 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.

1.6.4.2. 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 a las necesidades de la aplicación. Los Nombres Distintivos están definidos en el estándar X.509, así como por las necesidades de la aplicación.

1.6.4.3. 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.

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	
	SSL Plus - Proteger un 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.coopacidigital	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	
Thawte	SSL123 Certificates	$149	1 Año	128-bit a 256-bit
	SSL Web Server Certificates	$249	1 Año	
	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-bit y 128- o 256-bit de cifrado SSL
	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-Leon	Autoridad Certificadora Autofirmada	11 Año	Gratis
	VeriSing Class 3 EV	2 Año	$1000/$1500
UNI	Autoridad Certificadora Autofirmada	10 Año	Gratis
UCA	Zimbra Collaboration Suite	1 Año	Gratis
UNAN-Managua	Go.Daddy	2 Año	$69.99/$89.99
Banco Central de Nicaragua	Trustwave Organization Validation CA	3 Año	$149/$1199
Asamblea Nacional	Zimbra Collaboration Suite	10 Año	Gratis

Tab. 2 Certificados Digitales utilizados por entidades Nacionales

2. 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).

2.1. ¿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.

2.2. 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 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.

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.

2.3. 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.

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 hots, 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.

1. 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**.

2. Comandos

Algunos comandos de **Postfix** más interesantes:

newaliases: Actualiza la base de datos de las 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. 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.

MTA	Desarrollo	Seguridad	Características	Rendimiento	CompSendMail	Modular
QMail	Normal	Alta	Altas	Alto	Complementos	Si
SendMail	Alto	Baja	Altas	Bajo	X	No
Postfix	Bajo	Alta	Normales	Alto	Si	Si
Exim	Normal	Baja	Altas	Normal	SI	No

Tab. 3 Comparación con otros MTA (Agentes de Transporte de correo).

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. CYRUS

Es un sistema de mail diseñado principalmente para entornos de empresas o similares.
Es altamente escalable y con un buen rendimiento. Implementa varios estándares, como IMAP y POP.

3.1 Cyrus IMAP

Cyrus IMAP (Internet Message Access Protocol) es desarrollado y mantenido por el Andrew Systems Group de la Carnegie Mellon University.

A diferencia de otros servidores IMAP, Cyrus usa su propio método para almacenar el correo de los usuarios. Cada mensaje es almacenado en su propio fichero. El beneficio de usar ficheros separados es una mayor fiabilidad ya que sólo un mensaje se pierde en caso de error del sistema de ficheros. Los metadatos, tales como el estado de un mensaje (leído, etc.) se almacenan en una base de datos. Además, los mensajes son indexados

para mejorar el rendimiento de Cyrus, especialmente con muchos usuarios e ingentes cantidades de mensajes. No hay nada tan rápido como el servidor IMAP Cyrus.

3.2 Cyrus SASL

SASL son las siglas de Simple Authentication and Security Layer, un método para añadir soporte para la autenticación a protocolos basados en la conexión que ha sido estandarizado por la IETF (Internet Engineering Task Force). Se usa en servidores (en este caso Cyrus IMAP) para manejar las peticiones de autenticación de los clientes. Para ello, el protocolo incluye un comando para identificar y autenticar un usuario contra un servidor y para, opcionalmente, negociar la protección de las subsiguientes interacciones del protocolo. Si se negocia su uso, una capa de seguridad es añadida entre el protocolo y la conexión.

4. 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.

4.1. 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.

4.2. 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 de 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 inter operar 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.

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 server 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 server, 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 server 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 server para autenticarlo. Si el server no puede ser autenticado, se le avisa del problema al usuario y se le informa que no se puede establecer una conexión cifranda y autenticada con ese server. Si el server 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 server, 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 el cliente 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.

5. 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.

6. 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 via (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.

7. 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 via 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.

8. 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.

9. Herramientas de Seguridad

9.1. 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 válido.

Verificar que el documento ha sido firmado por una determinada persona.

9.2. 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.

9.3. Manejo de Certificados digitales

Un certificado digital es un contenedor de datos que alberga identidades (por ejemplo de una persona, sus nombre, dirección e mail) 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.

9.4. 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.

9.5. Accesibilidad

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

10. OPEN-XCHANGE

Es un sistema de mensajería diseñado para pequeñas y grandes empresas es una nueva plataforma de gran alcance de colaboración y trabajo en grupo. Aumenta la productividad a través de trabajo en equipo, reduce costos y tiene máxima flexibilidad técnica. Existen dos versiones de este producto: la versión comercial (software propietario) y la versión open-source (software libre).

Groupware se refiere a los programas informáticos que integran el trabajo de un proyecto con muchos usuarios concurrentes que se encuentran en diversas localizaciones o estaciones de trabajo, típicamente conectadas a través de la red Internet o de una intranet.

10.1. Características

Open-Xchange es una plataforma web rentable 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.

10.2. Funcionamiento Orientado

Open-xchange es un substituto del alto rendimiento y bajo costo para la plataforma Exchange de Microsoft. Con una funcionalidad completa de una plataforma madura de la colaboración. OX maneja no solamente citas y tareas, también el e-mail, los calendarios, los contactos, los proyectos, los documentos, búsqueda y foros. Con OX, usted puede manejar la información usando los favoritos que se enlazan a una variedad amplia de objetos de datos, tales como e-mail, hojas de cálculo o presentaciones. Si necesita consolidar las comunicaciones de su empresa, OPEN-XCHANGE le ofrece todo.

OX permite que usted conecte con Microsoft Outlook y los dispositivos Palm usando los conectores. De acuerdo con las tecnologías más avanzadas le ofrece una seguridad de la mejor clase contra virus y Spam. La arquitectura abierta de OX le ofrece la flexibilidad de configurar el software para ajustarlo a su infraestructura y proteja su inversión a largo plazo.

OX está testeado en diferentes escenarios y por miles de usuarios en todo el mundo y es la inspiración de centenares de programadores que hacen subir como la espuma toda la comunidad de software libre. Toda esta energía y entrega mejora continuamente el producto, asegurando todas las expectativas de desarrollo.

Open-Xchange Server soporta:

- Dispositivos SyncML.
- Cualquier navegador.
- Microsoft Outlook y Microsoft Outlook Express gracias al Outlook OXtender. Se trata de un software que permite que el outlook interactué con el servidor Open-Xchange Server como si fuera un Microsoft Exchange Server.
- WebDav interfaz (XML), LDAP, iCal, HTTP(S), SMTP, IMAP, POP3 y SyncML.

10.3. OXtenders e integración

El desarrollo de Open-Xchange se fundamenta en estándares como WebDAV y XML. Contiene modulo anti-spam y una API para JAVA. Otras características del software OX son:

- E-mail, colaboración y mensajería instantánea.
- Vista de equipo y funcionalidades de calendario y gestión de proyecto.
- Soporte para el intercambio de datos con ERP, CRM y aplicaciones Microsoft Office.
- Diferentes niveles de permisos y propiedad.

- Colocación flexible de frames.
- Configuración de atajos de teclado individuales.
- Carpetas públicas.
- Creación de las plantillas de la vista.
- Apariencia personalizable.

10.4. Beneficios

- Aumenta la productividad y disminuye el coste total de la propiedad.
- Una seguridad más robusta.
- Una comunicación más rápida.
- Incremento en la flexibilidad e interoperabilidad.
- Interfaz mucho más sencilla y amigable.

10.5. Módulos al Open-Xchange

Portal.

El módulo de entrada a Open-Xchange constituye un intento de poner a disposición del usuario un resumen de lo ocurrido durante los últimos días y el trabajo previsto para el día de hoy y los venideros. Incluye citas, tareas y correos electrónicos, ordenados por tipo de datos, todo en una única página, muy fácil de leer. Todas las alertas y cabeceras sirven como enlaces a documentos, adjuntos y datos. Muy útil al llegar por la mañana a la oficina.

Calendario.

El módulo de calendario simplifica la coordinación de reuniones en grandes grupos de trabajo. El estado de libre/ocupado muestra la disponibilidad de todos los participantes así como los recursos, como salas de reuniones y conferencias o proyectores. Open-Xchange

es capaz de calcular la ventana de disponibilidad más próxima para los miembros de tu equipo basándose en los parámetros que se elijan.

Todos los participantes, tanto si sin empleados como contactos, recibirán una invitación de manera automática si así se desea. Los miembros del equipo pueden aceptar o rechazar la petición de reunión. Usando la vista del equipo puede obtenerse una vista de todas las entradas del calendario de su equipo en un día en particular con la información relevante enlazada.

Contactos.

El módulo de contactos de Open-Xchange es la solución a todos estos dilemas. Una libreta de direcciones global, contactos internos y externos relacionados con cada proyecto y contactos privados de acceso restringido. Todos los tipos de contactos pueden manejarse usando las categorías. Y, lo mejor de todo, los contactos pueden enlazarse basándose en la relación que tienen contigo.

Tareas.

El módulo de tareas de Open-Xchange puede ayudarnos a gestionar un equipo, a tener una vista de las reuniones y los participantes necesarios para lograr un hito (del inglés, milestone). Nos permite tener acceso a un montón de listas muy útiles: listas de proyectos, listas de tareas, etc. Esto nos permitirá organizarnos y priorizar nuestro trabajo. Además, podremos enlazar o adjuntar documentos a las tareas.

Proyectos.

Es una herramienta de gestión de proyectos que le permite a los miembros del equipo acceder a la información que necesitan para llevar a cabo sus tareas. Hoy en día, casi todas las empresas enfatizan muchísimo el trabajo en equipo. Un equipo bien gestionado es altamente productivo y ayuda a la empresa a mejorar su posición de mercado.

Pero a menudo es difícil organizar y gestionar un equipo. El software específico que promete automatizar la gestión de un proyecto a menudo no cumple las expectativas

porque es complicado y difícil de aprender y usar. Lo que realmente se necesita es un módulo de proyectos que todo el mundo pueda usar porque haya sido diseñado para ser intuitivo.

Una herramienta de gestión de proyectos que permita a la gente acceder a la información que necesitan para su trabajo, tanto si esa información se encuentra en un correo electrónico, como en un evento del calendario, documento o mensaje de foro. Una plataforma que consigue que la información no se duplique y esté centralizada.

Documentos.

Open-Xchange proporciona la parte más importante de una gestión de documentos, pues se concentra en aquellas características que nos permiten trabajar más rápido, incluso en grandes volúmenes de datos. Tanto si se trata de un control automático de versiones como si hay que bloquear un documento mientras se están editando, o si se trata de recuperar rápidamente un documento, Open-Xchange permite trabajar con los documentos usando herramientas comunes y de manera intuitiva. Además, nos permite acceder a documentos que necesitamos a través de Internet rápidamente y con seguridad, pues incluye un sistema de permisos.

Conocimiento.

No todos en su empresa utilizarán las características avanzadas de estos módulos, pero es bueno saber que están ahí. Bases del conocimiento, marcadores globales, foros internos y boletines de noticias son algunos de los componentes avanzados de Open-Xchange, para que construya su sistema de colaboración empresarial de acuerdo a su compañía.

Open-Xchange puede ser un catalizador para crear una cultura de innovación, pues une las herramientas necesarias y las pone en las manos de los empleados, quienes las usarán para desarrollar, difundir y publicar sus ideas.

Favoritos.

Permite visualizar las listas de sus favoritos de una manera ordenada a través de un árbol de directorio de fácil manejo. Esto le permitirá también editar, mover, borrar de una manera más sencilla.

Foro.

Para ver y participar en el Foro institucional.

Tablero.

Funciona como un “Periódico Mural Virtual” por área y de domino Público.

E-Mail.

Esta opción le permitirá ingresar al su casilla de correo.

VI. *METODOLOGIA*.

1. Diseño metodológico.

- Recopilación de información.
- Instalación de Sistema Operativo.
- Configuración de los servicios que integran un Servidor de Correo Electrónico con sus protocolos seguros.
- Configuración y Administración de Open-Xchange Server.
- Análisis de Comunicación Segura.

2. Recursos a Software.

- Sistema Operativo Open Source: Univention Corporate Server 2.4-4 basado en el núcleo de la distribución Debian GNU/Linux.
- Paquetería software (Open-Xchange Server, Postfix, Cyrus, Bind9, OpenSSL, etc)

3. Recursos Hardware.

- PC Escritorio con Hardware interno:
- Disco duro SATA 150 GB.
- Memoria RAM 2 GB.
- Procesador Intel Atom Duo 1.7 GHz.

VII. DESARROLLO E IMPLEMENTACION

1. Sistema Operativo implementado

Univention Corporate Server (UCS) es un sistema operativo basado en el núcleo de la distribución Debían GNU/Linux, la distribución de UCS implementada es la versión 2.4-4

UCS se compone de tres elementos principales:

- UCS sistema base
- Univention Sistema de Gestion
- UCS componentes

El Sistema de Gestion Univention proporciona una administración en la totalidad de las cuentas, los miembros del dominio (usuarios, grupos y hosts) y servicios como DHCP y DNS son administrados dentro de un servicio de directorio, para esto el sistema hace uso de la norma OpenLDAP y componentes Kerberos;

Proporciona los componentes de OpenSSL y del servicio de DNS ya que están incluidos en el asiendo que sea más extensible y dependiendo de la versión del sistema UCS se incorporan más paquetes que enriquecen el funcionamiento como un servidor maestro proporcionando una solución flexible sobre cualquier arquitectura cliente-servidor.

Los componentes de UCS tienen como objetivo ampliar el sistema con funciones tales como la infraestructura de cliente ligero, servicios de terminal, trabajo en grupo o en un servicio de Windows, todos los cuales integran el Sistema de Gestión de Univention.

UCS permite no solo una gestión sencilla y cómoda de servicios individuales, sino también la administración de los regímenes de permisos complejos de grandes organizaciones en varios sitios con muchos servidores y clientes y decenas de miles de usuarios. Su diseño modular ofrece muchas interfaces de ampliación y modificación.

En general UCS es un sistema operativo diseñado para aplicaciones multi-usuario y multi-tarea desde el principio, donde la atención se centró siempre en la estabilidad, la seguridad y la compatibilidad con otros sistemas operativos. Ya que Linux está

predestinado para ser utilizado en entornos complejos, sin embargo, la gestión de sistemas Linux solía ser considerada como difícil y lejos de ser cómodo. Este es el punto donde entra UCS

2. Instalación y Configuración del SO

La instalación y configuración del sistema aborda las fases más importantes para obtener los componentes deseados de los servicios que se implementan de igual forma se indica los aspectos sobre el acceso de los servicios que ofrece el sistema mediante las herramientas de administración de UCS

2.2 Selección de la función del sistema

Los siguientes están disponibles para elegir:

- Maestro de controlador de dominio
- Controlador de dominio de copia de seguridad
- Slave controlador de dominio
- Miembro servidor
- Base del sistema

El primer sistema para instalarse en un dominio UCS siempre debe ser un controlador de dominio principal. La instalación de nuevos sistemas de UCS requiere un controlador principal de dominio el cual es buscado automáticamente por medio de la red, al detectar un sistema controlador principal va a permitir elegir entre los diferentes roles del sistema en la instalación. La única excepción a esto es el sistema de base que se puede instalar sin una conexión a un controlador de dominio principal. (Ver **fig. 9**)

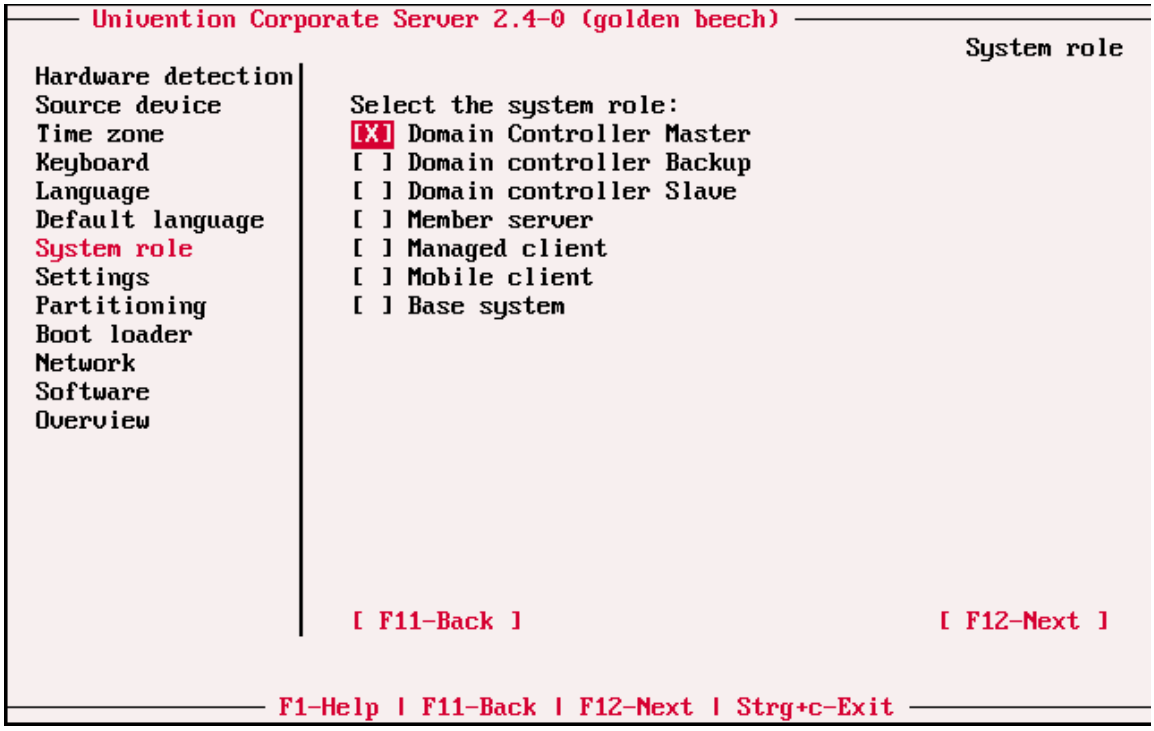


Fig. 9 Funcion del sistema

2.3 Configuración de dominio

Donde se establece el nombre de domino completo (FQDN) del sistema en la que el equipo debe ser accesible en la red por ejemplo mail.ejemplo.com.

El nombre del dominio se establece en el campo LDAP que es derivado del nombre de domino completo. El campo de entrada de LDAP aparece únicamente en el funcionamiento del sistema maestro.

La contraseña de **root** es la contraseña para el controlador de domino maestro que está instalado, esta contraseña también se introdujo para el usuario **Administrator** que es el usuario creado por el sistema en la instalación y configuración del sistema.

En el funcionamiento posterior el usuario **Administrator** puede gestionar de forma independiente en la administración superior y completa de todo el sistema como usuario **root**.

En la **fig. 10** la configuración para el servidor en desarrollo.

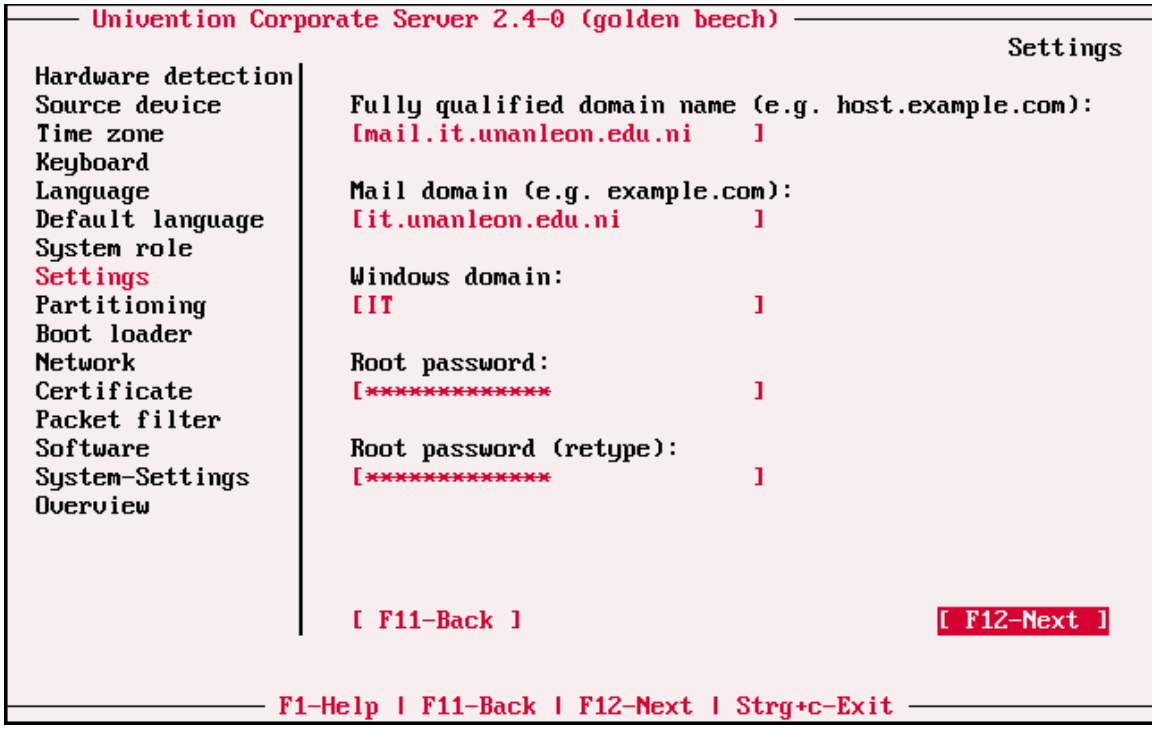


Fig. 10 Configuración del Dominio

2.4 Configuración de red

La configuración de la red muestra todas las tarjetas de redes disponibles en el sistema como una ficha individual (solo interfaces de red con el sistema ethX se muestran). Si no se detecta tarjeta de red el instalador crea una tarjeta de red virtual que puede ser utilizado para seguir la instalación. Las interfaces de red se pueden configurar para IPv4 y IPv6.

Configuración de direcciones IPv4

Si la opción DHCP no fue elegido, la dirección IP para ser vinculado a la tarjeta de red debe ser introducida. Además la máscara de red también se debe introducir.

Configuración de direcciones IPv6

La dirección IPv6 puede ser configurado de dos maneras:

Autoconfiguración de direcciones sin estado. (SLAAC) se emplea en la configuración dinámica, es decir la IP se genera automáticamente a partir de los anuncios de enrutador enviados desde los router IPv6

Como alternativa la dirección también se puede configurar estáticamente mediante la introducción de la dirección IPv6 y IPv4. En contraste con DHCP, en SLAAC no hay sección de datos adicionales como DNS. Existe un protocolo adicional para este (DHCPv6) que sin embargo no se emplea en la asignación dinámica

Otros ajustes de red se pueden realizar en configuración de red global. Las direcciones IP de las puertas de enlace estándar en la subred se pueden introducir en IPv4 puerta de enlace y Gateway IPv4. Para IPv6 una puerta de enlace debe ser introducido en la configuración estática, pues la configuración dinámica es opcional.

Una puerta de enlace configurada aquí tiene preferencia sobre anuncios de enrutador que de otro modo podrá ser capaz de cambiar la ruta.

Hay dos tipos de servidores DNS

Un servidor DNS externo se emplea para la resolución de nombre de host y direcciones fuera del dominio de UCS. Un servidor de dominio DNS es un servidor de nombres local en el dominio UCS solo administra nombre de host y direcciones IP que pertenecen al dominio UCS, si una dirección no se encuentra en el inventario local un servidor DNS externo es automáticamente solicitado. Los datos del DNS se guardan en los servicios de directorio LDAP, es decir todos los servidores de dominio DNS entregan los mismos datos

Durante la instalación de un controlador de dominio principal solo un servidor DNS externo se solicita. Un servidor DNS local también está configurado en el controlador de dominio de copia de seguridad y sistema de esclavitud respectivamente aquí puede configurar que servidor DNS debe ser utilizado principalmente para la resolución de nombres.

En la configuración de red del servidor se utiliza el DHCP de forma dinámica. (Ver **fig. 11**)

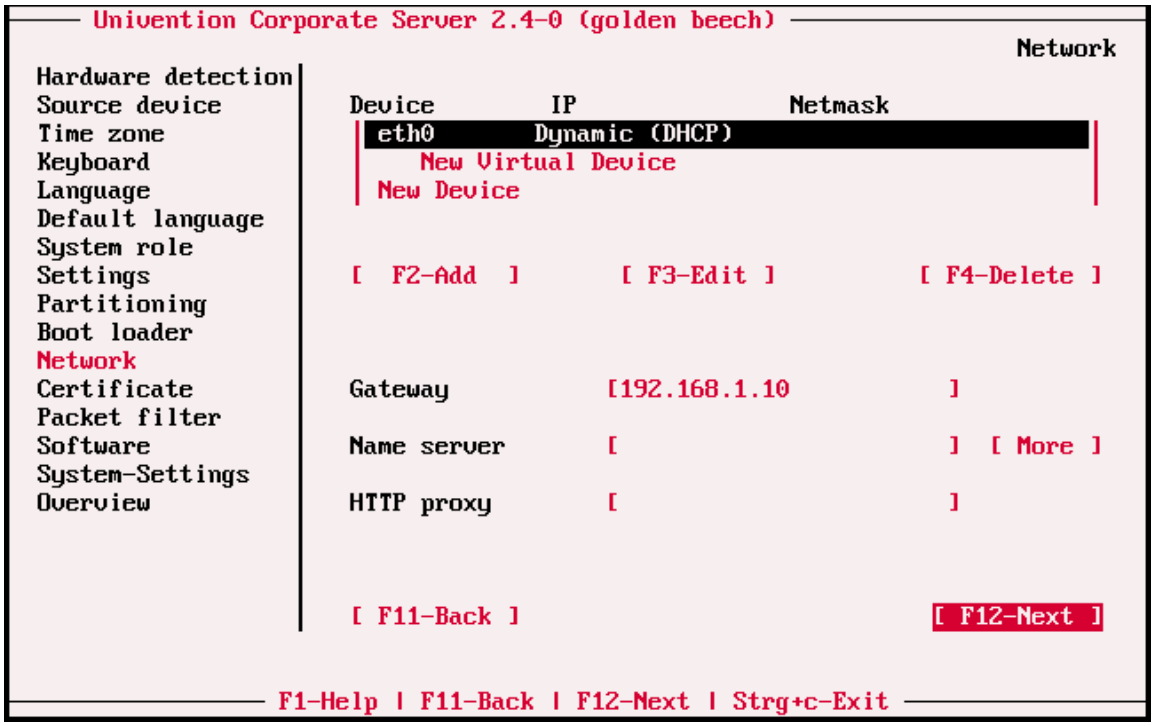


Fig. 11 Configuración de Red por DHCP

2.5 Certificado SSL

Su infraestructura es administrada en un servidor maestro de UCS controlador de dominio. Los certificados se utilizan por el UCS en el sistema de autenticación mutua y para el certificado de las conexiones de red.

