SOLUCIÓN PARA EL MEJORAMIENTO DEL SERVICIO DE CORREO ELECTRÓNICO EN LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA.

DAVID FERNANDO ANDRADE SOLANO.
VÍCTOR ANDRÉS CASTRO DUEÑAS.

Documento final de trabajo de grado para optar al título de Ingeniero en Electrónica y Telecomunicaciones

Director

GUEFRY LEIDER AGREDO MENDEZ
Ingeniero en Electrónica y Telecomunicaciones

UNIVERSIDAD DEL CAUCA
FACULTAD DE INGENIERÍA ELECTRÓNICA Y TELECOMUNICACIONES
DEPARTAMENTO DE TELECOMUNICACIONES
POPAYÁN
2012

TABLA DE CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

LISTA DE ACRÓNIMOS

MTA*:* *Mail Transport Agent*, Agente de Transporte de Correo.

MDA: *Mail Delivery Agent,* Agente de Reparto de Correo.

MUA: *Mail User Agent,* Agente de Usuario de Correo.

SMTP*:* *Simple Mail Transfer Protocol*, Protocolo Simple de Transferencia de Correo.

POP: *Post Office Protocol*, Protocolo de Oficina de Correo Postal.

IMAP*:* *Internet Message Access Protocol*, Protocolo de Acceso a Mensajes de Internet.

TCP: *Transmission Control Protocol,* Protocolo de Control de Transmisión.

ESMTP: *Enhanced Simple Mail Transfer Protocol*, Protocolo Simple de Transferencia de Correo Mejorado.

MIME: *Multipurpose Internet Mail Extensions,* Extensiones Multipropósito de Correo de Internet.

GNU: *GNU is not Unix,* GNU no es Unix.

SPF: *Sender Policy Framework,* Entorno de Políticas del Remitente.

GPL: *General Public License*, Licencia General Pública.

DNS: *Domain Name System,* Sistema de Nombres de Dominio.

LDAP: *Lightweight Directory Access Protocol,* Protocolo Ligero de Acceso a Directorios.

SSL: *Secure Sockets Layer*, Nivel de Sockets Seguro.

TLS: *Transport Layer Security,* Protocolo de Seguridad del Nivel de Transporte.

SASL: *Simple Authentication and Security Layer,* Protocolo de Autenticación Simple y Nivel de Seguridad.

DNSBL: *DNS Black List,* Listas Negras Basadas en DNS.

UTM: *Unified Threat Management,* Gestión Unificada de Amenazas.

UML: *Unified Modeling Languaje*, Lenguaje Unificado de Modelado.

FLOSS: *Free/Libre and Open Source Software,* Software de Código Abierto y de Software Libre.

OpenBRR: *Open Business Readiness Rating,* Puntuación para la Preparación de Negocios Abiertos.

QSOS: *Qualification and Selection of Open Source software,* Calificación y Selección de Software de Código Abierto.

OSMM: *Open Source Maturity Model,* Modelo de Madurez de Código Abierto

QualOSS: *QUALity of Open Source Software,* Modelo de Calidad de Software de Código Abierto.

OMM: *QualiPSo Open Source Maturity Model,* el Modelo de Madurez de Código Abierto.

DKIM: *Domainkeys Identified Mail,* Correo Identificado por Claves de Dominio.

INTRODUCCIÓN

Debido a la constante evolución de las tecnologías de información se han creado diversos servicios que son ofrecidos a través de un sistema de telecomunicaciones, estos servicios a medida que pasa el tiempo imponen mayores exigencias en el desempeño y la capacidad de los elementos hardware y software, debido a que se busca desarrollar y ofrecer servicios de mejor calidad y de mayor seguridad para los usuarios.

El servicio de correo electrónico es uno de los servicios más utilizados por los usuarios y por tal motivo, se considera uno de los más importantes en Internet. Este servicio permite a los usuarios enviar y recibir mensajes, aunque existen varios aspectos que se deben tener en cuenta para que esta tarea se pueda realizar de manera segura y confiable, sabiendo que el correo electrónico además de representar al propio usuario que lo emite, también está representando al dominio al que pertenece.

A medida que ha pasado el tiempo han aparecido amenazas que afectan el desempeño del servicio como es el caso de los virus, ataque externos que puede sufrir el sistema o la circulación de *spam*[1], que además de ser una molestia para el usuario, ocupa los recursos de almacenamiento del sistema.

Un aspecto importante a tener en cuenta en el servicio de correo electrónico es la autenticación de usuarios, esto permite evitar la suplantación de cuentas, verificando que el usuario que está enviando el mensaje es el verdadero remitente, de esta manera se pueden aumentar los niveles de seguridad en el servicio reduciendo el envío de *spam*.

Las contraseñas que utilizan los usuarios para poder acceder al servicio de correo electrónico también son de gran importancia, estas son propias de cada usuario y para manejo exclusivo de su información, por lo tanto, la robustez de éstas es primordial para que no sean fáciles de descifrar y de esta manera proteger los mensajes.

De acuerdo a los aspectos y problemas descritos anteriormente, se evidencia la necesidad de una revisión detallada al proceso de autenticación y control de *spam* en el servicio de correo.

En este documento se presenta un aporte a la solución de esta problemática del servicio de correo electrónico de la Universidad del Cauca, de tal manera que con el uso de herramientas software y disponiendo de las adecuadas configuraciones en los servidores, se pueda actuar ante las amenazas que se presentan en la red.

Este documento se divide en cuatro (4) capítulos, en el primero se detalla el sistema actual del correo de la Institución y las falencias que éste presenta y que son de mayor interés para solucionar por parte de la administración del área de Servicios de Internet de la División de TIC de la Universidad del Cauca, también se presenta la captura de

[1] *Spam*: mensajes de correo electrónico no deseado

requerimientos para atender a las necesidades del sistema de correo. En el segundo capitulo se muestran los parámetros de selección y la evaluación de las herramientas que se van a utilizar para contribuir a las soluciones de las falencias presentadas en el primer capítulo y por último se presentan las mejoras implantadas en el sistema de correo con las respectiva descripción de cada uno de los elementos integrados. El tercer capítulo evidencia las pruebas de las configuraciones realizadas y de las herramientas usadas y se encuentran las evidencias de que el sistema ya cuenta con las mejoras requeridas. El cuarto capítulo contiene las conclusiones que se obtuvieron al desarrollar este trabajo y algunas recomendaciones que se deben tener en cuenta para la utilización del servicio de correo.

Las instalaciones y las configuraciones realizadas, se exponen en los documentos anexos. En el Anexo A se presenta la teoría acerca del correo electrónico, este es un anexo de generalidades con el fin de tener mayor claridad de lo que se está trabajando. En el Anexo B se muestra un soporte escrito generado por el ingeniero Jefe del área de Servidores y Servicios de Internet de la División de TIC de la Universidad del Cauca en donde expone su satisfacción en relación a los parámetros escogidos para evaluar las Herramientas *antispam.* El Anexo C contiene la aplicación de la metodología de evaluación de software para la selección de la herramienta *antispam* y en el Anexo D se muestra la configuración de un servicio de correo electrónico con las herramientas necesarias para su implementación. En el Anexo E se encuentran las configuraciones realizadas a las herramientas *antispam* utilizadas, el Anexo F contiene la configuración de la autenticación y cifrado para el sistema de correo. En el Anexo G se exponen las configuraciones para contar con un sistema de verificación de robustez de contraseñas y en el Anexo H se presenta las configuraciones de los clientes de correo