En los datos de la creación de la autoridad certificadora auto firmada se encentra:

El campo Código del País de 2 caracteres del nombre del país de acuerdo con la norma ISO 3166-1 debe introducirse, por ejemplo NI para Nicaragua, el campo Estado federal o provincia, el campo Ciudad de ubicación de la empresa, el campo Nombre de Departamento. La dirección del correo electrónico se creara a partir del nombre de

dominio. Esta información será utilizada en la infraestructura de este certificado. (Ver **fig. 12**)

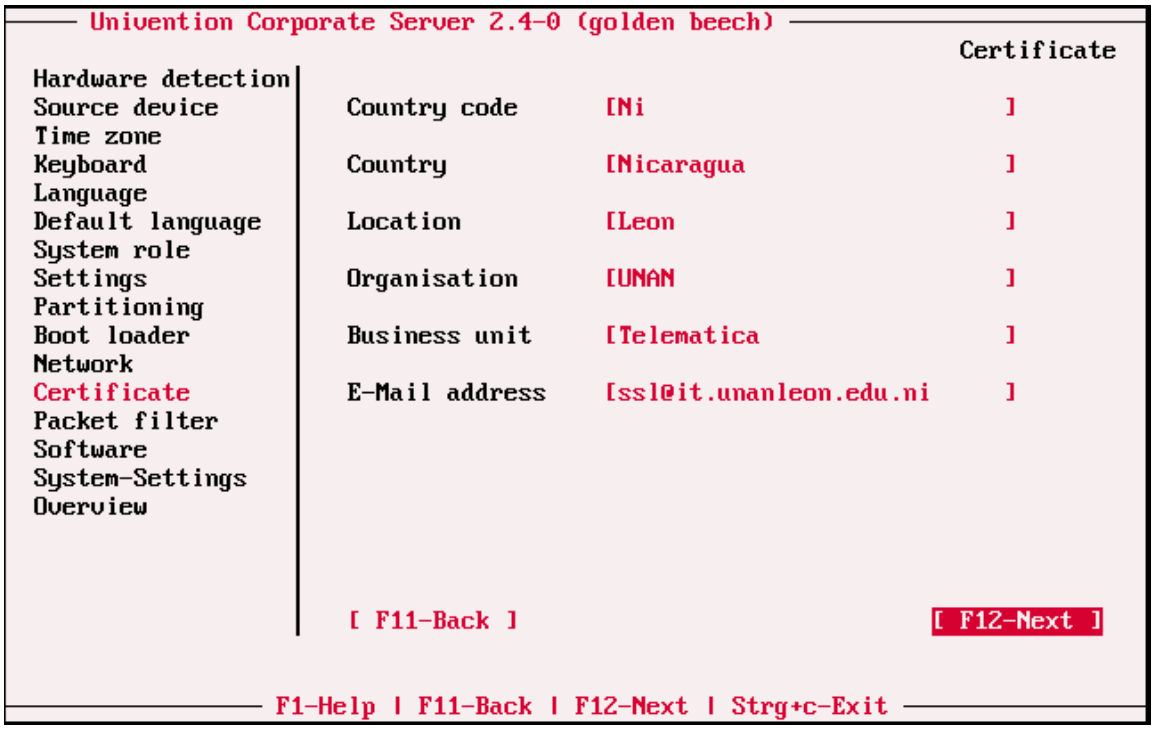


Fig. 12 Creación de la Autoridad Certificadora

2.6. Filtrado de Paquetes

En las opciones de seguridad el instalador de Univention permite pre-configurar los perfiles de paquetes de filtros que son los siguientes:

- Desactivado (no hay servicio y serán bloqueado para dar un funcionamiento de un host ordinario)
- Selección típica de servicios (típicamente algunos servicios innecesarios serán filtrados, dependiendo de la versión del sistema a instalar se encuentra un mejor equipaje de paquetes)
- Bloqueado de instalación. Solo SSH, HTTPS y LDAP están permitidos

En la instalación del servidor se utiliza la selección típica de los servicios para identificar qué servicios serán instalados y cuáles no como ilustra la **fig. 13**.

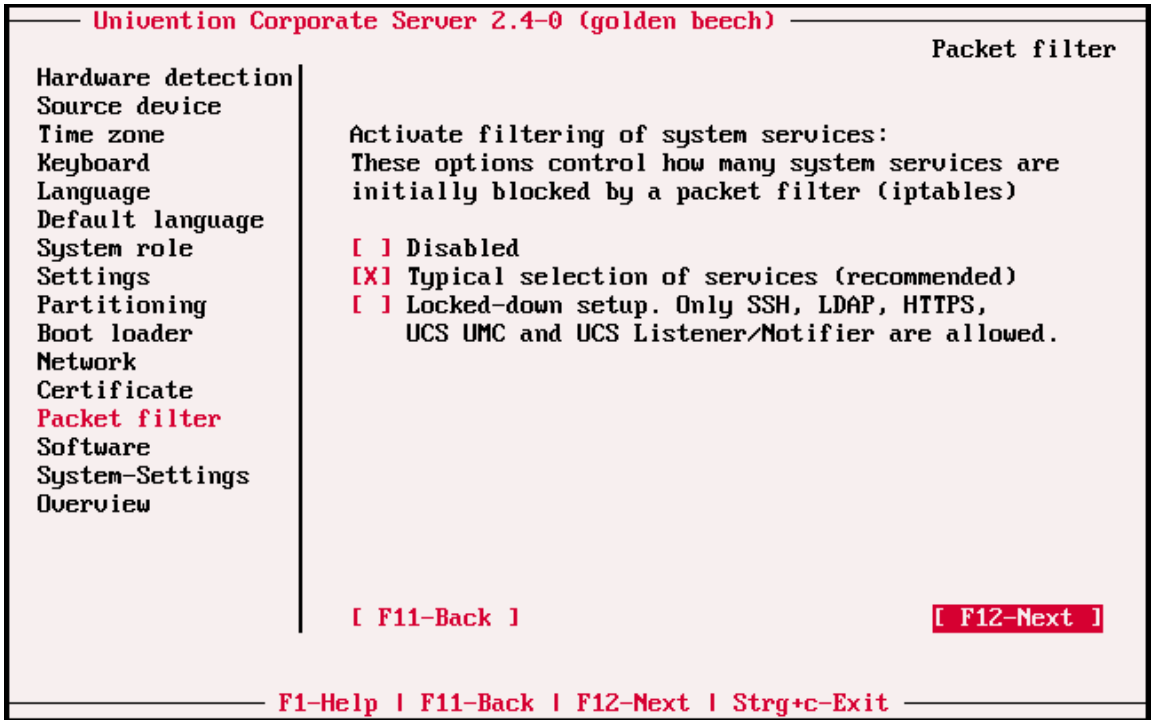


Fig. 13 Paquetes de servicios

2.7. Selección de los componentes de software

Los componentes son paquetes de software que están conectados entre sí en cuanto al contenido y se puede instalar para proporcionar una variedad de servicios. Componentes pueden consistir en varios subcomponentes. Los subcomponentes pueden instalarse individualmente, o todos juntos.

Los servicios del sistema

(1) Conector de Univention AD – Solución para la sincronización bidireccional de los servicio de directorio y Active Directory

(2) Backup (Bacula) – solución de copia de seguridad empresarial

(3) Open-Xcahnge – webmail ()

(4) Samba PDC en NO-DC Master – esta opción permite el funcionamiento de un PDC de Windows. Estableciendo como controlador de dominio al sistema.

(5) OpenSSH server – servidor para proporcionar un cifrado de inicio de sesión SSH remoto

En la siguiente **fig. 14** se encuentran los servicios del sistema utilizados

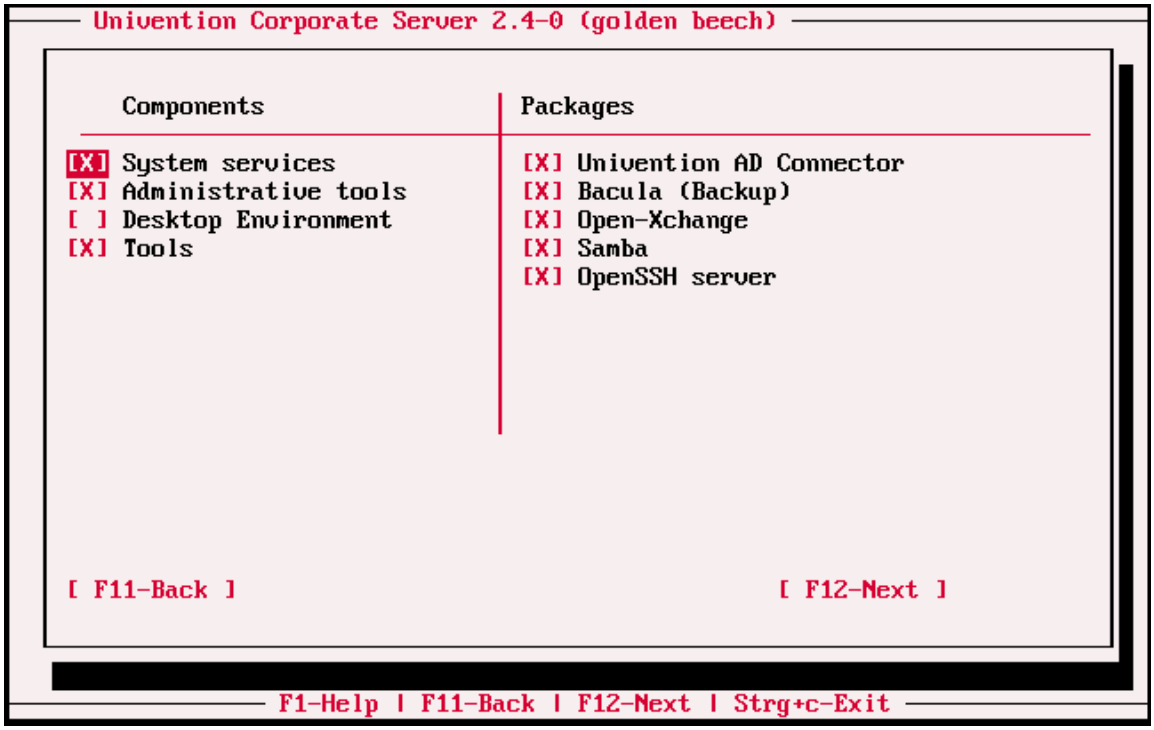


Fig. 14 Servicios del sistema

2.8. Las herramientas administrativas

Univention Directory Manager - componente central de gestión del sistema UCS

Univention Management Console - administración de sistemas UCS a través de una interfaz web.

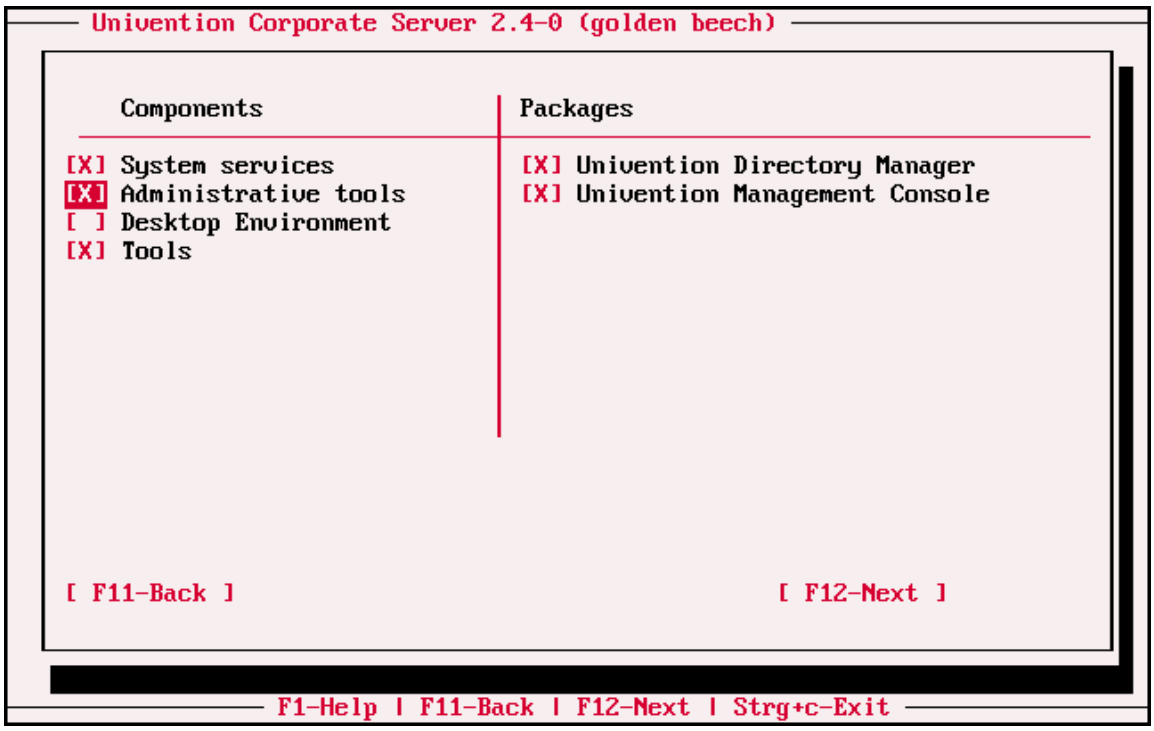


Fig. 15 Herramientas de administración

2.9. Entorno de escritorio

Interfaz gráfica de usuario - X.org infraestructura y gestor de ingreso GDM.

Escritorio KDE - Un entorno de escritorio fácil de usar.

Mozilla Firefox - un web browser.

- Java plugin / tiempo de ejecución - Java integración para el navegador Firefox.
- Plugin Flash - Una instalación del programa para integrar el plugin de Flash en Firefox

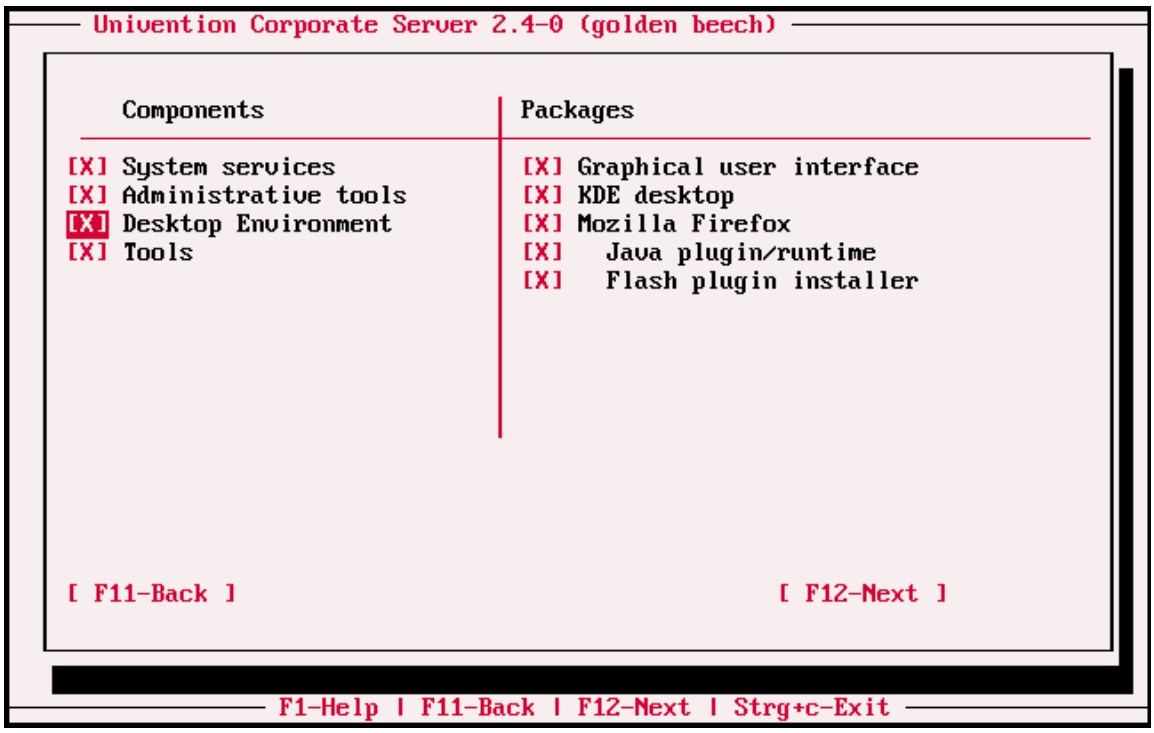


Fig. 16 Componentes de la Interfaz Grafica

2.10. Herramientas

Java - The Sun Java Runtime Environment

Herramientas de Línea de comandos - El editores vim y emacs, la herramienta menos para visualizar el texto, el texto basado en navegador web elinks, el nmap puerto de escáner, la compresión zip y herramientas unzip, la herramienta de descarga wget y expulsión para el script de apertura controlada de una unidad de DVD. (Ver la **fig. 17** siguiente).

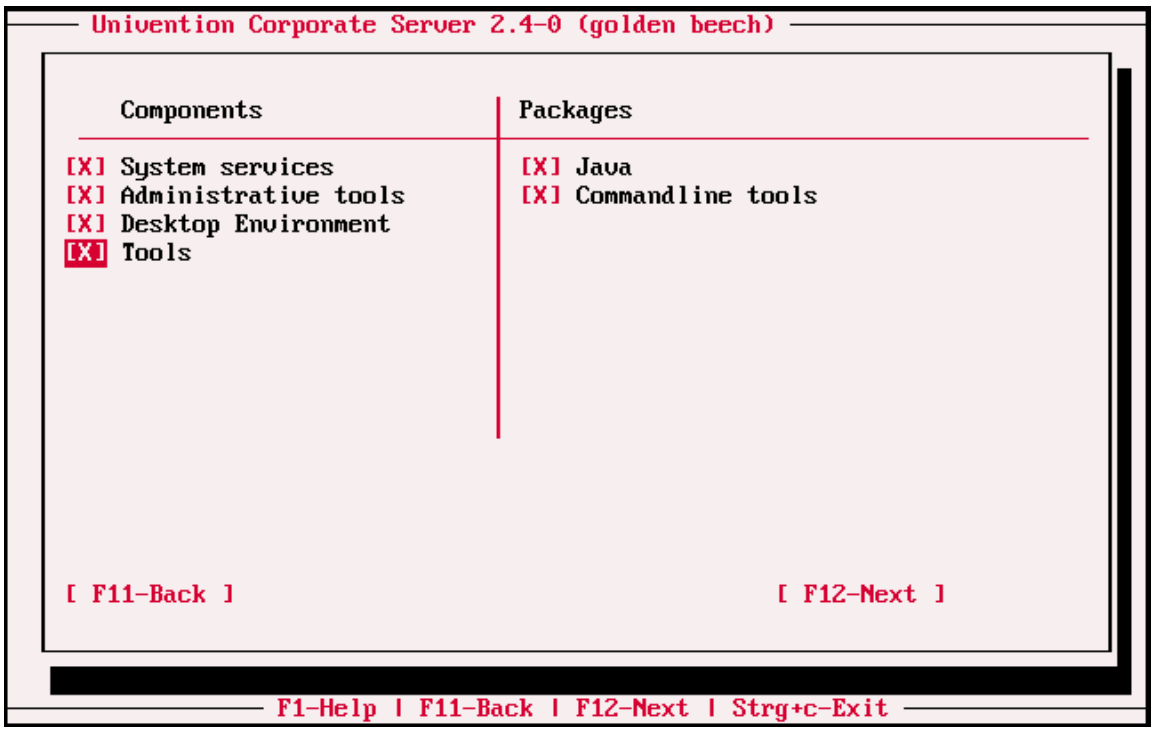


Fig. 17 Herramientas

2.11. Configuración del sistema

En la **fig. 18** se puede especificar si un repositorio de software local debe estar configurado en la UCS sistema. El sistema local de UCS y otros sistemas UCS pueden utilizar este repositorio de software para instalaciones y actualizaciones. Un repositorio de software también es necesario para las instalaciones basadas en red. La creación de auto cuota especifica si el directorio / home es para ser compartido a través de NFS y en caso de que los Servicios de componente de Windows está instalado como el directorio de usuario a través de Samba.

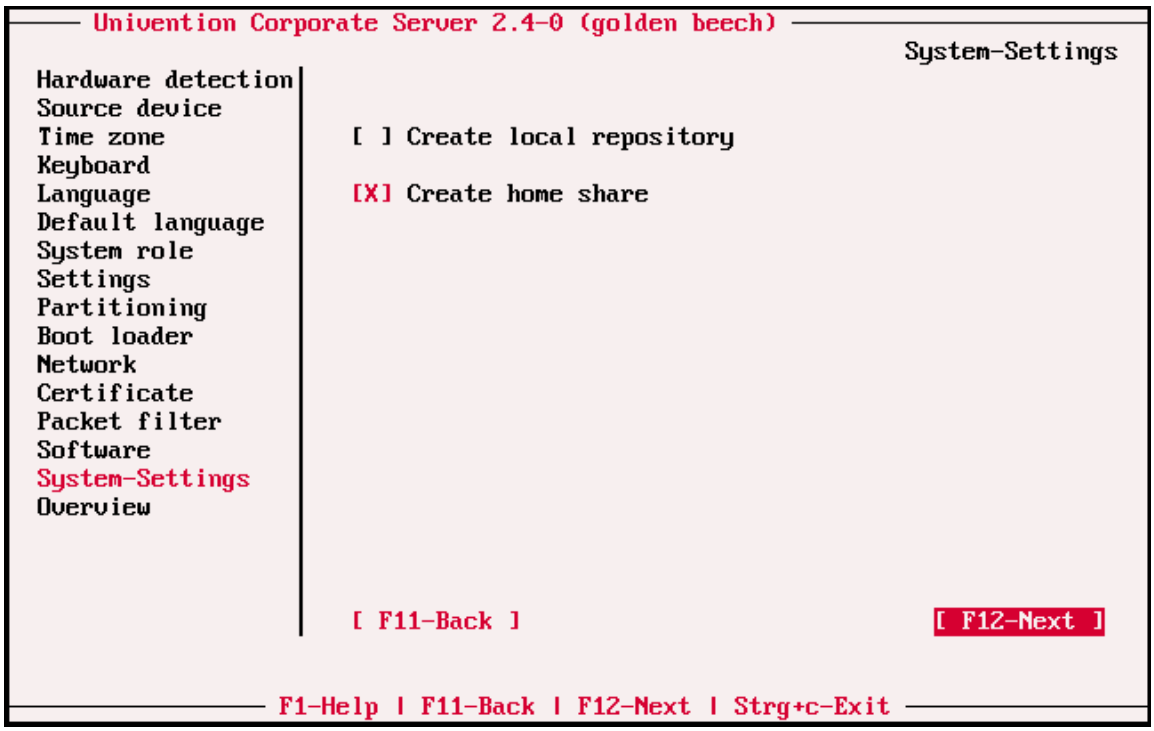


Fig. 18 Cuotas para los directorios del sistema

2.12. Visión de conjunto

Esta **fig. 19** muestra los valores de red y el nombre de domino que se ha establecido en la instalación y configuración del sistema.

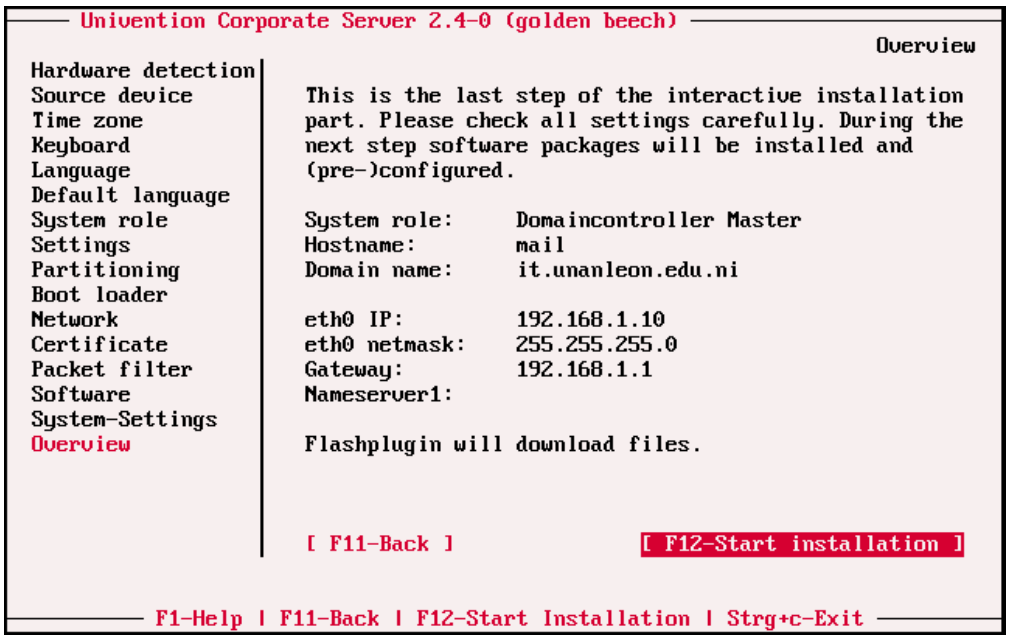


Fig. 19 configuraciones establecidas

La **fig. 20** se muestra datos importantes sobre cómo acceder a las interfaces de administración y configuración del sistema que serán de mucho interés para los administradores.

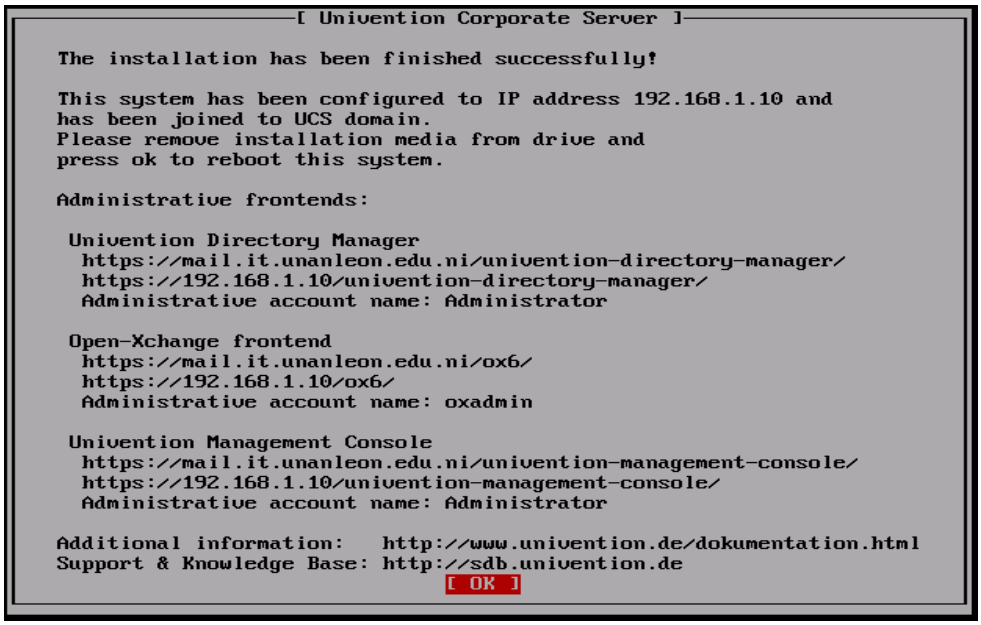


Fig. 20 Instalación finalizada y configuraciones de administración

El usuario **root** o **Administrador** puede iniciar sesión con la contraseña declarada durante la instalación. Ahora se encuentra el sistema UCS corriendo en el ordenador, en la **fig. 21** se muestra la interfaz del sistema.

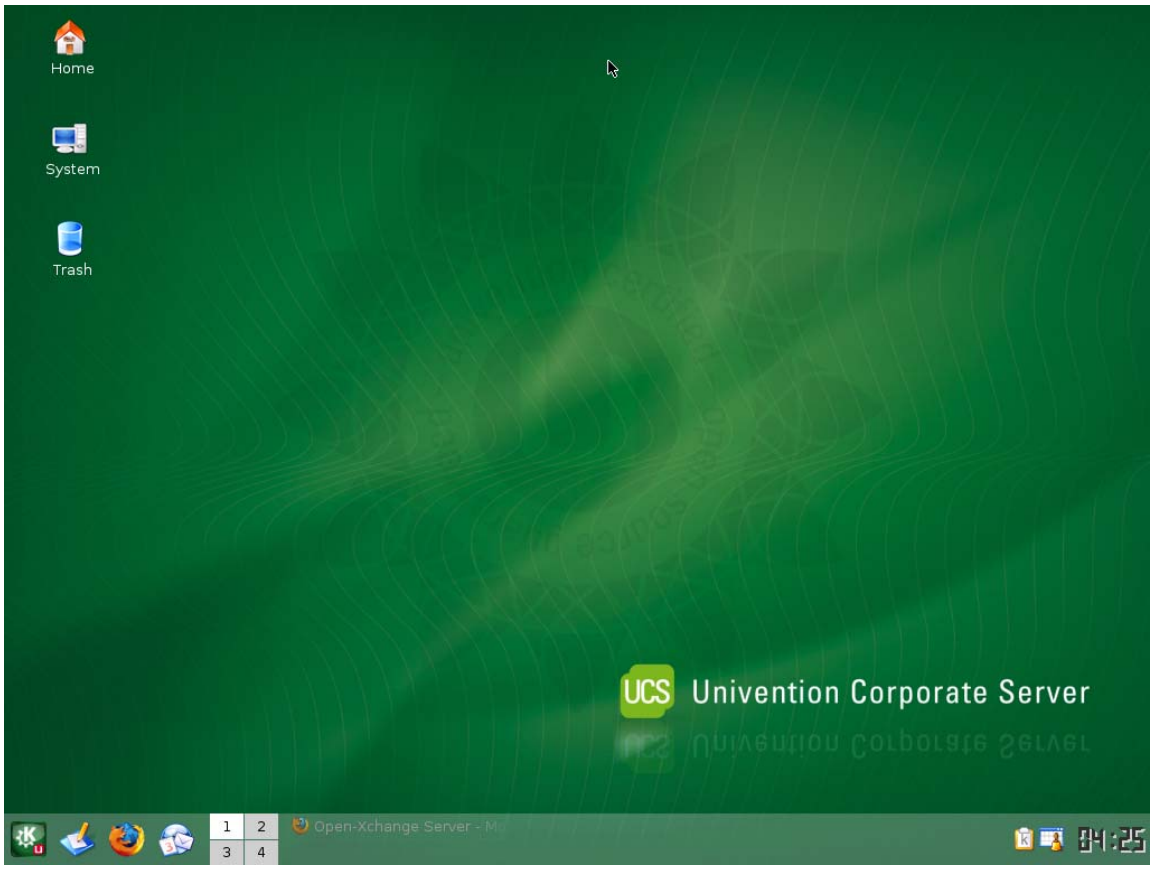


Fig. 21 Interfaz del sistema UCS

3. Configuración y administración del Web Mail Open-Xchange Server

Open Xchange Server proporciona a los administradores web la posibilidad de gestionar el aspecto y las características disponibles en la interfaz de usuarios para ajustar el nivel de la habilidad de cada usuario y grupos de sistemas permitiendo el control sobre el contenido de la edición y visualización de los privilegios. Todo en el WebGUI de Open-Xchange Server es una plantilla que permite la personalización, manteniendo el contenido del sitio y el estilo independiente.

De manera local para entrar a la interfaz web del controlador de dominio maestro de correos Domain controller Master mail con Open-Xchange se accede mediante: **http://Direcion-IP-del-Servidor/usc-overview/** (Ver la **fig. 22**) en el navegador también es posible acceder con **http://Nombre-del-Servidor.nombre-del-dominio/usc-overview /** si la resolución de nombre es configurada correctamente.

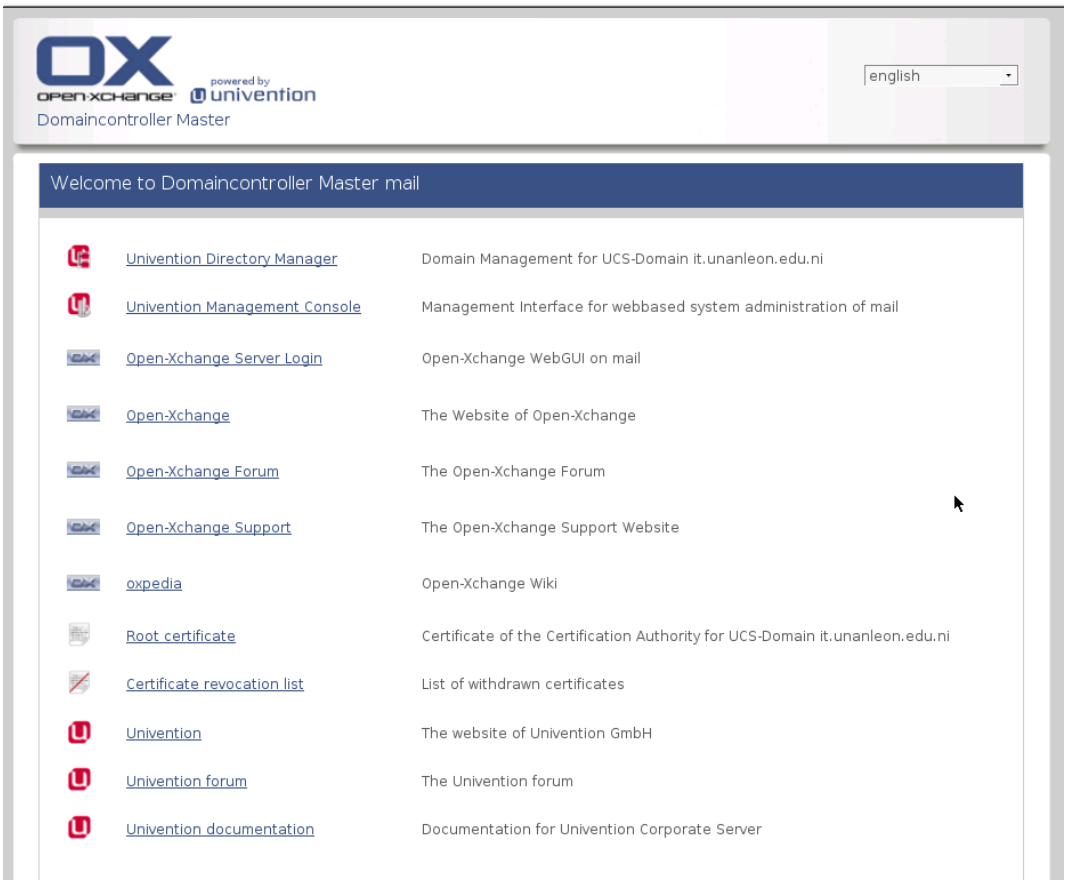


Fig. 22 Domain Controller Master mail

El directorio de administración de Open-Xchange permite una cómoda gestión de los objetos de un directorio LDAP. Los objetos pueden ser por ejemplo, los usuarios, grupos, equipos o entradas de DHCP junto con el directorio de Univention

Open-Xchange utiliza JavaScript y CSS en las funciones para visualizar la superficie de la interfaz web lo que puede causar problemas de visualización en algunos navegadores.

Para la administración se utiliza el usuario **Administrator** y la contraseña especificada para el usuario **root** en la instalación del UCS.

4.1 Creación gestión de cuentas de usuario

Dependiendo de la licencia e instalación utilizada (existen otras versiones de UCS), los asistentes que se muestran pueden variar y constar con más herramientas que mejorar y enriquecen el sistema, en este trabajo se utiliza una versión libre y de licencia gratuita, la **fig. 23** muestra la interfaz.

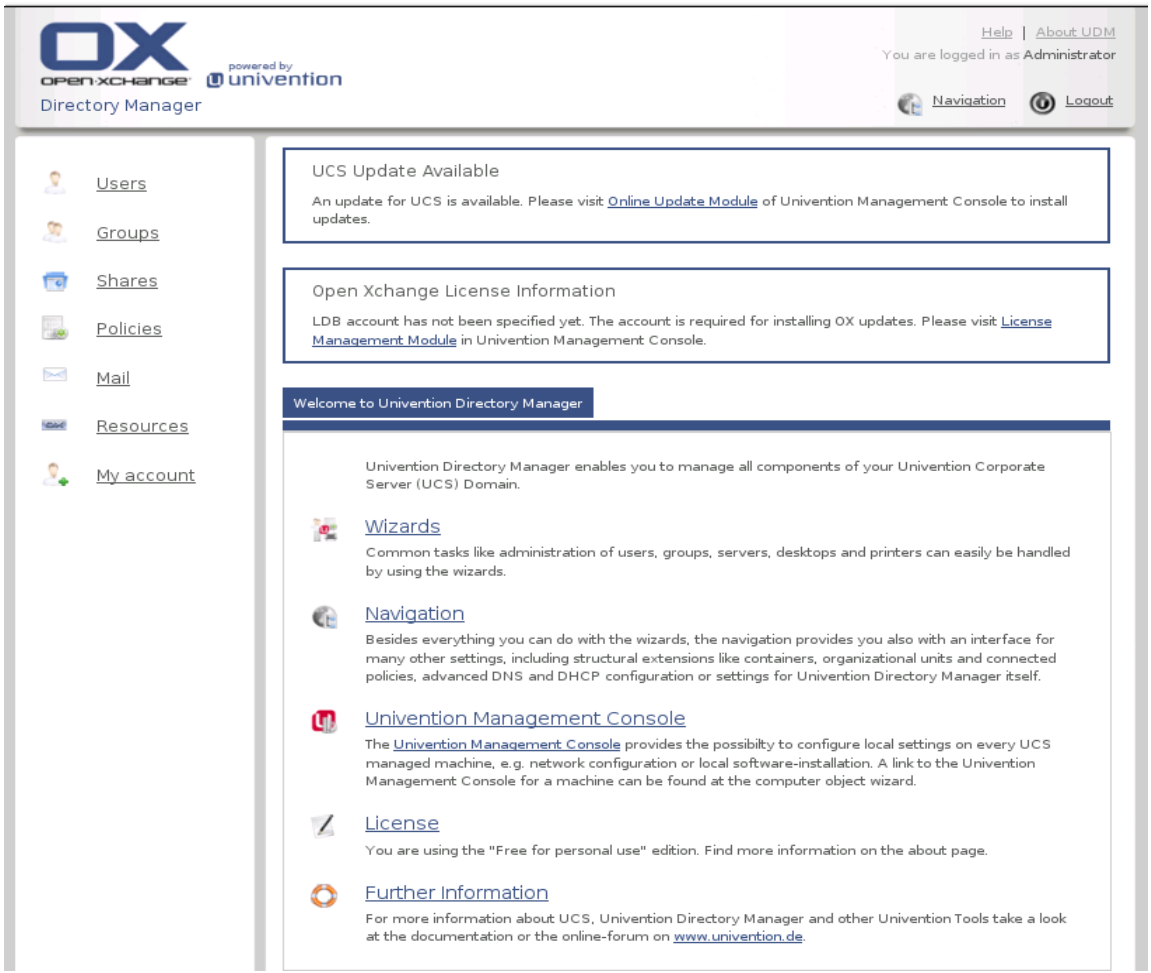


Fig. 23 Interfaz de Administración de cuentas y grupos de correos

Para continuar en la configuración y administración del web mail se crearan los usuarios que tendrán su correo bajo el dominio que se ha creado desde la instalación. Desde la pestaña **User** del menú principal.

Ahora se muestran los usuarios creados por el sistema desde su instalación y configuración (**Véase fig. 24**) donde se encuentran usuarios de manejo y prueba como lo es el usuario **oxadmin** y súper usuario **Administrator**, al iniciar sesión con alguno de estos usuarios creados por el sistema se utilizara la contraseña establecida en la instalación y configuración del sistema UCS.

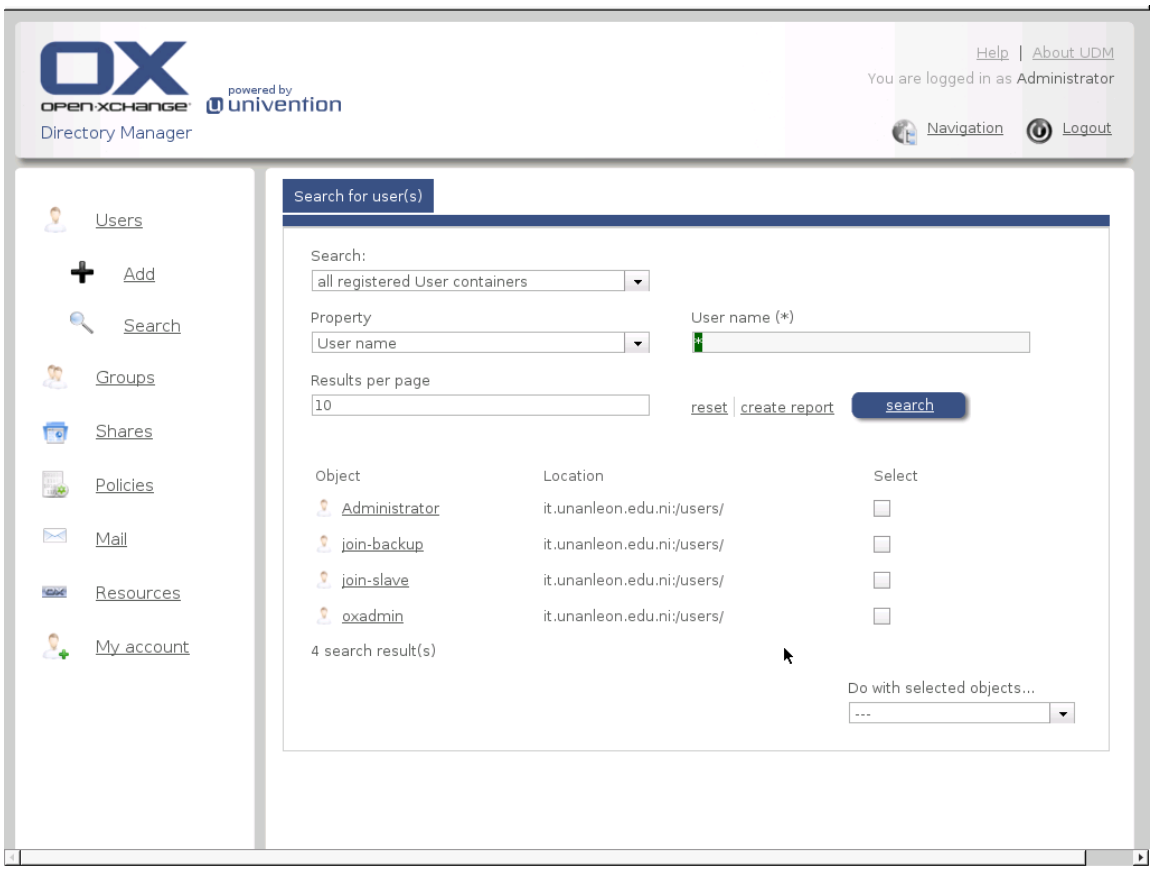


Fig. 24 Lista de usuarios del sistema

En la creación de usuarios que poseerán un correo electrónico bajo el dominio establecido en la configuración del servidor, la interfaz de administración Open-

Xchenge Server presenta un fácil manejo intuitivo en la creación de usuarios y grupos así como otros aspectos en la configuración y administración.

Generalmente se suele tener un solo domino en el servidor pero se encuentran opciones antes de crear el usuario están por el caso de que puede haber uno o más dominós configurados en el servidor.

En la siguiente **fig. 25** se tiene el panel de creación y configuración de los usuarios de correo electrónico y también se pueden crear usuarios administradores para el sistema.

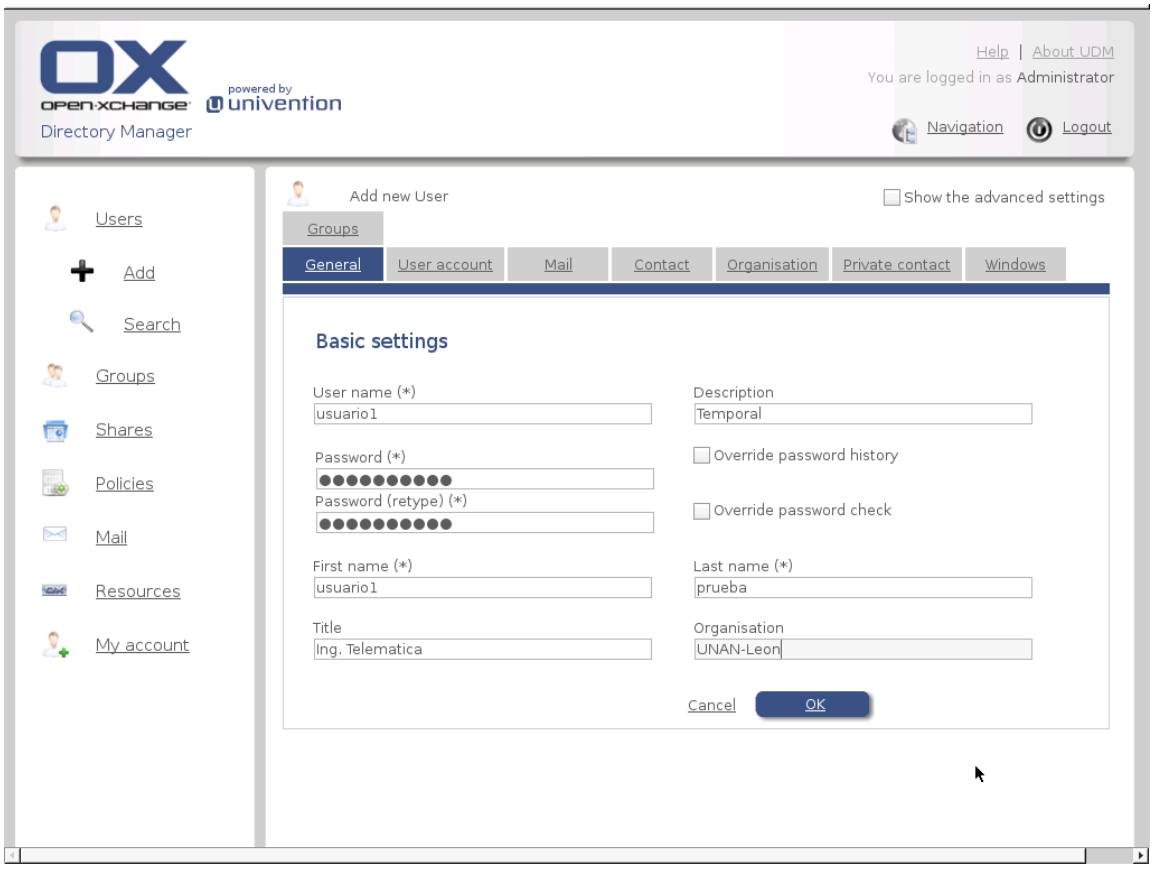


Fig. 25 Creación de Usuarios

Open-Xchange server ofrece más opciones de configuración para cada una de las cuentas de los usuarios como las siguientes:

User account: (Cuenta de usuario) aquí se encuentra el control de la cuenta del correo electrónico como su fecha de caducidad, la fecha por defecto no es válida. A partir de la fecha que se especifique en este campo un usuario que intente iniciar sesión en el sistema será notificado que su cuenta de usuario fue validada y ya no tiene acceso al sistema, esto puede cambiar si la fecha se actualiza o se elimina para que el usuario recupere el derecho de iniciar sesión.

También la contraseña tiene una fecha de caducidad que puede ser configurada y se puede indicar que en una fecha determinada influido por esa casilla de verificación cambiar la contraseña en un próximo inicio de sesión. Si la fecha de caducidad de la contraseña se alcanza o se excede se le pregunta al usuario su va a cambiar su contraseña y así podrá recuperar su acceso al sistema. Si un valor es declarado para el intervalo de caducidad de contraseña en la ficha políticas o si el valor es heredado a partir de un objeto de nivel superior, entonces la fecha de expiración se ajusta automáticamente una vez que el usuario ha cambiado su contraseña. La nueva fecha de caducidad se calcula por la fecha en que se cambió la contraseña además del valor declarado en el campo intervalo de caducidad.

Mail: la principal dirección de correo electrónico del usuario se declara aquí. Otras direcciones también pueden ser declaradas aquí para el usuario. Los E-mail dirigido a este correo serán entregados a la misma bandeja de entrada como los correos enviados al correo principal.

Contact: los datos relativos al número de teléfono, calle ciudad, código postal se almacenan en los atributos del domicilio social dentro del directorio LDAP.

Organization: esta pestaña contiene los números para los miembros del personal, también se puede establecer la categoría del miembro del personal e introducir información sobre la ubicación del personal dentro de un edificio de trabajo u otro.

Private contact: en esta pestaña se guarda información de algún contacto de interés para el usuario.

Windows: esta pestaña se utiliza para la configuración de la cuenta del usuario de Windows. Los valores estándar de Samba se utilizan para los campos vacíos en la configuración. La ruta del directorio que va a ser para los usuarios de Windows se

introducen por ejemplo **\\usc-file-server\nombre-usuario** también pueden ser almacenados en una unidad que puede ser especificada.

El Windows script login: inicio de sesión específica la secuencia de comandos para el recurso compartido Netlogon por el usuario se introduce en esta pestaña por ejemplo scripts\user.bat. El directorio de perfiles de usuarios de Windows también se introduce por ejemplo **\\ucs-file-server\user\profile**. En la identificación relativa (RID) es la parte del SID local, si un usuario se le debe asignar un cierto RID o ID si no se asigna RID automáticamente se le asignara uno secuencialmente. El RID no puede ser cambiado posteriormente. Los números enteros a partir de 1000 están permitidos para declarar un RID debajo de 1000 están reservados grupos estándar y otros objetos especiales

en el campo **Allow the authntication only on these Windows** se especifican los usuarios que pueden iniciar sesión si no se indican el usuario puede iniciar sesión.

Groups: esta pestaña tiene el propósito de definir la pertenencia a grupos de usuario si no se ha hecho la selección de grupo para el usuario su grupo será el principal. También se puede especificar el grupo primario para el usuario. Si el grupo principal de un usuario se ha eliminado por una modificación LDAP externa, el grupo predeterminado se asignara al objeto del usuario.

También se encuentra un panel avanzado de configuración que cuenta con más opciones como: **Contact other, Passwords, Mail quota, Univention Directory Manager View, UMC Access, Options,** se muestra en la **fig. 26.**

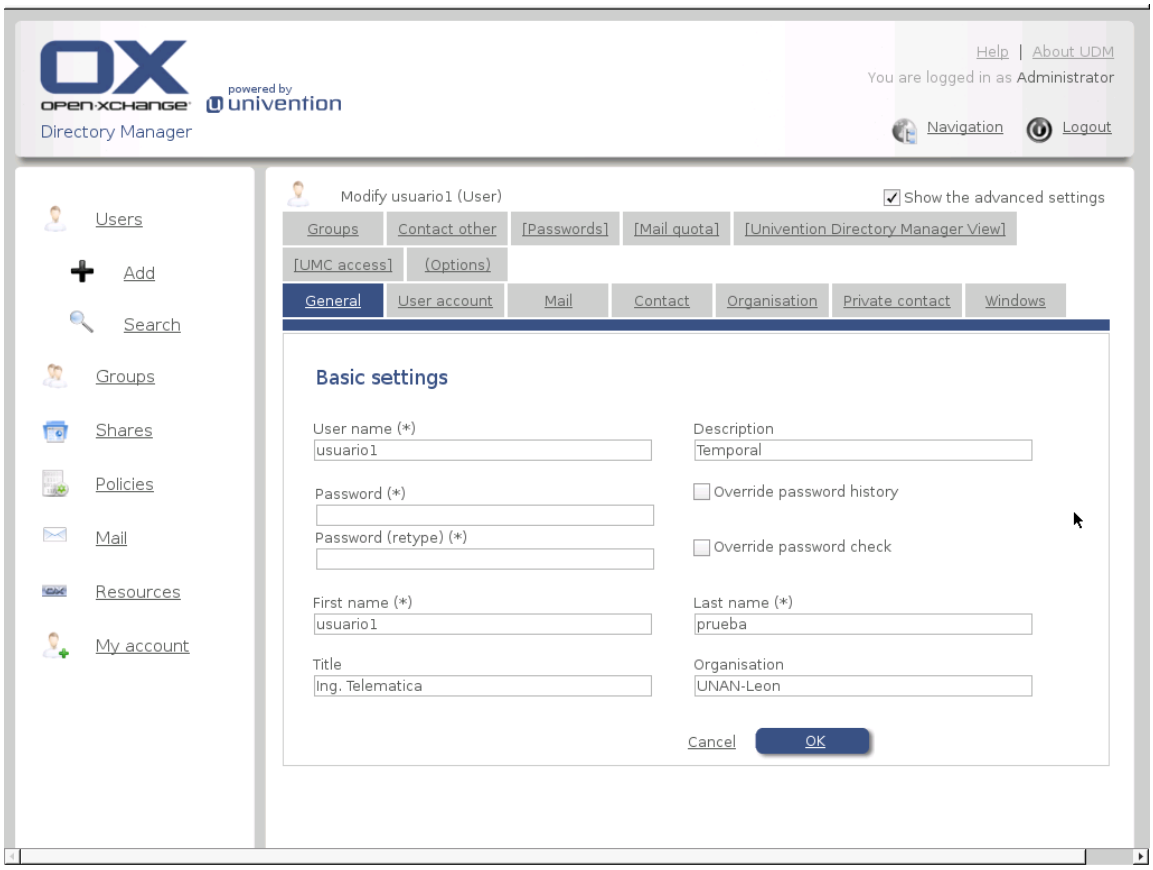


Fig. 26 Configuración de usuarios: Opciones Avanzadas

Una vez creado el usuario, puede acceder a su cuenta de correo electrónico con Open-Xchange Server desde el navegador introduciendo **http://Nombre-del-dominio/** del correo electrónico si el DNS ya está configurado para que pueda resolver esta dirección. Inicialmente se muestra una interfaz sencilla del correo electrónico también se muestra un asistente para la sincronización con otras cuentas de correo.

En el momento de creación de los usuarios en el Univention Directory Manager dentro de la configuración **General** del usuario que se ha creado se puede definir el lenguaje para la cuenta de correo. Esto también se puede cambiar en las configuraciones de correo una vez que se haya iniciado sesión y se establece un modo más completo de la vista de componentes del correo electrónico se ve en la **fig. 27**

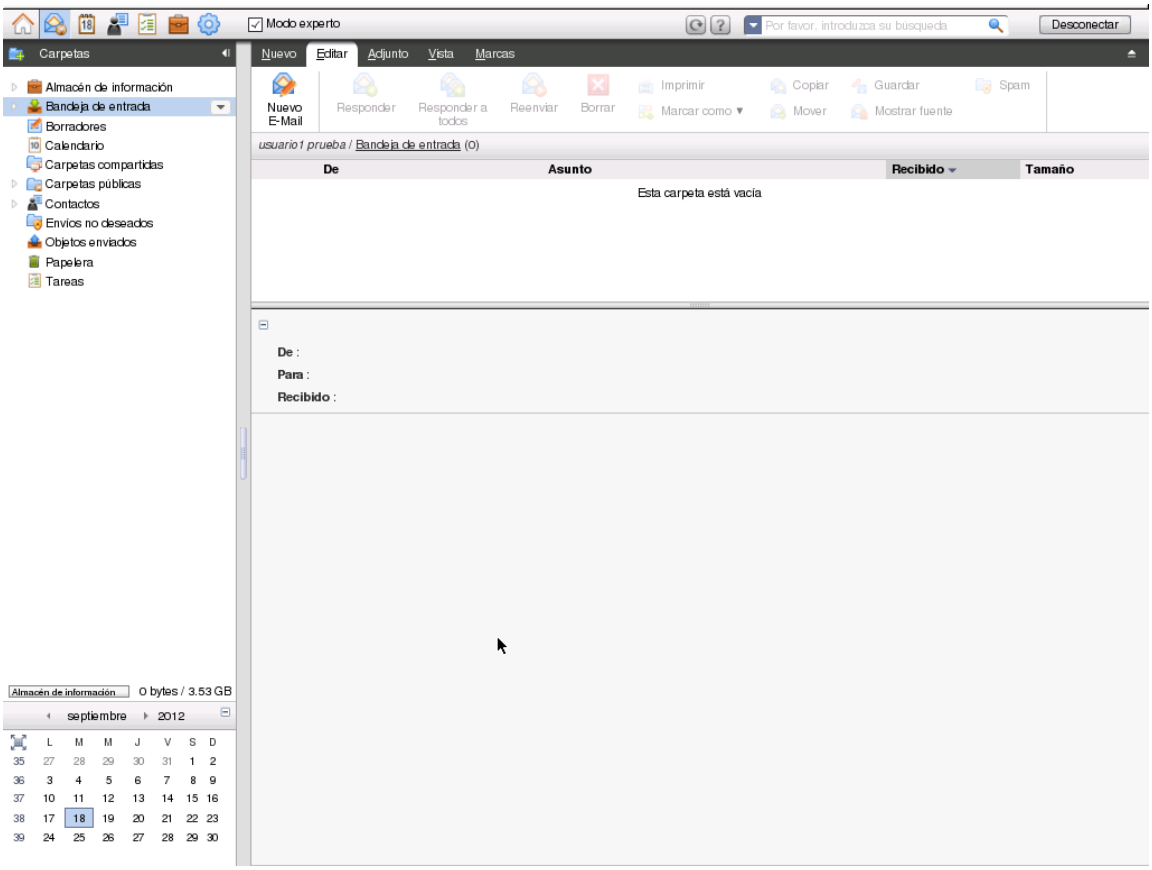


Fig. 27 Interfaz del correo electrónico con Open-Xchange Server

4.2 Sincronización de cuentas externas

Si se desea sincronizar el correo electrónico al iniciar sesión en la cuenta de correo se inicia el asistente que guiara a través de algunos ajustes básicos en torno a la sincronización con otras cuentas de correos como se ve en la **fig. 28.**

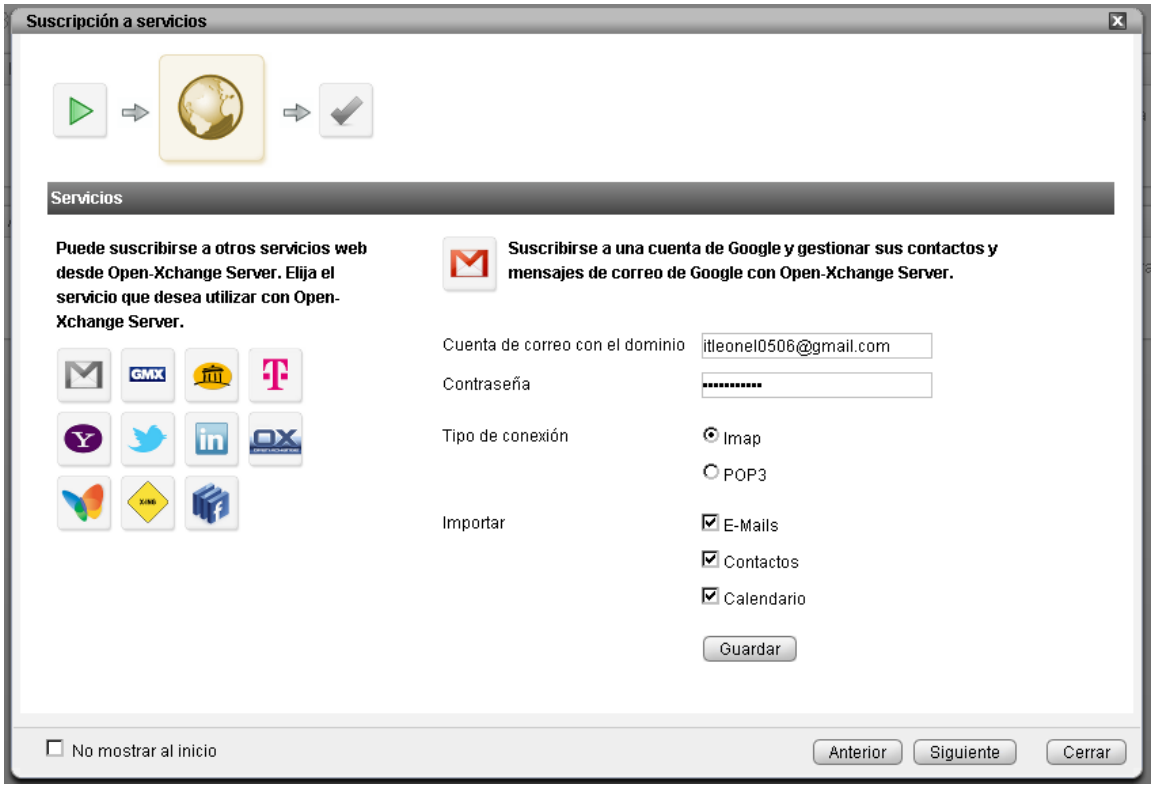


Fig. 28 Sincronización del correo electrónico local con otras cuentas externas

Luego de especificar la cuenta de correo, la contraseña y el tipo de conexión se guardan y se inicia automáticamente la suscripción y sincronización. También se reciben mensajes que indican el estado de la sincronización.

4.3 Creación y administración de Grupos de usuarios:

Entre los puntos de administración del menú principal se encuentra el de **Groups** en donde se encuentran y se crear nuevos grupos para su debida gestión en la siguiente **fig. 29** se ven los grupos que se han creado desde la instalación y configuración del sistema UCS.

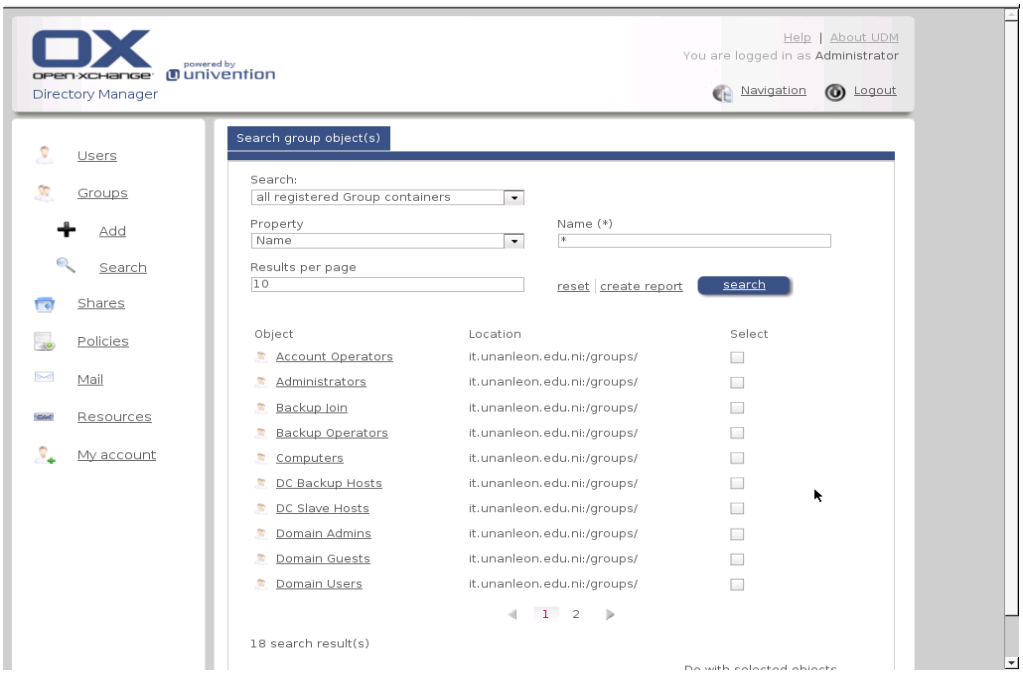


Fig. 29 Lista de grupos creados por el sistema parte 1

Estos son objetos que están en el directorio LDAP. En la **fig. 30** siguiente esta la segunda parte de grupos.

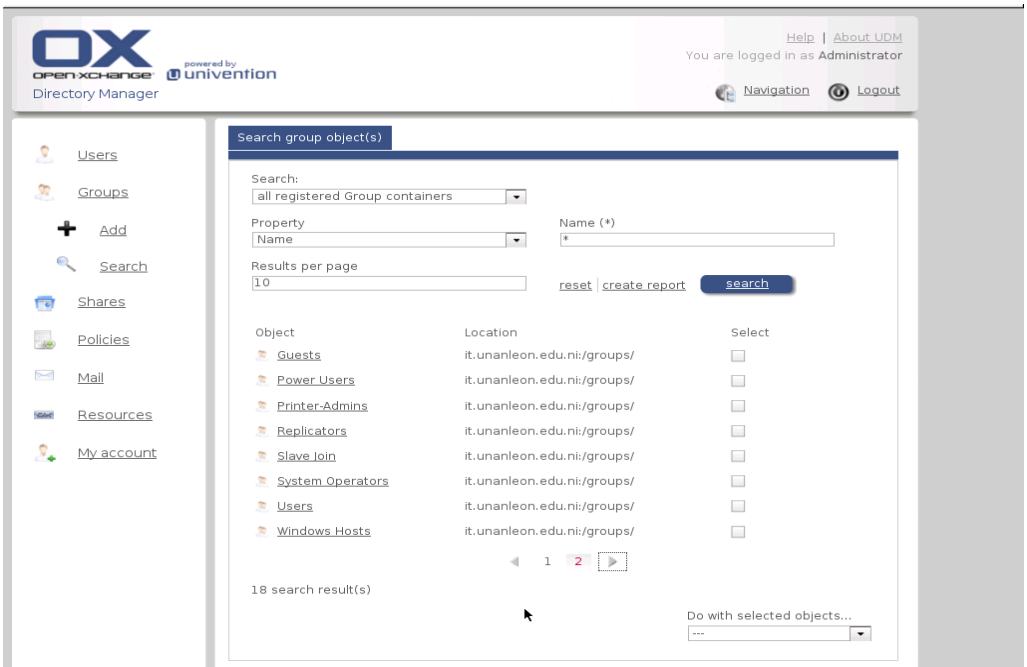


Fig. 30 Lista de grupos creados por el sistema parte 2

Para la creación de un nuevo grupo se selecciona el contenedor del grupo a crear y se indican los datos del nuevo grupo como se ve en la **fig. 31.**

También se puede chequear la vista avanzada para indicar otros puntos más detallados en el grupo que se está creando como una lista de acceso y otras opciones. La pestaña **Members** es donde se añaden los miembros que pertenecerán al grupo que se haya seleccionado.

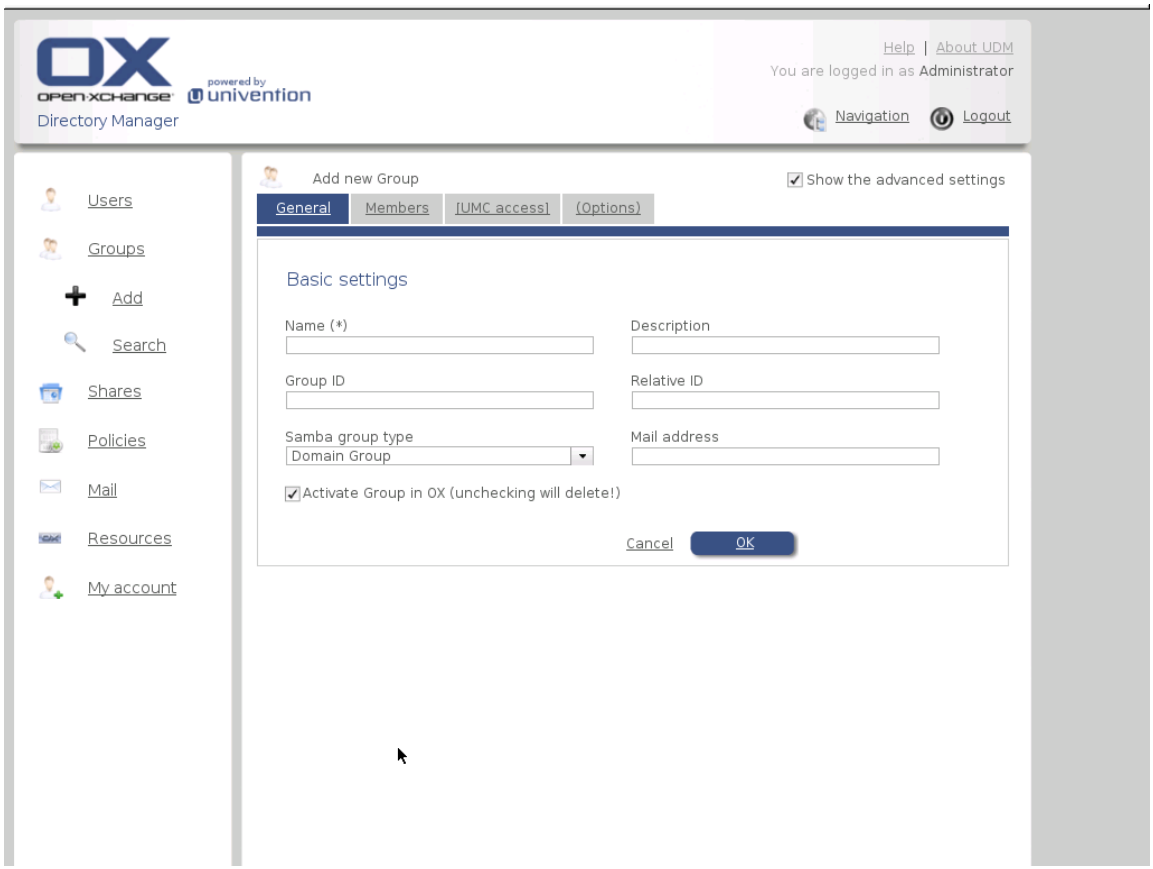


Fig. 31 Configuraciones básicas para crear un grupo y opciones avanzadas

Como se ha podido apreciar en el menú principal se encuentran otros submenú de administración que no se especificaran en este trabajo pero si pueden ser tomados en cuenta por los administradores de UCS una vez que haya instalado y configurado el sistema. Dependiendo de las necesidades del administrador el hara uso de las herramientas presentes en el sistema para resolver.

4.4 Interfaz de gestión para la administración del sistema

Otro punto que no se abordó en su totalidad pero se hace de su mención en el documento por su importante función de gestión y administración que ofrece el sistema y que también se ha especificado en la instalación y configuración del UCS es:

Univention Management Console con **Open-Xchange Server.** Lo cual es una interfaz de gestión para la administración del sistema basado en web permitiendo la creación, modificación de algunas variables de configuración en el sistema. Como forma de seguridad también ofrece una interfaz para poder iniciar sesión con el usuario creado por el sistema y la contraseña indicada en los parámetros de configuración del sistema UCS.

Se encuentra la interfaz de administración de Univention Management Console, donde están las herramientas para gestionar variables, registros, servicios y ver estadísticas sobre el sistema entre otros. Ver la **fig. 32** siguiente.

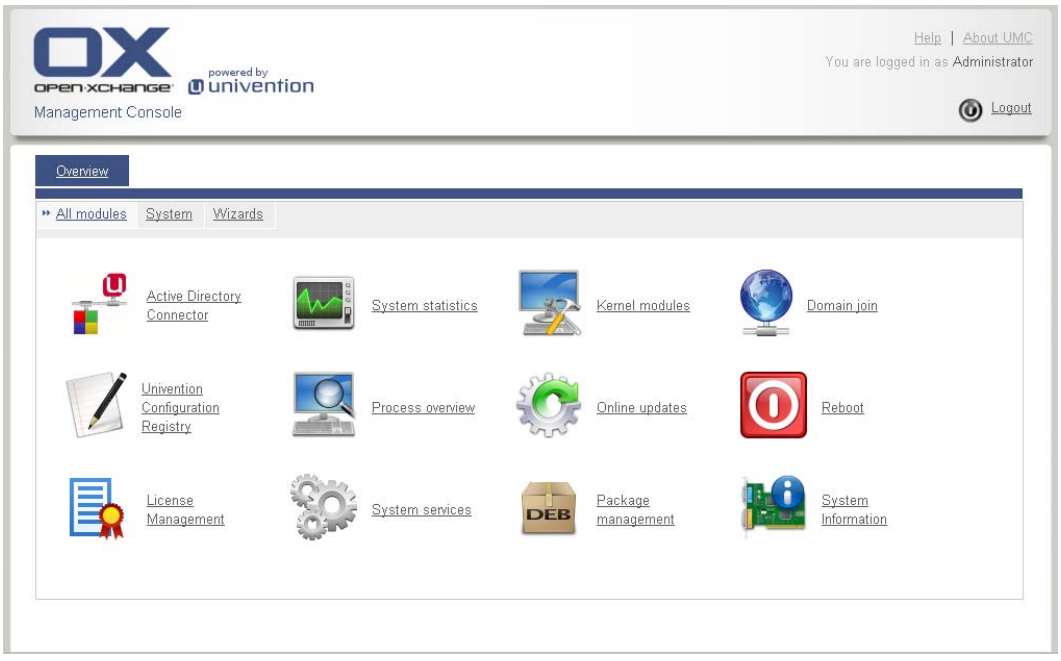


Fig. 32 Interfaz de administración de Univention Management Console

En las configuraciones necesarias para el correcto funcionamiento del servidor de correo electrónico y la utilización de la Autoridad Certificadora una de las herramientas más utilizada fue: **Univention Configurate Registry** para ubicar archivos de configuración como por ejemplo los certificados creados por la autoridad certificadora que se creó en la instalación y configuración del sistema. (Ver **fig. 33**)

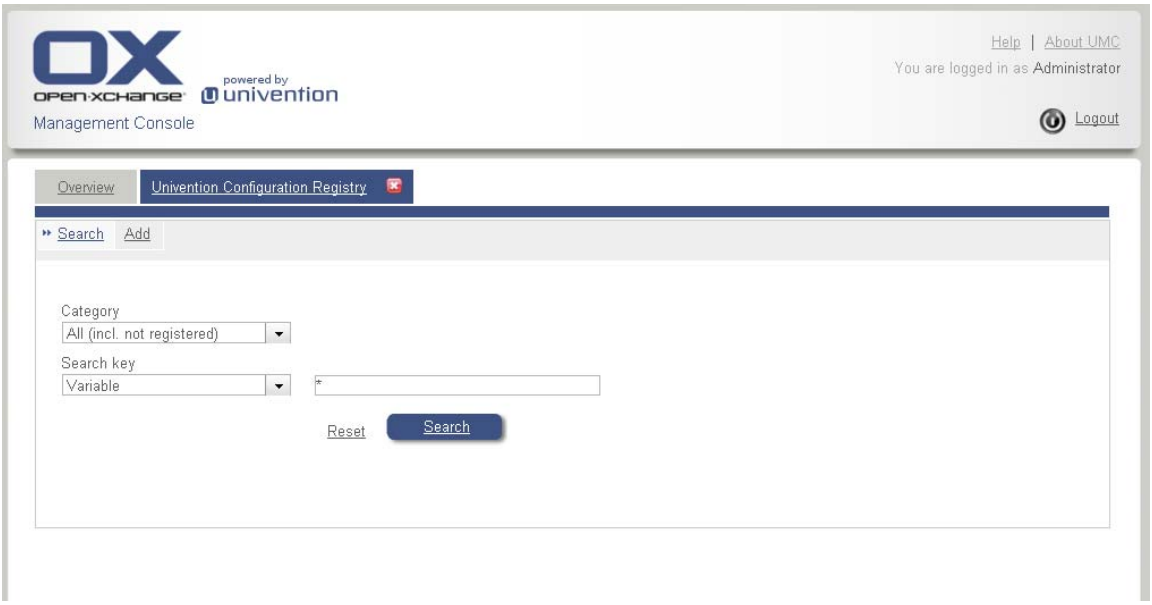


Fig. 33 Panel de control Univention Configuration Registry

4. Configuración de las herramientas de seguridad

4.1. Configuración de los servicios que integran un Servidor de Correo Electrónico Seguro

4.1.1. Autoridad Certificadora

Como herramienta de seguridad se utiliza SSL (Secure Sockets Layer) es un protocolo orientado a la implementación de sesiones de transporte seguras brindando los siguientes servicios: privacidad, Autenticación e Integridad.

Desarrollado por Netscape Corporation y RSA Data Security. Típicamente utilizado con Http pero puede ser usando con cualquier tipo de servicio que lo soporte ya que es independiente de la aplicación como servicios de correo con SMTP, POP3, IMAP, Túneles VPN, etc.

Trabaja entre la capa de aplicación y la capa de Transporte del modelo OSI o TCP/IP (ver **fig. 34**)

Fig. 34 Ubicación de SSL en la torre OSI

Soportado por los principales Browsers y Servidores WEB: Mozilla Firefox, Internet Explorer, IIS, Apache, etc

Para las aplicaciones que requieren una conexión segura SSL con Apache la URL seria https//; por lo general el servidor escucha por el puerto 443 para SSL. Las funciones que el protocolo SSL puede cumplir son las siguientes:

- Autenticación
- Privacidad
- Confidencialidad
- Compresión
- Fragmentación

Durante la conexión entre el cliente y servidor se inician unas series de faces que se conocen como las fases del **handshake** que se utilizan para el intercambio de una serie de mensajes para negociar la seguridad pero valga decir que todo esto es transparente para el usuario;

- Fase1: Selección del conjunto de algoritmos para mantener la confidencialidad y autenticación
- Fase2: Intercambio de Claves
- Fase3: Creación de la clave de sesión
- Fase4: Verificación del servidor
- Fase5: Autenticación del Cliente
- Fase6: Indicación del inicio de la sesión segura

Para trasmitir los datos cifrados, el cliente y el servidor se ponen de acuerdo en el formato en que van a enviar la información cifrada, este consenso lo realiza el Protocolo record SSL. Para cifrar los datos se apoya en los algoritmos acordados en el protocolo handshake. El protocolo record SSL es el encargado de la seguridad en el intercambio de los datos, cifrando los protocolos que llegan de capas superiores como son la capa de Aplicación de OSI y la subcapa Handshake.

Durante una comunicación con SSL, se pueden abrir varias sesiones, y dentro de cada sesión se puede mantener varias conexiones SSL. El manejo de la apertura o el cierre de las conexiones se hace a través del protocolo handshake.

Estos son los componentes del protocolo de registro (record):

-MAC-DATA: Código de autenticación del mensaje -ACTUAL-DATA: Los datos de aplicaciones a transmitir -PADDING-DATA: Los datos requeridos para rellenar el mensaje cuando se usa cifrado por bloque Durante una comunicación con SSL, se pueden abrir varias sesiones, y dentro de cada sesión se puede mantener varias conexiones SSL. El manejo de la apertura o el cierre de las conexiones se hace a través del protocolo handshake.

Existen dos tipos de estado:

- Estado de sesión
- Estado de conexión

Estado de sesión incluye estos componentes:

- Identificador de sesión
- Certificado
- Método de compresión
- Algoritmo de cifrado
- Clave maestra
- Flag de nuevas conexiones

El estado de conexión incluye estos componentes

- Números aleatorios del servidor y cliente
- Número secreto del cliente para MAC
- Número secreto del servidor para MAC
- Clave secreta del cliente
- Vectores iniciales
- Clave secreta del servidor
- Números de secuencia

Desde la instalación y configuración del sistema se han especificado parámetros para la creación de una Autoridad Certificadora (en inglés Certification Authority CA), la cual es una entidad de confianza del emisor y del receptor de una comunicación. Esta confianza de ambos permite que cualquiera de los dos confié a su vez en los documentos firmados por la Autoridad Certificadora, en particular, en los certificados que identifican ambos extremos.

Un certificado es un documento emitido y firmado por una Autoridad Certificadora que identifica una clave pública como su propietario. Cada certificado está identificado de manera univoca y tiene un periodo de validez consignado en el propio certificado. Un certificado permite validar la identidad de otro extremo de una comunicación ya sea una persona o un dispositivo.

Estos parámetros de configuración para la creación de la Autoridad Certificadora se pueden ver en la **fig. 35** la cual aparece en la instalación y configuración del sistema. Además de estos datos la autoridad certificadora necesita de una contraseña para poder

firmar las peticiones de certificados esta contraseña será la que se ha definido como la contraseña del usuario **root**.

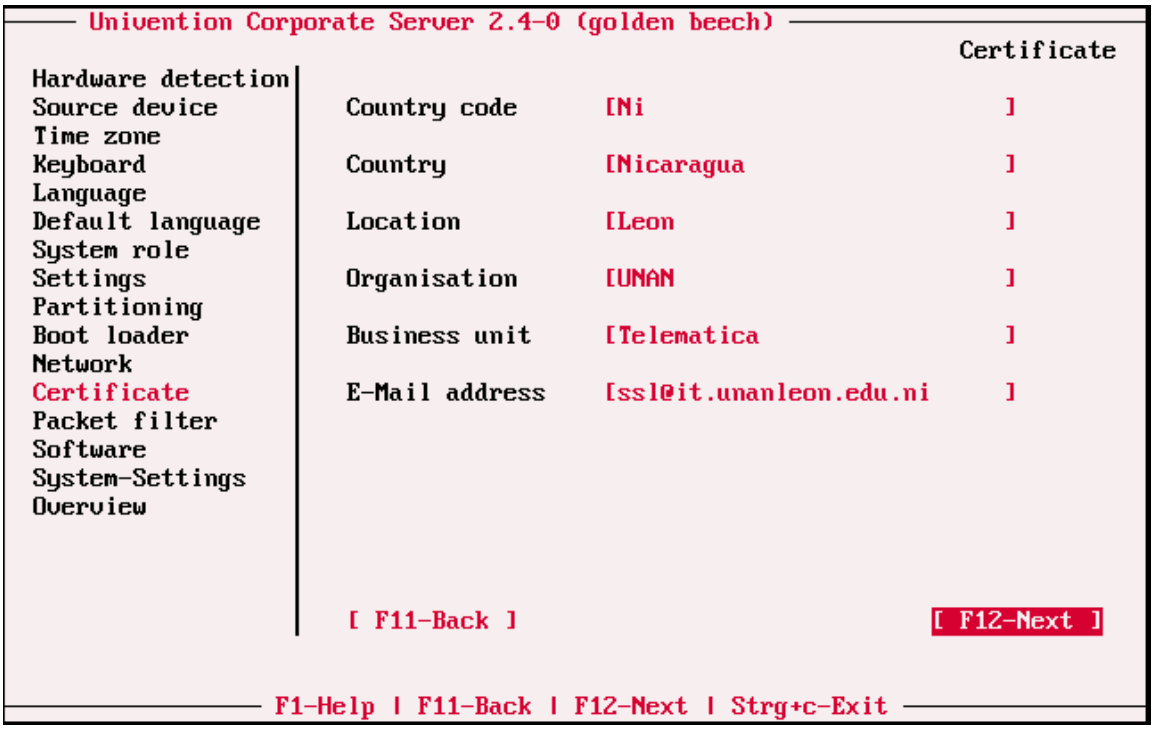


Fig. 35 Creación de la Autoridad Certificador (CA)

4.1.2. Configuración de la seguridad en los protocolos del correo electrónico

Entre los servicios más importantes que conforman el funcionamiento del correo electrónico se encuentran SMTP el cual es el transporte de correo, es quien se va a encargar de mandar/recibir el correo, IMAP es un protocolo que se utiliza para ver los mensajes y es muy utilizado para acceder al correo vía Web y POP que a diferencia de IMAP se puede descargar los mensajes en el equipo de trabajo, dejándolos o no en el servidor

Para configurar el SMTP seguro se deben realizar modificaciones en los ficheros de configuración del Postfix. Partiendo de que se dispone de una autoridad certificadora que

proporciona la firma electrónica para los certificados. A continuación se debe indicarle al Postfix donde están y que se quiere que ofrezca TLS. Para esto en la ruta **/etc/postfix/** en el fichero **main.cf** se introducen las siguientes líneas:

```
smtpd_use_tls = yes

smtpd_tls_auth_only = yes

smtpd_starttls_timeout = 300s

smtpd_timeout = 300s

smtpd_tls_cert_file =

/etc/univention/ssl/mail.it.comp.unanleon.edu.ni/cert.pem

smtpd_tls_key_file =

/etc/univention/ssl/mail.it.comp.unanleon.edu.ni/private.key

smtpd_tls_received_header = no

smtpd_tls_session_cache_timeout = 3600s

tls_random_source = dev:/dev/urandom
```

Ahora se restringe que las autentificaciones al envió se realicen únicamente en un canal cifrado mediante el protocolo TLS y se obliga que todas las comunicaciones con el demonio smtpd se hagan a través de TLS. Estableciendo una transferencia segura obteniendo SMTPS. Se reinicia el servicio Postfix y se comprueba el correcto funcionamiento del mismo ver la **fig. 36**:

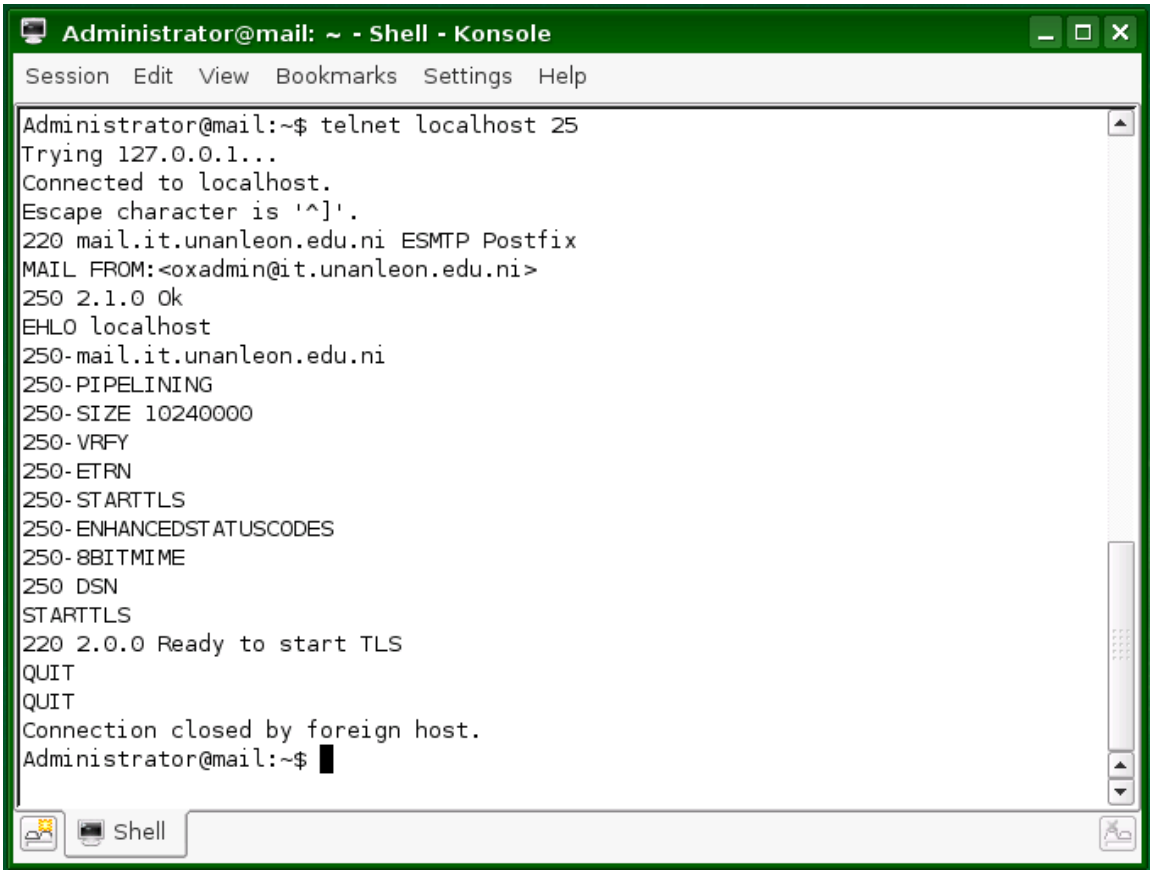


Fig. 36 Telnet al puerto 25 del servidor

Para la seguridad en los protocolos IMAP y POP se debe activar el cifrado del canal de comunicación en el servicio de Cyrus por lo cual se modifican dos ficheros **cyrus.conf** y **imap.conf** que se encuentran en la ruta: **/etc/imapd/**.

En el fichero **cyrus.conf** se des comenta o modifican las siguientes líneas:

```
imap          cmd="/usr/lib/cyrus/bin/imapd -C /etc/imapd/imapd.conf -U 30"
listen="imap" prefork=0 maxchild=400

imaps         cmd="/usr/lib/cyrus/bin/imapd -C /etc/imapd/imalpd.conf -s -U 30"
```

```
listen="imaps" prefork=0 maxchild=400
```

Se indica que el servicio imaps se debe añadir a la lista de los que deben iniciarse con el servicio Cyrus y se fuerza a usar un canal cifrado.

En el fichero imapd.conf se modifican las siguientes líneas:

```
tls_cert_file: /var/lib/cyrus/cert.pem
tls_key_file: /var/lib/cyrus/private.key
tls_ca_path: /etc/univention/ssl/ucsCA/certs/
tls_session_timeout: 1440
tls_cipher_list: TLSv1:SSLv3:SSLv2:!NULL:!EXPORT:!DES:!LOW:@STRENGTH
idlemethod: idled
```

Reiniciar el servicio: **cyrus2.2 restart**

Los servicios de IMAP y POP ya se encuentran certificados bajo la autoridad certificadora auto-firmada que se ha creado. Para identificar los servicios actualmente en ejecución se utiliza el siguiente comando ver la **fig. 37** siguiente:

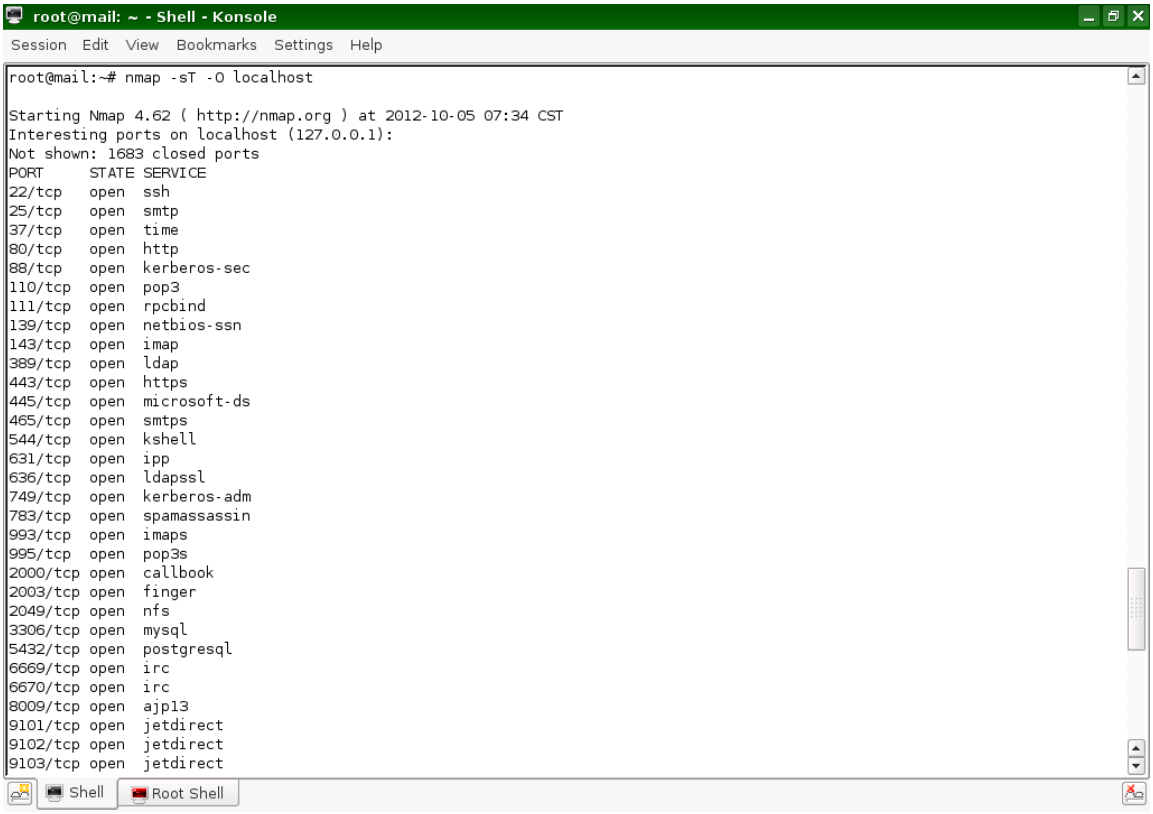


Fig. 37 Puertos, estado y servicios del sistema

Se identifican los protocolos que integran el funcionamiento del correo electrónico configurados con seguridad en correcta ejecución como son **smtps:465, imaps:993** y **pop3s:995.**

Los Servicios Postfix y Cyrus no tiene permisos para leer los certificados desde la ubicación estándar ***/etc/ssl/*** así como Apache2, pero si se utilizaran los mismos y es necesario ejecutar los siguientes comandos:

Para los certificados de Postfix:

```
mkdir /etc/univention/ssl/mail.it.comp.unanleon.edu.ni/

cp /etc/ssl/certs/ssl-cert-snakeoil.pem
```

/etc/univention/ssl/mail.it.comp.unanleon.edu.ni/ cert.pem

cp /etc/ssl/private/ssl-cert-snakeoil.key
/etc/univention/ssl/mail.it.comp.unanleon.edu.ni/ private.key

Para los certificados de Cyrus:

mkdir /etc/univention/ssl/ucsCA/certs/

cp /etc/ssl/certs/ssl-cert-snakeoil.pem /etc/univention/ssl/ucsCA/certs/cert.pem

cp /etc/ssl/private/ssl-cert-snakeoil.key /etc/univention/ssl/ucsCA/certs/private.key

En los ficheros establecer permisos para la correcta lectura: **chmod 600 /etc/…**

4.1.3. Configuración de Https en Apache2

Al finalizar con la instalación y configuración del sistema en los archivos de configuración del servidor web apache2 donde se ha creado el host-virtual se tienen que indicar o habilitar el modulo SSL en el servidor web Apache. Para habilitar el modulo ssl se debe modificar la configuración de Apache2 para añadir las directivas:

SSLEngine on

SSLCertificateFile /etc/ssl/certs/ssl-cert-snakeoil.pem

SSLCertificateKeyFile /etc/ssl/private/ssl-cert-snakeoil.key

El archivo **ssl-cert-snakeoil.pem** es el certificado que se comparte con cada navegador para establecer una conexión segura y en el archivo **ssl-cert-snakeoil.key** se encuentra la llave para el intercambio de llaves en el inicio de la conexión. En el archive **default-ssl** que se encuentra en **/etc/apache2/sites-available/**.

Luego de añadir las directivas se tiene que especificar que todas las peticiones hechas al servidor web se redireccionen para que salgan por el puerto 443 para que tengamos una conexión segura con SSL. Esto se indica en el fichero de configuración **http.conf** que se encuentra en **/etc/apache2/** y se añaden las siguientes directivas de configuración:

```
RewriteEngine On

        RewriteCond %{HTTPS} off

        RewriteRule (.*)https://%{HTTP_HOST}%{REQUEST_URI}
```

Se guardan los cambios y se reinicia el servidor web:

- **/etc/init.d/apache2 restart**

Concluida la configuración de la herramienta de seguridad en el servidor web se verifica que el acceso al correo sea a través de **https://** obteniendo una comunicación segura entre el cliente y el servidor utilizando certificados auto-firmados por la autoridad certificadora que se ha creado.

En el navegador se introduce la dirección del dominio del servidor de correo: **mail.it.comp.unanleon.edu.ni** ahora en la **fig. 38** siguientes: aparece la pantalla de advertencia. Esto se debe a que la autoridad certificadora que se ha creado no es una CA reconocida por lo cual el navegador manda un mensaje de advertencia sobre la conexión.

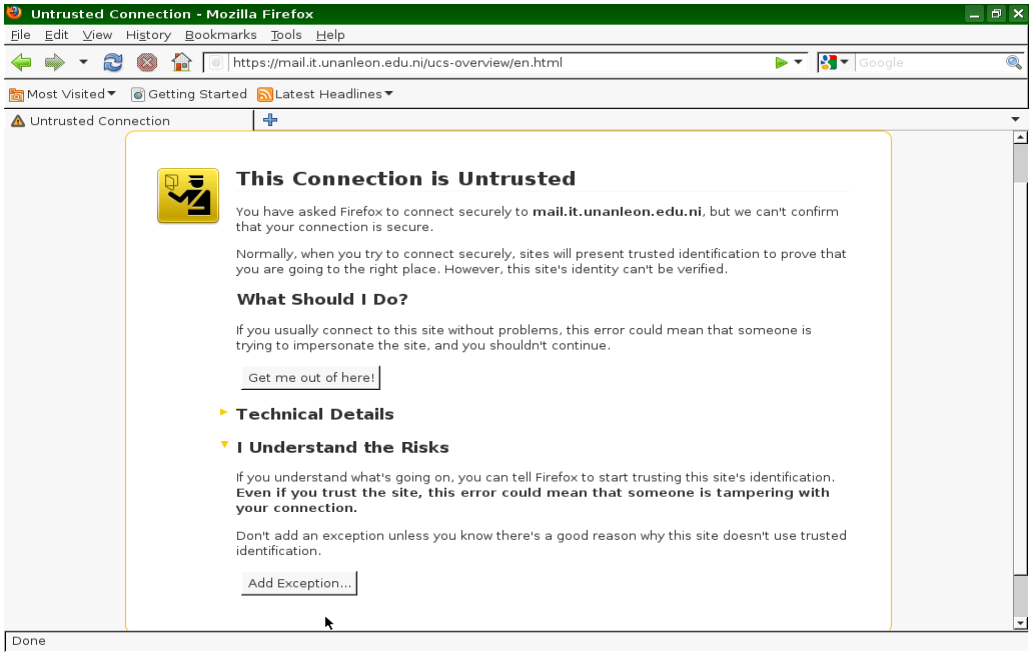


Fig. 38 Especificación de los riesgos de la conexión no identificada

En la **fig. 39** siguiente es donde se obtiene el certificado y se confirma la excepción de seguridad.

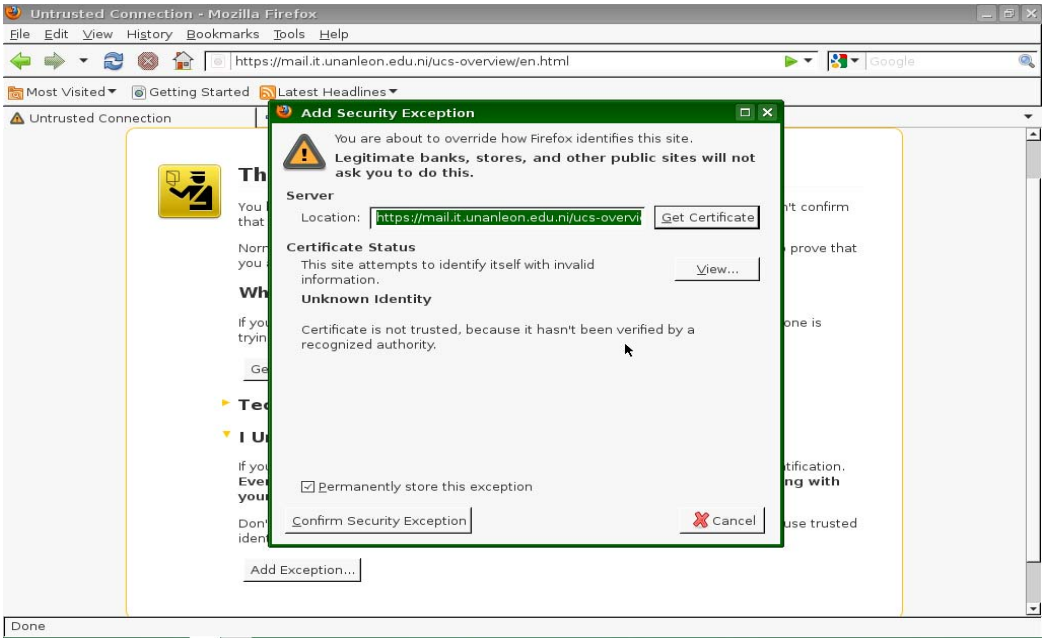


Fig. 39 Obtención del Certificado

También se puede ver el estado e información del certificado. Ahora ya la conexión se ha cifrado con diferentes algoritmos de seguridad entre el cliente y el servidor.

Como se ve en la **fig. 40** indica que la conexión se ha verificado por unanleon.edu.ni y ha sido cifrada. Proporcionando privacidad, autenticación, integridad, no repudio, firma digital por lo cual el usuario goza de una conexión más confiable y segura.

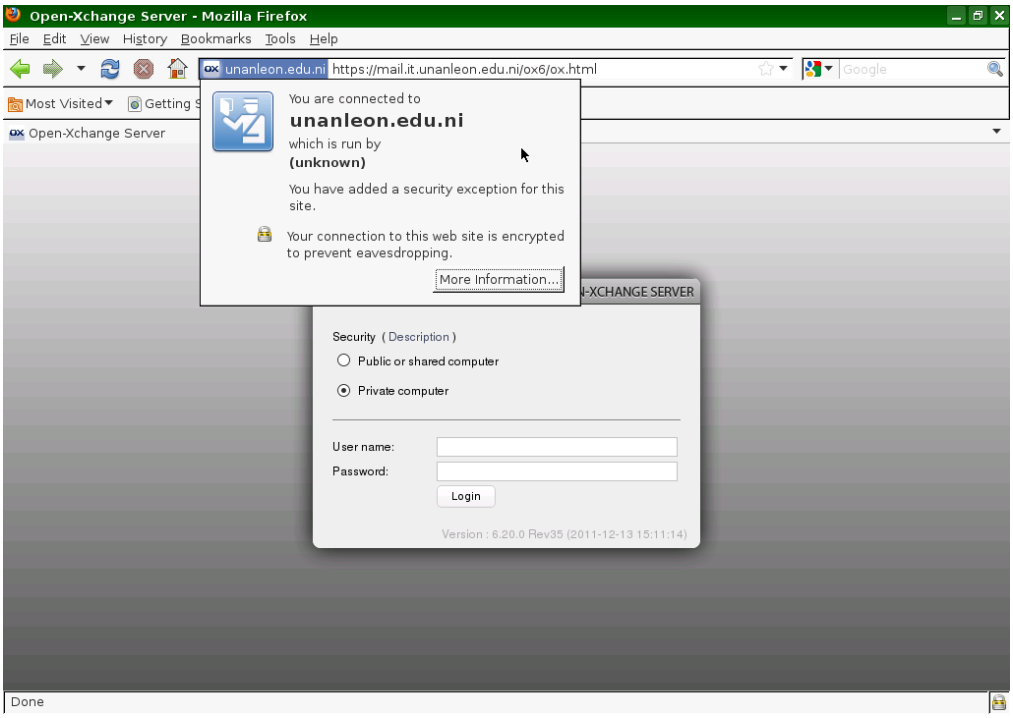


Fig. 40 Conexión Cifrada verificada por unanleon.edu.ni

El siguiente esquema (**Fig. 41**) ejemplifica el proceso de comunicación que se realiza entre el cliente y el servidor cuando se accede al correo electrónico vía web:

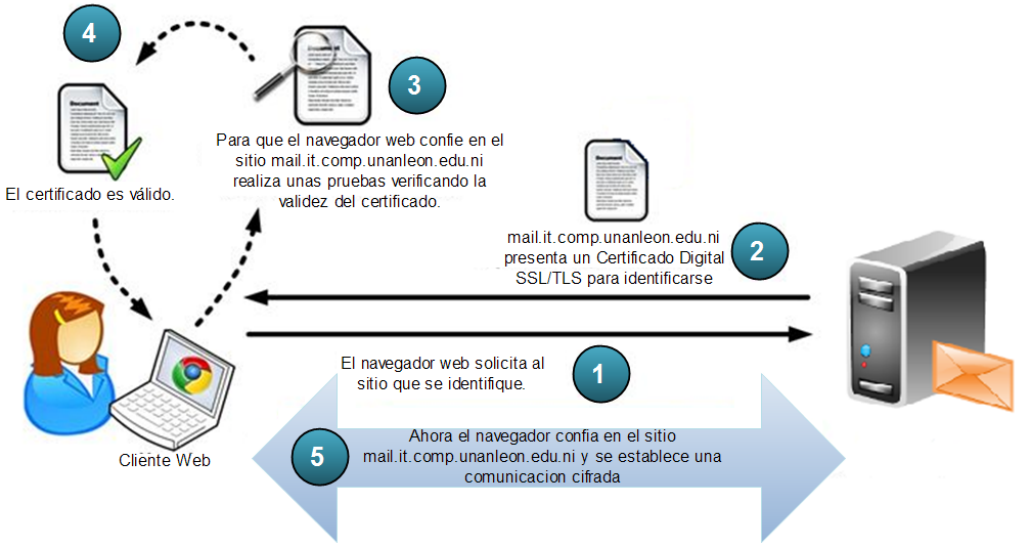


Fig. 41 Esquema de comunicación web con SSL/TLS en Apache

4.2 Implementación de filtros de virus y spam

El termino Spam se refiere a todos los correos electrónicos que no son apreciados ni solicitados. Spamassassin es un programa que intenta identificar si un correo electrónico es deseable o no basado en su origen, forma y contenido.

ClamAV es un código abierto (GPL) motor antivirus diseñado para la detección de troyanos, virus, malware y otras amenazas maliciosas. Es el estándar de facto para la exploración de pasarela de correo.

SpamAssasin y ClamAV son dos filtros de contenidos que serán utilizados desde Postfix a través de Amavisd-new el cual es una interfaz de alto rendimiento entre el cliente de correo (MTA) y los escáneres y virus

La configuración para la implementación del anti-spam y anti-virus para el correo electrónico es la siguiente:

En el fichero **/etc/default/spamassassin**

```
ENABLED=0
OPTIONS="-c -m 10 -a -H"
```

Editar **/etc/amavis/amavisd.conf** y como opciones tenemos que remarcar las siguientes:

```
$mydomain = 'mail.it.comp.unanleon.edu.ni';
$forward_method = 'smtp:127.0.0.1:10025';
$notify_method = $forward_method;
$final_spam_destiny = D_PASS;
$sa_tag_level_deflt  = 4.0;
$sa_tag2_level_deflt = 5.0;
$sa_kill_level_deflt = $sa_tag2_level_deflt;
```

La opción que merece más atención es **$forward_method**, que será la vía que utilizará amavisd-new para reinyectar el mensaje de correo en postfix; en este caso le hemos dicho que lo haga usando un smtp en localhost por el puerto 10025. Las otras lo que hacen es fijar algunas opciones sobre el SpamAssassin.

En el fichero **amavisd.conf**. Buscar la siguiente porción de código:

```
### http://clamav.elektrapro.com/
  ['Clam Antivirus-clamd',
    \&ask_daemon, ["CONTSCAN {}\n", '/var/run/clamd.ctl'],
    qr/\bOK$/, qr/\bFOUND$/,
    qr/^.*?: (?!Infected Archive)(.*) FOUND$/ ],
```

Y cambiar la ruta al socket **/var/run/clamd.ctl** a **/var/run/clamav/clamd.ctl** para que se corresponda con la opción LocalSocket del fichero **/etc/clamav/clamav.conf**.

Para que amavisd-new haga uso de SpamAssassin se debe verificar que no existe esta línea en el fichero de configuración de amavisd-new. Se debe comentar.

```
@bypass_spam_checks_acl  = qw( . );
```

En la configuración de postfix, la idea es hacer que en los puertos por defecto (25 y 465) postfix pase todos los emails por amavisd-new. Y luego, crear un proceso SMTP que solo correrá en la interfaz loopback (127.0.0.1) en el puerto 10025 y que pasará los correos a los usuarios sin pasarlo por amavisd-new. Esto es necesario para evitar que los correos entren en un bucle sin fin.

En **/etc/postfix/main.cf** añadir o editar:

```
content_filter=smtp-amavis:[localhost]:10024
Y en /etc/postfix/master.cf:
smtp-amavis unix -      -       y       -       2       smtp
        -o smtp_data_done_timeout=1200
        -o disable_dns_lookups=yes
127.0.0.1:10025 inet n  -       y       -       -       smtpd
        -o content_filter=
        -o local_recipient_maps=
        -o relay_recipient_maps=
        -o smtpd_restriction_classes=
        -o smtpd_client_restrictions=
        -o smtpd_helo_restrictions=
        -o smtpd_sender_restrictions=
```

```
-o smtpd_recipient_restrictions=permit_mynetworks,reject

-o mynetworks=127.0.0.0/8

-o strict_rfc821_envelopes=yes
```

La primera línea crea el filtro para amavis y la segunda crea el servidor local por el que permitirá cualquier correo sin intentar filtrarlo.

Para finalizar líneas del **sources.list** que se utilizan:

```
## Debian - stable

deb http://ftp.us.debian.org/debian/  stable main contrib non-free

deb-src http://ftp.us.debian.org/debian/  stable main contrib non-free

## Actualizaciones de seguridad

deb http://security.debian.org/  stable/updates main contrib non-free

deb-src http://security.debian.org/  stable/updates main contrib non-free

#Filtros Spam y Virus

deb http://www.backports.org/debian stable spamassassin postfix clamav

deb-src http://www.backports.org/debian stable spamassassin postfix clamav

deb http://people.debian.org/~aurel32/BACKPORTS stable main

deb-src http://people.debian.org/~aurel32/BACKPORTS stable main
```

Comprobar que amavisd-new acepte conexiones: Verificación del funcionamiento de los filtros de seguridad:

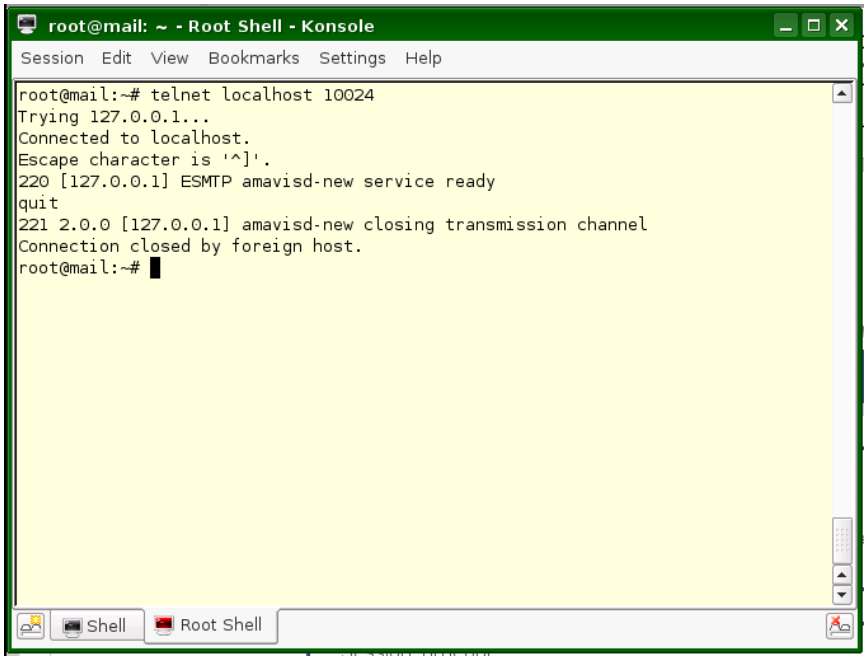


Fig. 42 Funcionamiento de amavis-new puerto 10024

Comprobar también que Postfix pueda recibir de vuelta los mensajes filtrados:

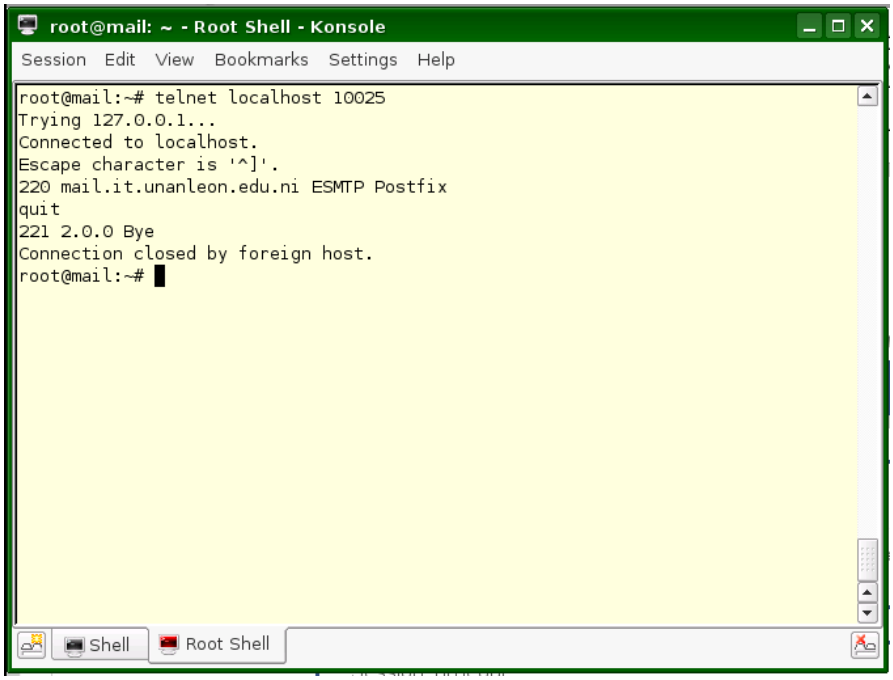


Fig. 43 Verificación del recibo de Postfix

4.3 Métodos de Backup para el servidor de correo electrónico

Para realizar una copia de seguridad del servidor de correo se puede utilizar las siguientes opciones:

Implementación de herramientas de virtualización:

- VMware
- XEN
- KVM
- Citrix

Si no se utiliza herramientas de virtualización se debe realizar una copia de los buzones de cada usuario que ha sido registrado en el servidor de correo los cuales se encuentran en la siguiente ruta:

/var/spool/cyrus/mail/domain/i/mail.it.comp.unanleon.edu.ni/

Este proceso se mejora con la implementación del comendo rsync para realizar copias de seguridad en GNU/Linux

Para la implementación de esta herramienta realizar los siguientes pasos:

```
sudo apt-get install rsync

rsync –av -- delete /var/spool/cyrus/mail/domain/i/mail.it.comp.unanleon.edu.ni/* /media/DISCO/Backup
```

Ahora se debe realizar una copia de seguridad de la base de datos LDAP donde se encuentran las configuraciones del dominio como usuarios, grupos, permisos y todos los datos del servidor.

Exportar LDAP completo:

```
slapcat –l backup.ldif
```

Nota: El archivo backup.ldif es donde se guardara toda la base de datos LDAP su formato es .ldif

Importar archivo .ldif

```
slapadd –c –l backup.ldif
```

De esta forma importamos backup.ldif en nuestro LDAP, la creación de un script para este proceso es muy importante para programar dicha tarea cada cierto tiempo.

5. Análisis de la comunicación en un canal seguro del correo electrónico

En el análisis de la comunicación de un usuario que acceda a su correo electrónico se utiliza Wireshark para la captura de las tramas en la comunicación cliente-servidor. El esquema de análisis siguiente se realiza mediante la utilización de un cliente de Windows Outlook que realiza un envío de correo a otro usuario que pertenece al dominio del correo electrónico.

La siguiente **fig. 44** presenta las tramas de comunicación capturadas con el Wireshark y muestra los protocolos y el proceso de comunicación entre el cliente y el servidor.

192.168.1.109	192.168.1.103	TCP	53884 > pop3s [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
192.168.1.103	192.168.1.109	TCP	pop3s > 53884 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 WS=7
192.168.1.109	192.168.1.103	TCP	53884 > pop3s [ACK] Seq=1 Ack=1 Win=65700 Len=0
192.168.1.109	192.168.1.103	SSL	Client Hello
192.168.1.103	192.168.1.109	TCP	pop3s > 53884 [ACK] Seq=1 Ack=224 Win=6912 Len=0
192.168.1.103	192.168.1.109	TLSv1	Server Hello, Certificate, Server Hello Done
192.168.1.109	192.168.1.103	TLSv1	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
192.168.1.103	192.168.1.109	TLSv1	Change Cipher Spec, Encrypted Handshake Message
192.168.1.103	192.168.1.109	TLSv1	[TCP Retransmission] Change Cipher Spec, Encrypted Handshake Message
192.168.1.109	192.168.1.103	TCP	53884 > pop3s [ACK] Seq=422 Ack=1357 Win=64344 Len=0 SLE=1298 SRE=1357
192.168.1.103	192.168.1.109	TLSv1	Application Data
192.168.1.109	192.168.1.103	TLSv1	Application Data, Application Data
192.168.1.103	192.168.1.109	TLSv1	Application Data
192.168.1.109	192.168.1.103	TLSv1	Application Data, Application Data
192.168.1.103	192.168.1.109	TLSv1	Application Data
192.168.1.109	192.168.1.103	TLSv1	Application Data, Application Data
192.168.1.103	192.168.1.109	TCP	pop3s > 53884 [ACK] Seq=1820 Ack=708 Win=8064 Len=0
192.168.1.103	192.168.1.109	TLSv1	Application Data
192.168.1.109	192.168.1.103	TLSv1	Application Data, Application Data
192.168.1.103	192.168.1.109	TCP	pop3s > 53884 [ACK] Seq=1889 Ack=782 Win=8064 Len=0
192.168.1.103	192.168.1.109	TLSv1	Application Data
192.168.1.109	192.168.1.103	TLSv1	Application Data, Application Data
192.168.1.103	192.168.1.109	TLSv1	Application Data
192.168.1.109	192.168.1.103	TLSv1	Application Data, Application Data
192.168.1.103	192.168.1.109	TLSv1	Application Data
192.168.1.109	192.168.1.103	TLSv1	Application Data, Application Data
192.168.1.103	192.168.1.109	TCP	pop3s > 53884 [FIN, ACK] Seq=2181 Ack=1004 Win=8064 Len=0
192.168.1.109	192.168.1.103	TCP	53884 > pop3s [ACK] Seq=1004 Ack=2182 Win=65024 Len=0
192.168.1.109	192.168.1.103	TLSv1	Encrypted Alert
192.168.1.109	192.168.1.103	TCP	53884 > pop3s [FIN, ACK] Seq=1041 Ack=2182 Win=65024 Len=0
192.168.1.103	192.168.1.109	TCP	pop3s > 53884 [RST] Seq=2182 Win=0 Len=0
192.168.1.103	192.168.1.109	TCP	pop3s > 53884 [RST] Seq=2182 Win=0 Len=0

Fig. 44 Análisis de la comunicación sobre un canal seguro

Al utilizar un cliente de correo electrónico este descarga los correos en la estación de trabajo local por medio del protocolo POP3 y al estar implementado de forma segura es POP3s en el puerto 995.

Para mejor la interpretación de la comunicación entre el cliente y el servidor se realizará el análisis a partir de la **fig. 45** siguiente que representa el escenario de las tramas anterior (**fig. 44**) capturadas con el Wireshark.

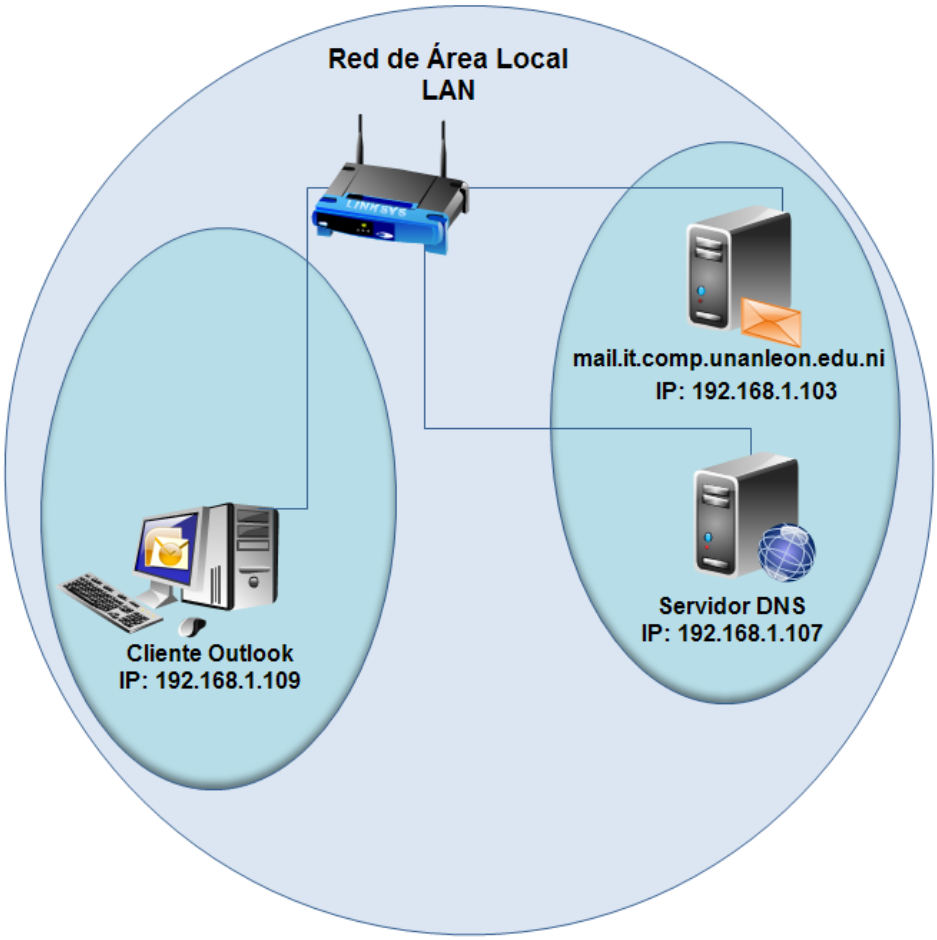


Fig. 45 ***Escenario de Comunicación sobre un canal seguro***

El escenario de la comunicación está formado por el servidor de correo electrónico, un servidor DNS, una estación de trabajo PC escritorio, como dispositivo de encaminamiento un Access Point (Punto de Acceso).

La comunicación inicia con el protocolo de comunicación orientado a la conexión y fiable del nivel de transporte TCP. El cual se encuentra entre la capa intermedia entre el

protocolo de internet (IP) y de Aplicación. Habitualmente, las aplicaciones necesitan que la comunicación sea fiable y, dado que la capa IP aporta un servicio de datagramas no fiable (sin confirmación), TCP añade las funciones necesarias para prestar un servicio que permita que la comunicación entre dos sistemas se efectúe libre de errores, sin pérdidas y con seguridad.

El inicio de la comunicación entre el cliente y el servidor se realiza utilizando TCP el cual se compone de tres etapas: establecimiento de la conexión, transferencia de datos y fin de la conexión. Esto se muestra en las tramas capturadas con Wireshark (ver **fig. 44**) en la ejecución del escenario (ver **fig. 44**).

El establecimiento del inicio de la conexión con TCP se ilustra en la **fig. 46** siguiente:

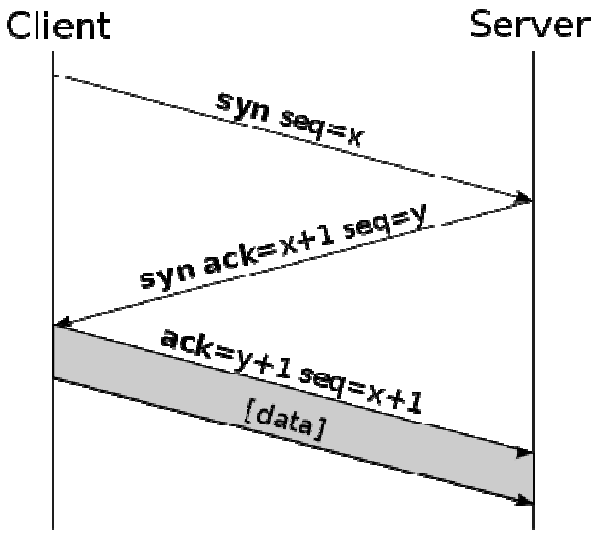


Fig. 46 Negociación en tres pasos TCP inicio de la comunicación

La segunda etapa en TCP es la trasferencia de datos, pero ya que esta comunicación se realiza utilizando SSL/TLS para transferir los datos cifrados, el cliente y el servidor se ponen de acuerdo en el formato en que van a enviar la información cifrada, este consenso

lo realiza el protocolo Record (Registro) SSL/TLS y se apoya en los algoritmos acordados en el protocolo Handshake.

Luego que se inicia la comunicación con TCP se inicia el intercambio de información con SSL/TLS aquí el cliente envía un mensaje **Cliente Hello** a través del protocolo handshake donde indica la versión TLS que soporta, la creación de la sesión, el conjunto de algoritmos para mantener la confidencialidad y autenticación de la comunicación (**Fig. 47**)

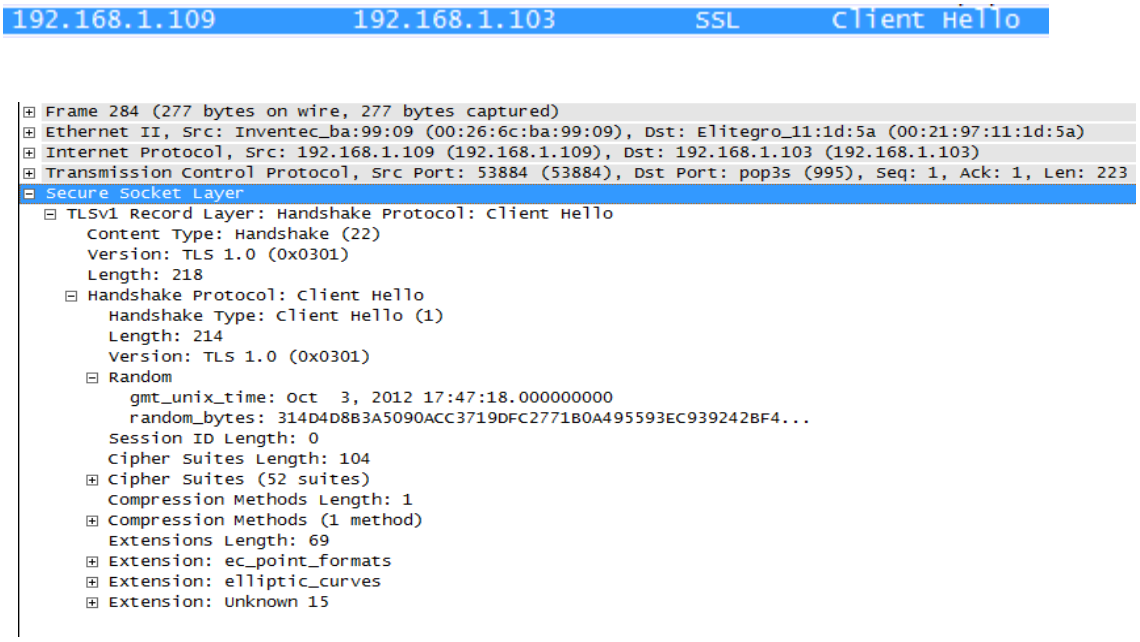
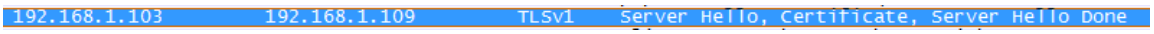


Fig. 47 Inicio de intercambio de información con SSL/TSL: Client Hello

El servidor de Correo le dice al cliente que su mensaje ha sido recibido por medio de TCP

Le envía un mensaje **Server Hello** utilizando el protocolo TLSv1 (Ver **Fig. 48**) el cual especifica el conjunto de algoritmos que se utilizaran para cifrar de toda la suite que ha indicado el cliente que posee, también el servidor le envía el certificado que lo identifica, su llave publica, periodo de validez, nombre de la AC que emitió el certificado, firma digital de la AC y otros datos más que indican cómo puede usarse el certificado.



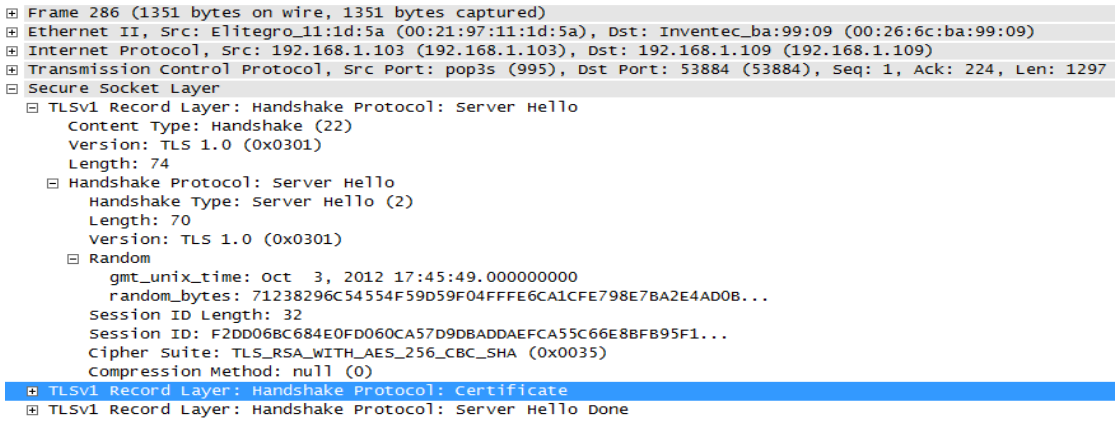


Fig. 48 Mensaje Server Hello

El certificado y los datos de la Autoridad Certificadora que se intercambian con el protocolo Handshake se muestra en la **fig. 49**.

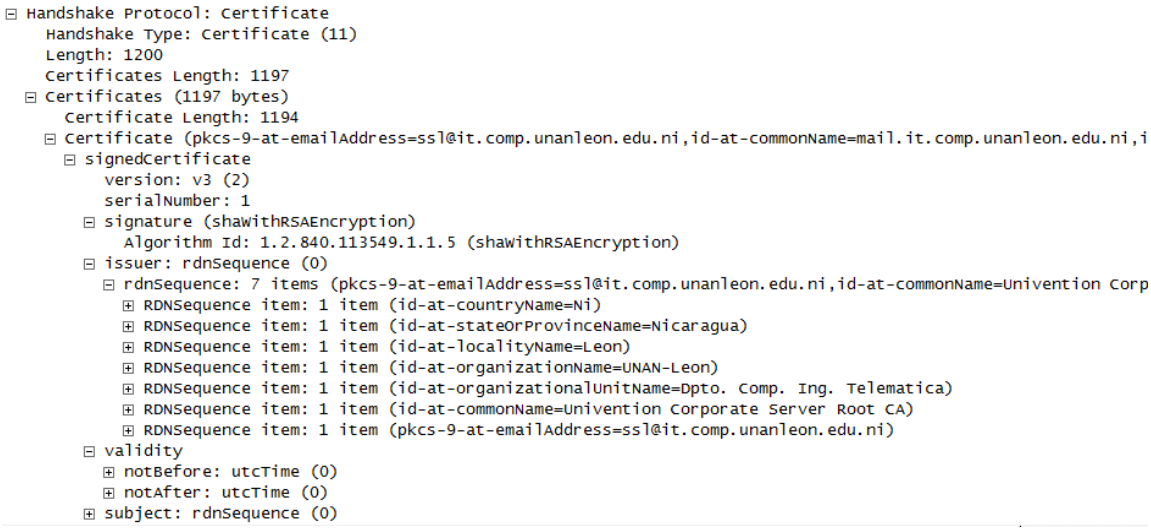


Fig. 49 Certificado enviado por el Servidor

Usando todos los datos generados en el handshake hasta ahora, el cliente (con la cooperación del server, y dependiendo del cipher siendo usado) crea el **premaster secret** para esta sesión, lo encripta con la clave pública del server (la cual se obtuvo del certificado del server que éste mandó), y envía el premaster secret encriptado hacia el server con el mensaje **Mensaje ClientKeyExchange** ver la **fig. 50** siguiente.

Durante este intercambio de información el protocolo Record está haciendo su trabajo, captando los componentes que necesita como campos de longitud, la descripción y contenido, al finalizar las fases del protocolo Handshake el protocolo Record toma los mensajes a transmitir, fragmenta los datos en bloques manejables, opcionalmente comprime los datos y aplica un MAC, cifra y transmite el resultado, al recibir los datos descifra, verifica, vuelve a montar descomprimir y luego entrega al más alto nivel POP3s en el puerto 995 y los clientes (Outlook).

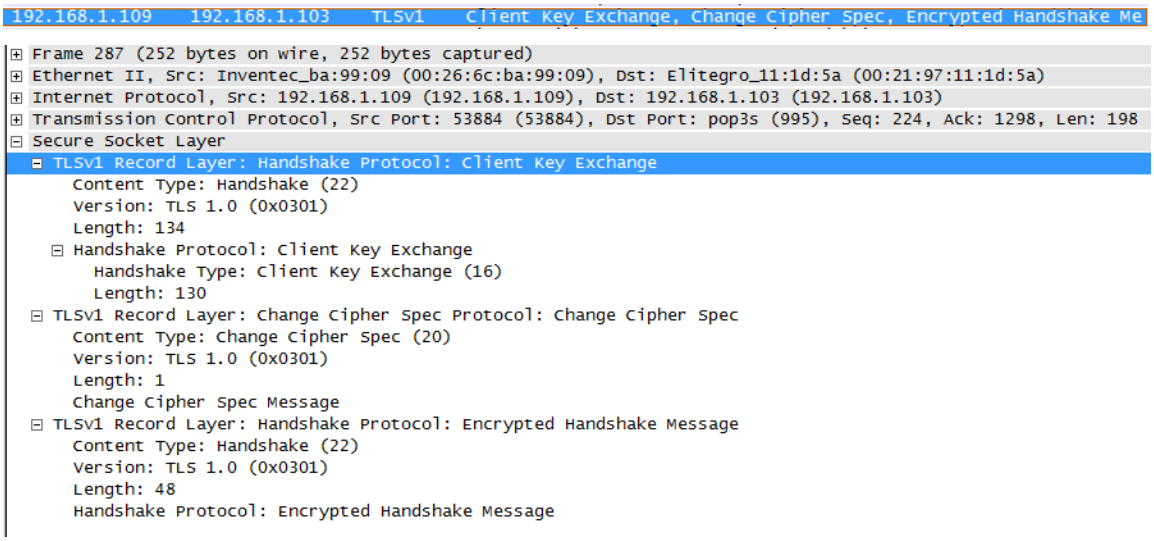
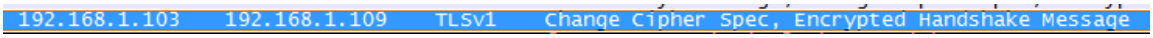


Fig. 50 Mensaje Cliente Key Exchange

Ahora el servidor le envía la indicación del inicio de la sesión en un canal seguro



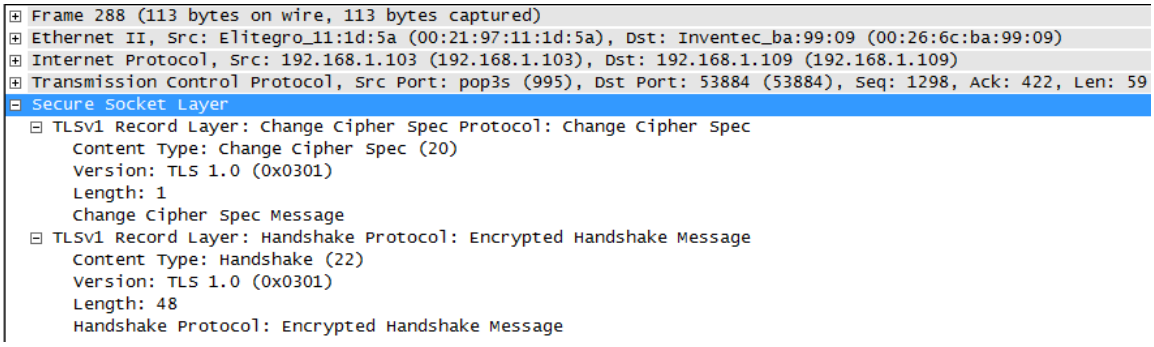


Fig. 51 Inicio de sesión en el canal seguro

El cliente manda una **ACK** indicando que ha recibido el mensaje del servidor esto con TCP. Con estos mensajes que se han intercambiado el cliente y el servidor se ha creado he iniciado la sesión en un canal seguro y se realiza el intercambio de datos desde la capa de aplicación como la comunicación se realiza utilizando el cliente de Windows Outlook se utiliza el protocolo POP en la capa de Aplicación donde los datos que trasmita este protocolo son cifrados.

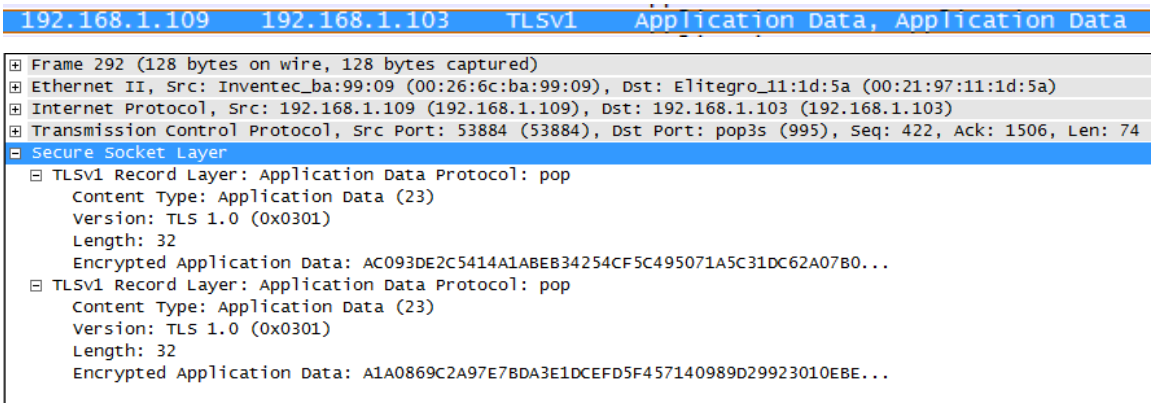
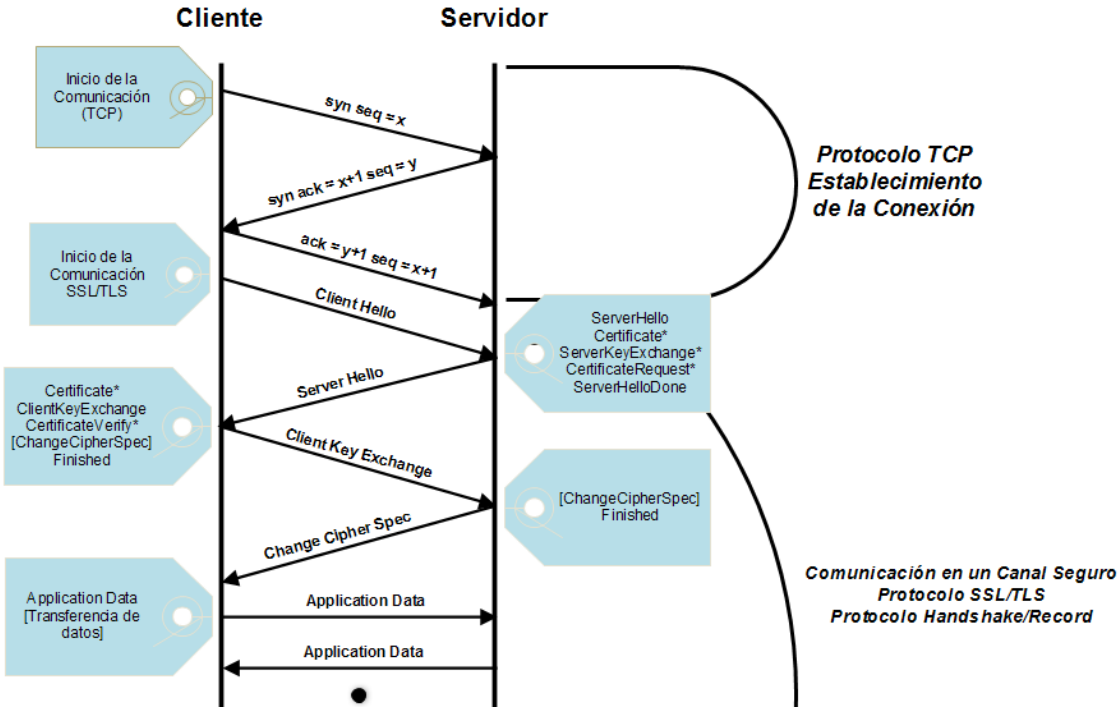


Fig. 52 Datos del nivel de Aplicación

Al finalizar la transmisión desde la capa de aplicación, el servidor envía un **FIN, ACK** ya que él conoce la longitud del mensaje y sabe cuándo el cliente ha terminado de transmitir todos los datos. El cliente indica su recibo con un **ACK** y envía un mensaje **Encrypted Alert (21)** que es una alerta de TLSv1 al recibir un **ACKs FIN**. Indicando el final de la

comunicación en un canal seguro con SSL/TLS. Ahora el cliente finaliza la comunicación con TCP enviando un **FIN, ACK** y el servidor envía un **RST** preguntando si desea reiniciar la conexión.

En la siguiente **fig. 53** está el esquema de intercambio de mensajes entre el cliente y el servidor desde que inicia la comunicación con TCP y el establecimiento del canal seguro por medio del protocolo Handshake SSL/TLS, hasta que se cierre la conexión TCP:



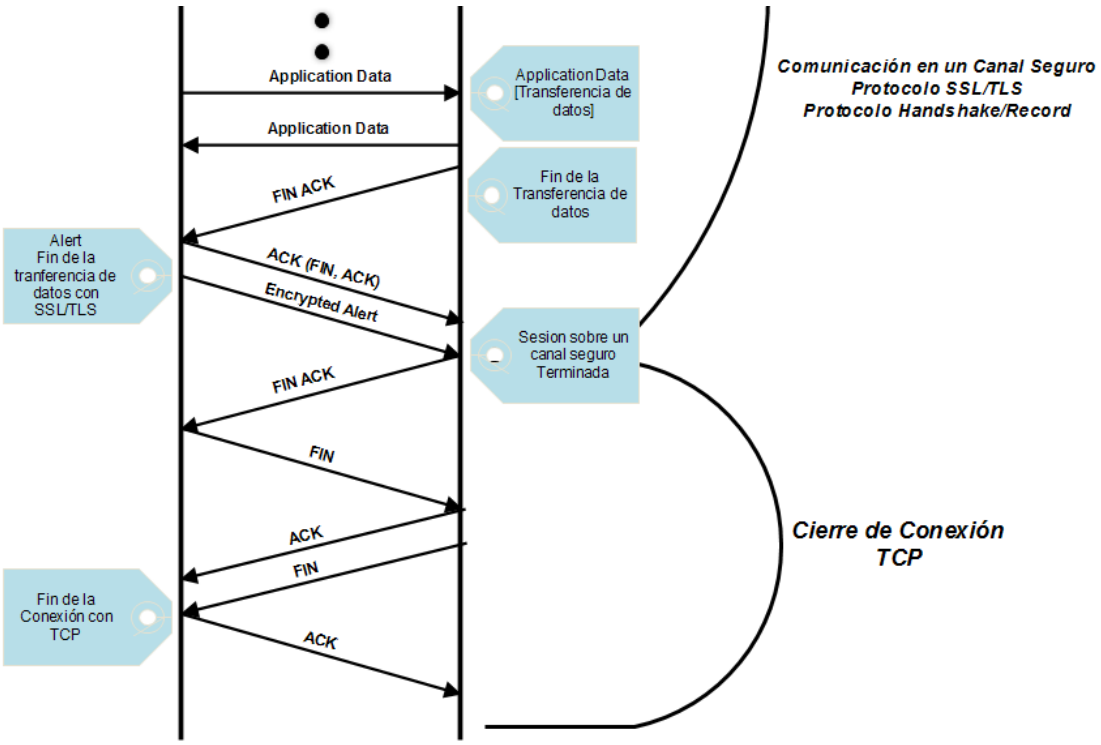


Fig. 53 Comunicación Cliente-Servidor TCP/SSL/TLS

VIII. CONCLUSIONES

La utilización del sistema operativo Univention Corporate server facilito el manejo e implementación de Open Xchange como la herramienta de almacenamiento y administración del correo electrónico aprovechando toda la robustez de este software.

Las herramientas de seguridad como el protocolo TLS y la implementación de una autoridad certificadora para el manejo de certificados digitales asociados a la configuración del servidor de correo electrónico ofrecen un canal de comunicación seguro para el acceso al servidor de correo ofreciendo autenticación, confidencialidad, integridad y privacidad de los dato intercambiados entre los usuarios.

Para el rechazo de Spam y virus se implementó como mecanismo de seguridad Spamassassin, ClamAV, Amavis-new y el filtro anti-spam que viene incorporado en Open Xchange que permite proteger de amenazas a los archivos adjuntos e impiden que las cuentas de correo electrónico se llenen de mensajería no deseada.

IX. RECOMENDACIONES

Mejorar los mecanismos de seguridad con el cifrado de los mensajes desde el nivel de aplicación implementando S/MIME para obtener las firmas digitales y el no rechazo y se fortalecen los servicios de seguridad con los protocolos seguros brindando un completo servidor de correo electrónico seguro.

Utilizar Open-Xchange como una alternativa Open Source ya que muchos proyectos son el resultado de la colaboración de desarrolladores de todo el mundo por esto el software es más robusto, eficiente y está mejor documentado que sistemas privados.

Desarrollar un módulo que ofrezca la opción de registrarse en el servidor de correo electrónico desde la interfaz web haciendo uso de la API de JAVA que proporciona el OXtender de Open Xchange Server.

Implementar los mecanismos que ofrece el sistema operativo Univention Corporate Server como Active Directory, Samba, LDAP y Kerberos para aprovechar sus beneficios y ofrecer un sistema de administración de grupos de usuarios y servicios con una autenticación segura sobre cualquier topología de red.

X. BIBLIOGRAFIA

Documentación (Libros, Artículos,)

[1] Br. Martha María Berrios Reyes M.M.B.R y Br. Ana Junieth Blandón González A.J.B.G (León, Agosto del 2006, UNAN-León) Configuración e Instalación de un completo servidor de correo con Postfix y Cyrus.

[2] Lic. Liuva Pastran Paniagua, Lic Karen Adalis Salís Salinas (León, Nicaragua, Diciembre del 2007) Configuración de Servidor Web y de Correo Electrónico en Red Hat.

[3] Ing. Jesús Manuel Puetate Espinoza (Riobamba - Ecuador 2009) Estudio de los Protocolos de Seguridad del Servicio de Correo Electrónico para Implementar un Webmail en el HCPCH.

[4] Univention GmbH, Mary-Somerville-StraBe 1 ((c) 2002 bis 2011) Univention Corporate Server Version 2.4-4.

[5] Br. Juan Carlos Bordas Montoya, Br. Arllen Javier Díaz Cáceres, Br. Nubia Consuelo Espinoza García. (León - Nicaragua, 2011) Configuración y Administración de Open-Xchange Server bajo la plataforma Linux.

Direcciones Web:

[6] Definición de autoridad certificadora y certificados
http://www.uned.es/csi/reduned/ca/

[7] SSL -Documentación- Configuración y descripción del proceso de creación
http://es.scribd.com/doc/12935728/SSL-en-debian-etch-

[8] Configuración de SMTP IMAP seguros y Open-Xchange Server
http://linuxsilo.net/articles/

http://gpl.netixia.com/openxchange/openxchange-sarge-howto.html
http://www.x-tend.be/~raskas/openxchange/
http://open-xchange.org/oxwiki/OXDebianSargeFromPackage

[9] Certificados
http://www.cacert.org/index.php?id=3

[10] Definición de los complementos del correo electrónico
http://jpertuz.wordpress.com/servidor-imap-y-pop/

[11] Protocolos y configuraciones CA
http://doc.otrs.org/3.0/en/html/smime.html

[12] http://www.ijs.si/software/amavisd/
Antivirus y anti-Spam Documentación: interfaz (Amavis-New)

[13] Protocolo Handshake
http://reocities.com/SiliconValley/byte/4170/articulos/tls/tls-hp.htm

[14] RFC de SSL/TLS
http://tools.ietf.org/html/rfc5246

[15] Protocolo TLS
http://www.monografias.com/trabajos74/protocolo-tls-transport-layer-security/protocolo-tls-transport-layer-security2.shtml

[16] Transmisión del protocolo Handshake
http://es.wikipedia.org/wiki/Transmission_Control_Protocol

[17] Análisis de Comunicación del canal seguro
http://seguridadyredes.wordpress.com/2010/05/28/wireshark-tshark-analisis-correo-entrante-imap-starttls-e-imap-idle-parte-2/

XI. ANEXOS

Diagrama de Arquitectura de Open-Xchange Server:

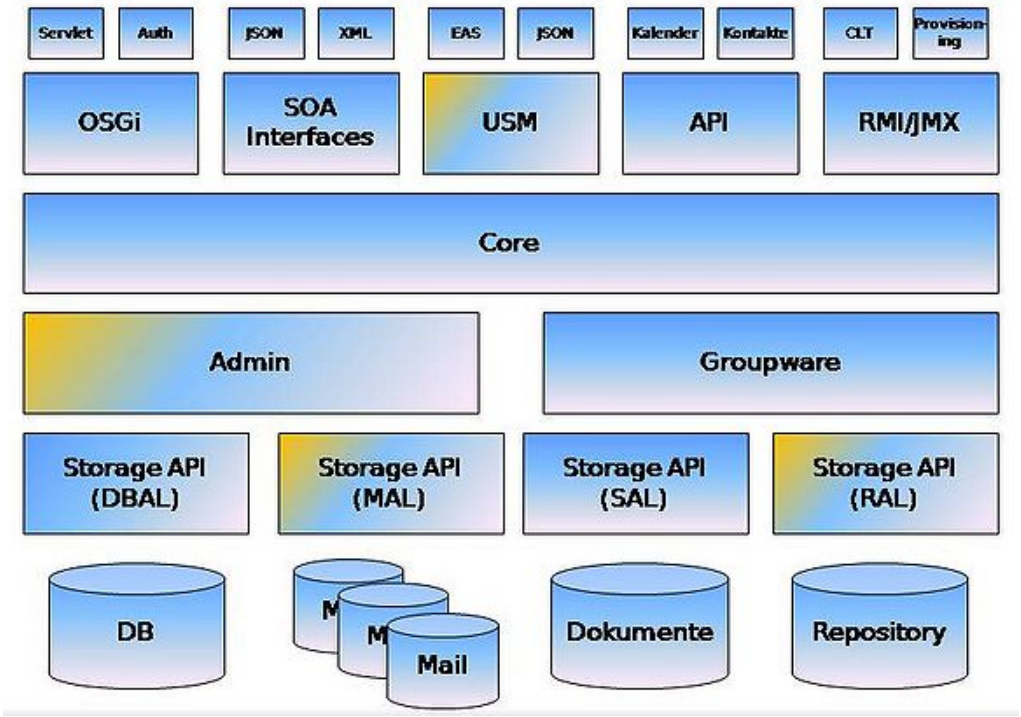


Fig. 54 Diagrama de Arquitectura de Open-Xchange Server

Arquitectura de Open-Xchange Server:

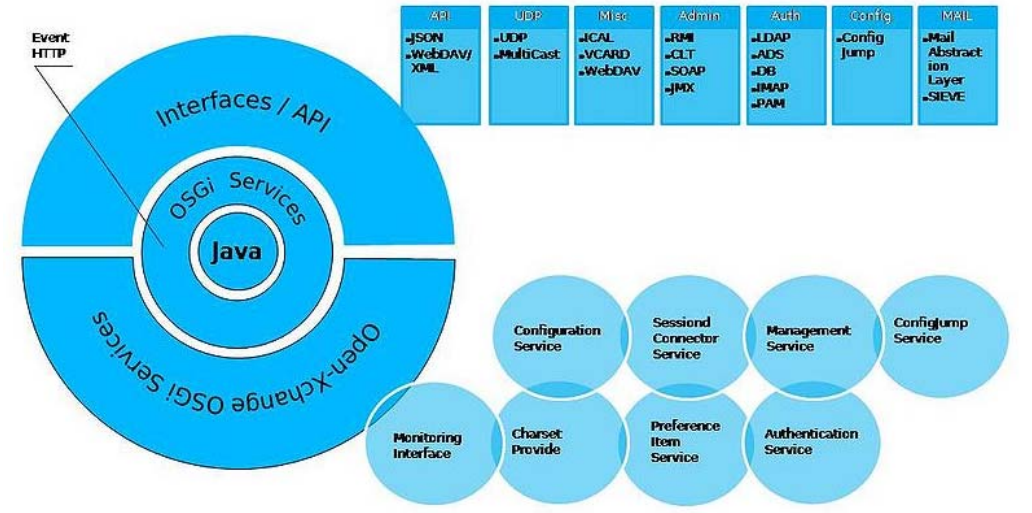


Fig. 55 Arquitectura de Open-Xchange Server

Arquitectura

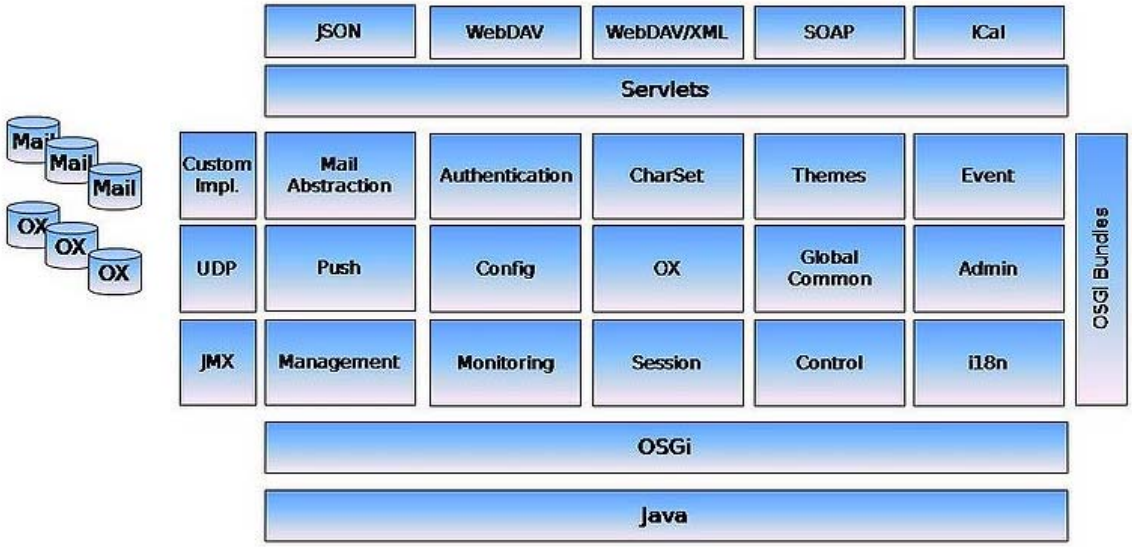


Fig. 56 Arquitectura

Open-Xchange Server Diagrama de Arquitectura WebGUI

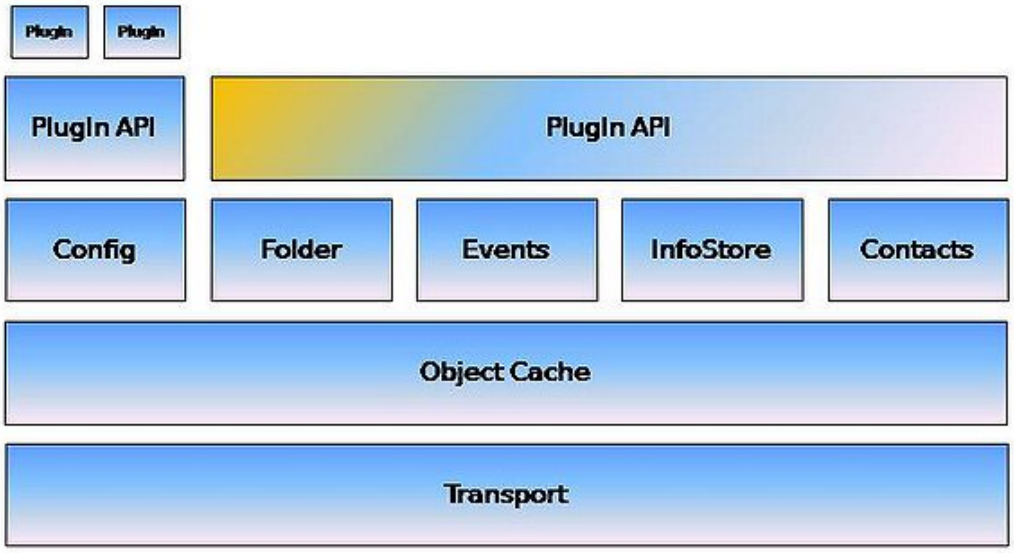


Fig. 57 Diagrama de Arquitectura WebGUI

Configuracion de una cuenta de correo electronico con Outlook 2010

En la pestaña Archivo ir a Configuracion de la cuenta y hay se creara una nueca cuenta la siguiente imagen ilustra la configuracion de la cuenta:

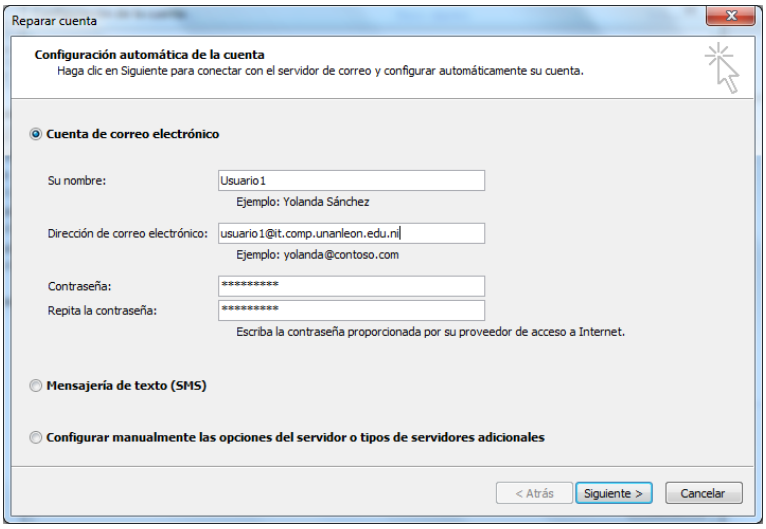


Fig. 58 Configuración de la cuenta de usuario

Chequear la opción de configuración manualmente y Siguiente:

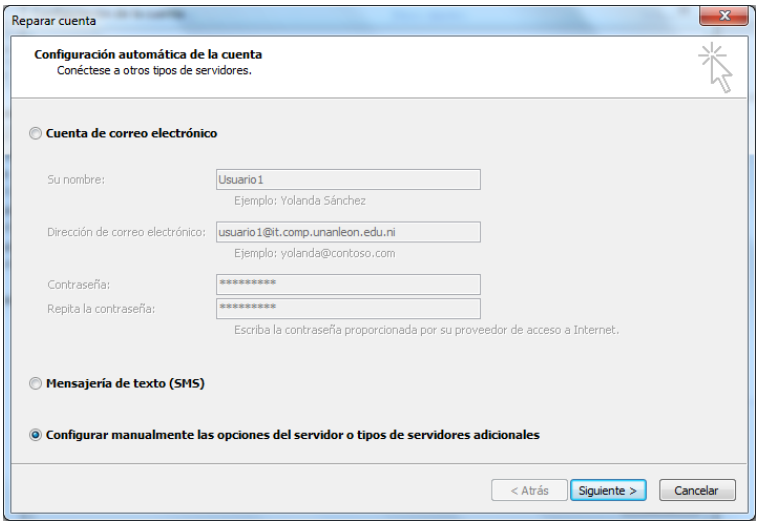


Fig. 59 Opción de configuración manualmente

Ahora aquí se establece la configuración de la cuenta del usuario luego de haberla creado en el servidor de correo su cuenta de correo y su contraseña, también se especifica la dirección del servidor de correo y el protocolo de comunicación por defecto que indica es POP3.

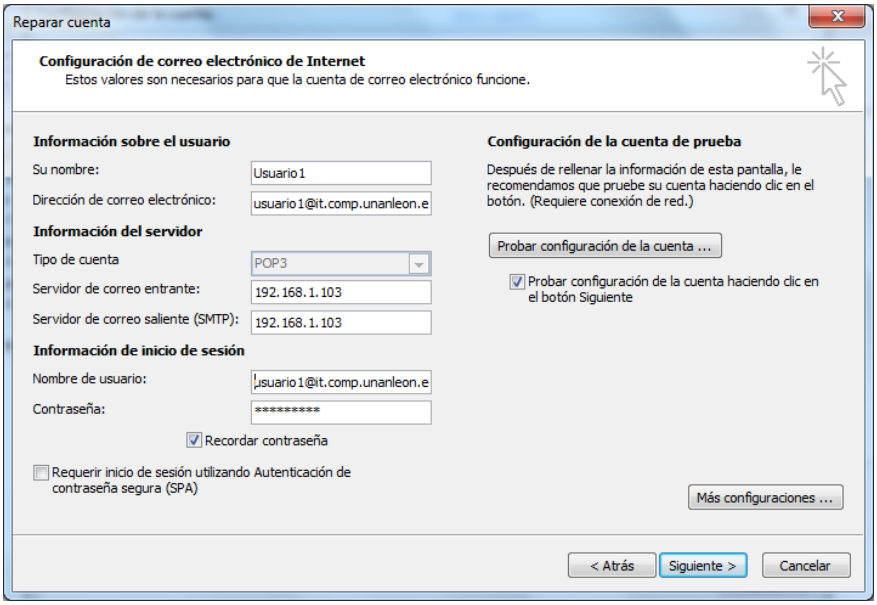


Fig. 60 Información de Servidor de Correo

En Mas Configuraciones se indica la siguiente opción:

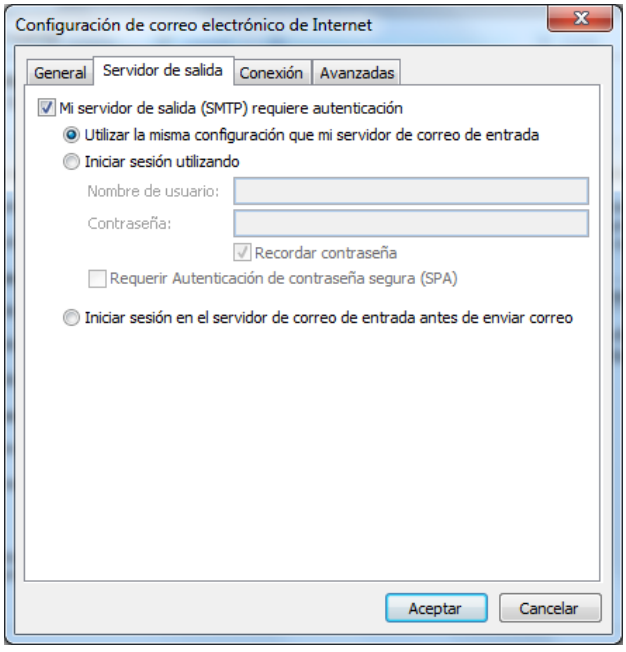


Fig. 61 Configuración Avanzada

Luego probar la configuración de la cuenta: donde se inicia la sesión de la cuenta configurada en el cliente Outlook y se envía un mensaje de prueba si esto no sufre problemas la configuración se completado correctamente.

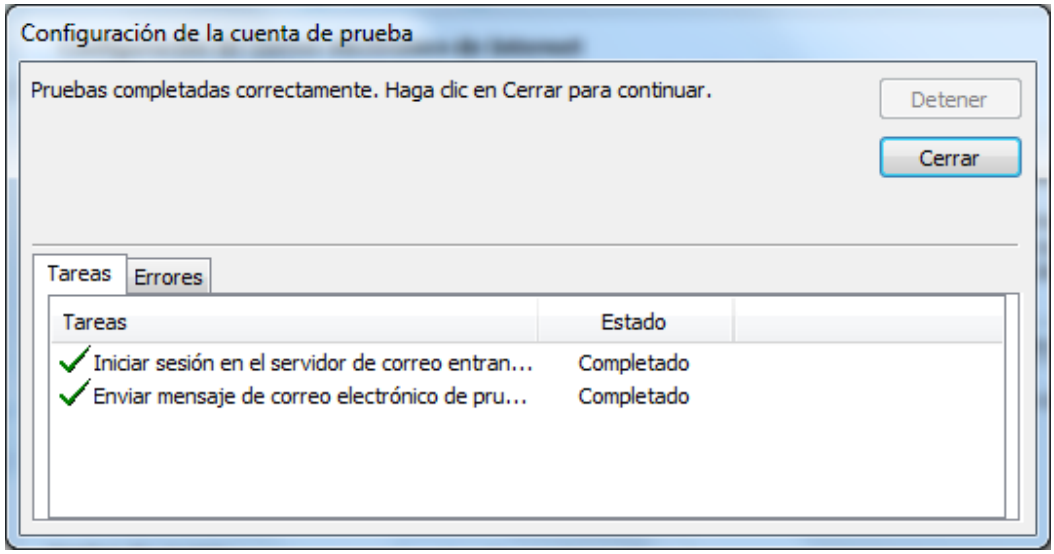


Fig. 62 Prueba y Sincronización de Configuración

Ahora ya está configurada la cuanta del usuario en el cliente de Windows Outlook 2010

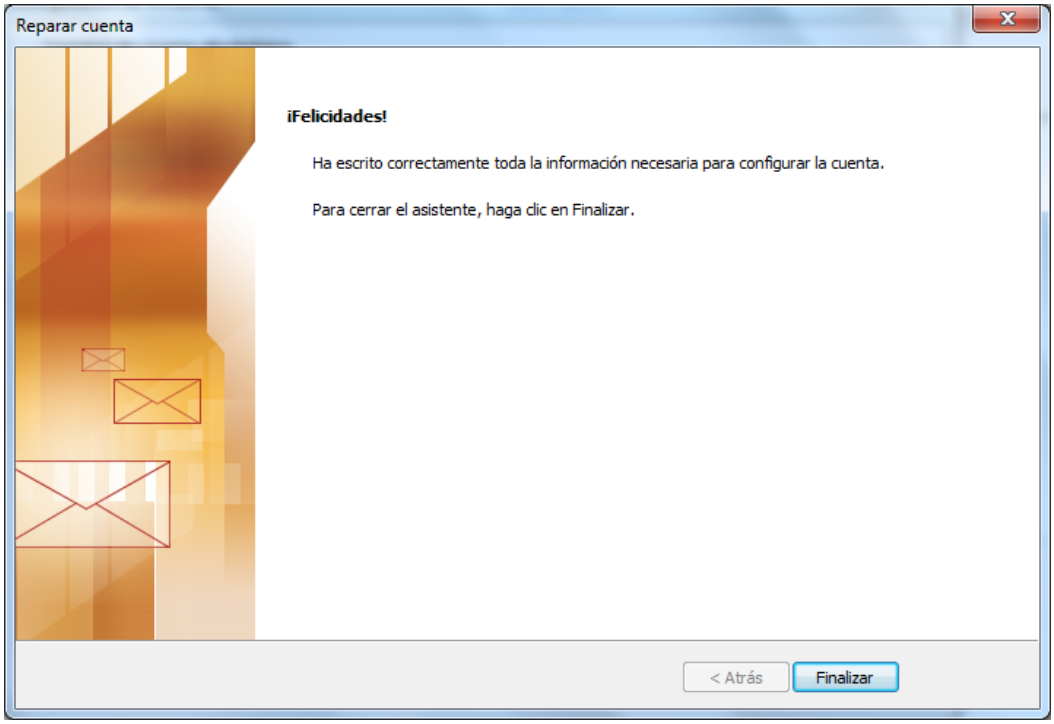


Fig. 63 Fin de la configuración

Instalación y Configuración del Servidor DNS en Ubuntu 10.04

Para instalar los paquetes para el servicio de bind9 se ejecuta la siguiente línea de comando:

```
apt-get instal bind9
```

Luego de finalizar la instalación ir a la ruta de los archivos de configuración del bind9 **/etc/bind/**

Ahora en el fichero **named.conf.default-zones** es donde se crean las zonas de los dominios con los cuales se va a trabajar en el trabajo es para el dominio de it.comp.unanleon.edu.ni:

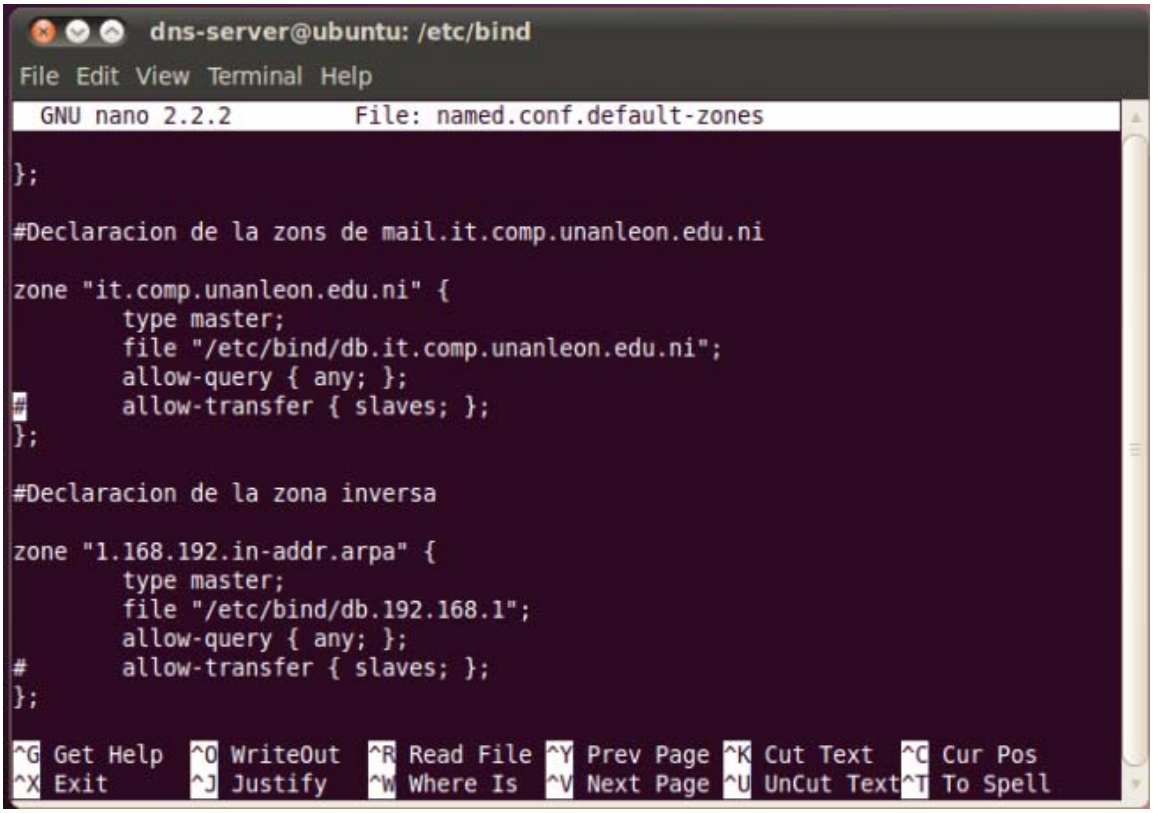


Fig. 64 Creación de zonas

Una vez declarada las zonas se debe crear los archivos de datos de las zonas declaradas para esto se realizara a partir de los ficheros db.127 y db.255

cp db.127 db.it.comp.unanleon.edu.ni

cp db.255 db.192.168.1

El fichero **db.it.comp.unanleon.edu.ni** debe tener la siguiente configuración:

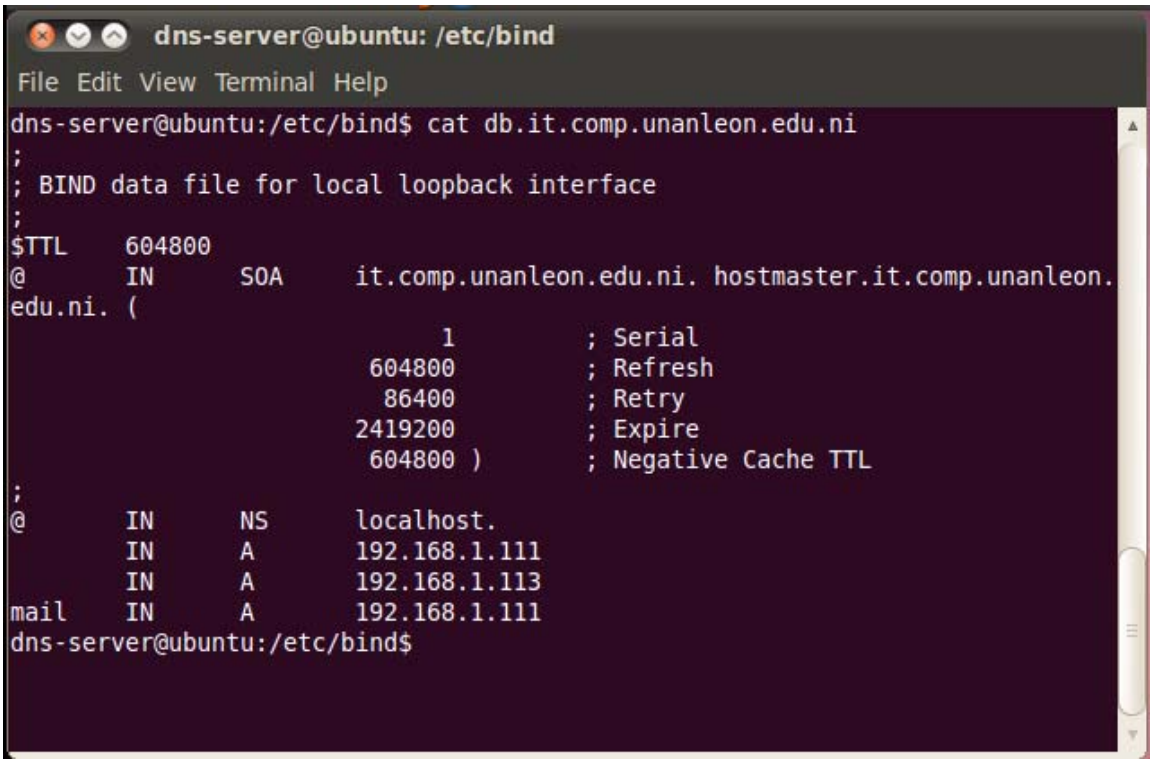


Fig. 65 Creación de zona inversa 1

Fichero **db.192.168.1**

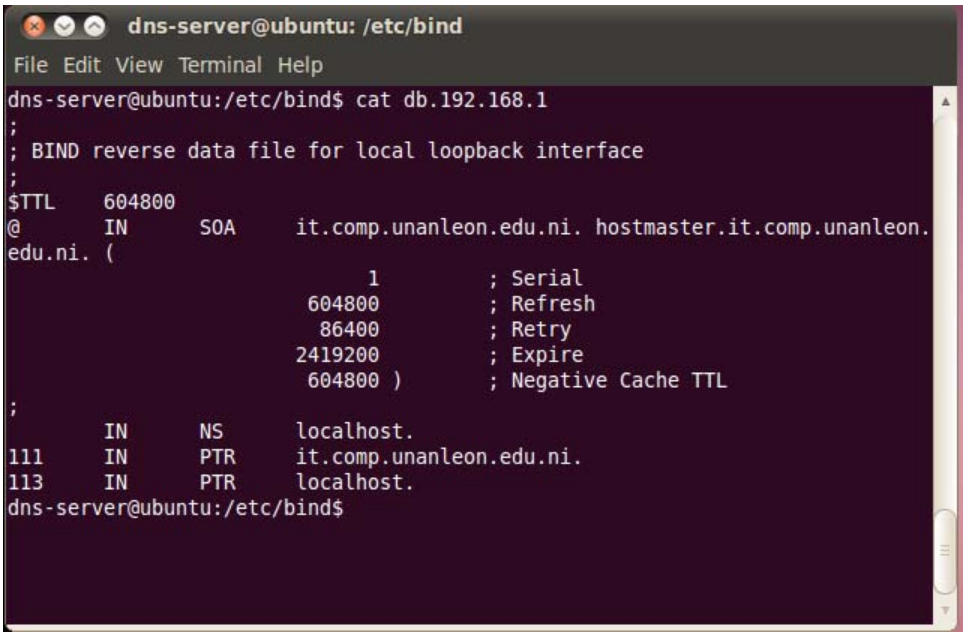


Fig. 66 Creación de zona inversa 2

Ahora ya están creados los archivos necesarios en la configuración del Servidor DNS

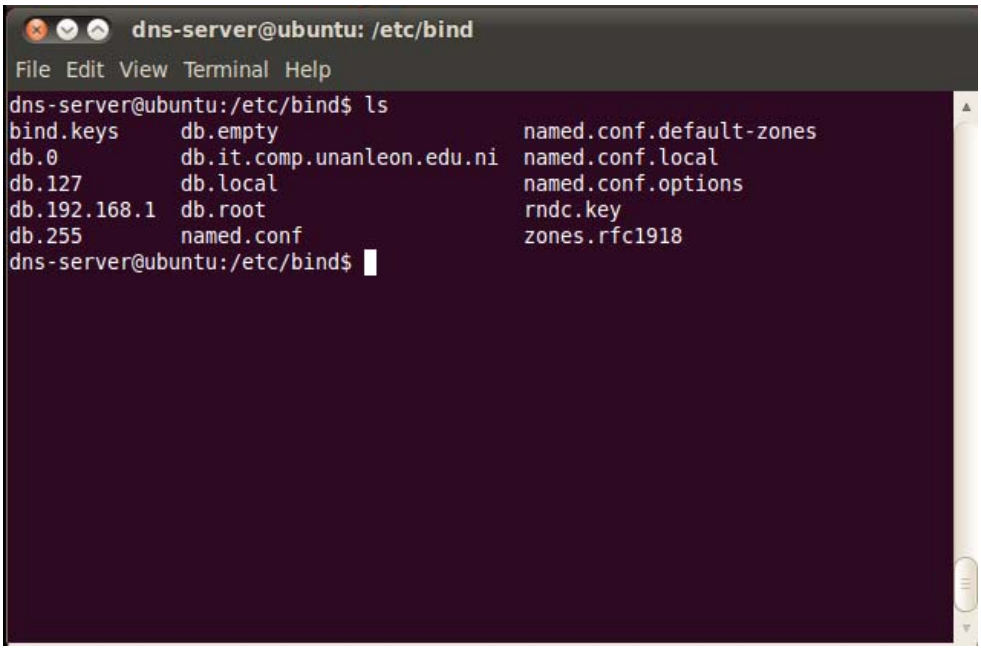


Fig. 67 Ficheros de configuración

Verificar el fichero **named.conf.option** con la siguiente configuración:

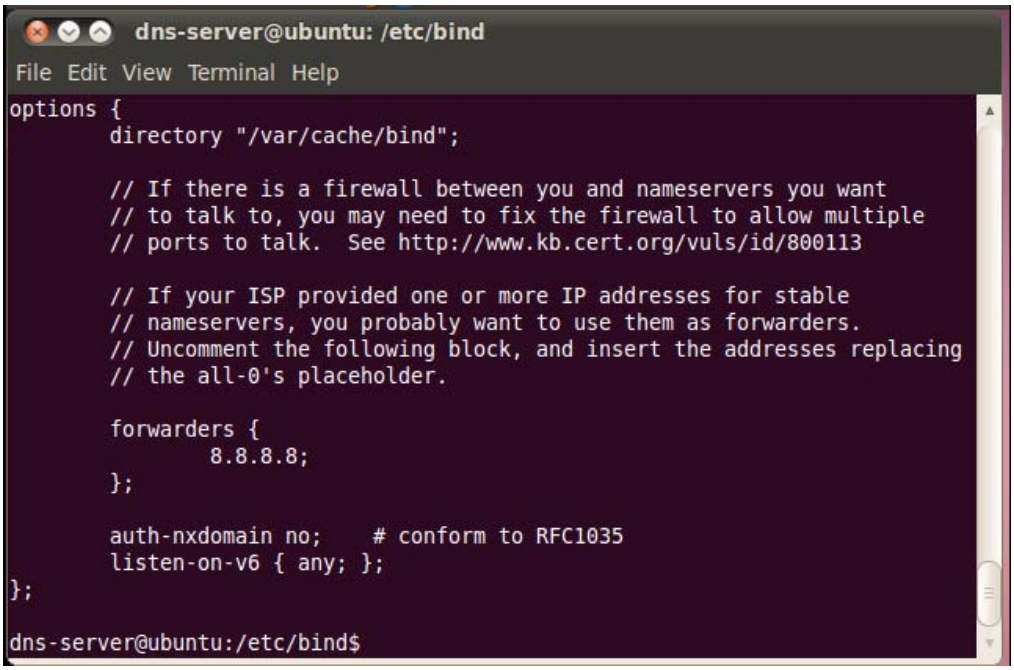


Fig. 68 Fichero named.conf.Option

Se debe reiniciar el servicio:

```
/etc/init.d/bind9 restart
```

Para verificar el correcto funcionamiento del servicio DNS utilizar los siguientes comandos:

```
$ dig www.it.comp.unanleon.edu.ni

$ host it.comp.unanleon.edu.ni

$ nslookup it.comp.unanleon.edu.ni
```

Si surge algún problema con la configuración del servicio utiliza:

named-checkconf: Que es un analizador de sintaxis que nos permitirá revisar si nuestro archivo de configuración está bien diseñado.

named-checkzone: Que es un analizador sintáctico de las zonas que creamos.

named-compilezone: Es similar a la **llamada-checkzone,** pero siempre se vuelca el contenido de la zona en un archivo especificado en un formato especificado.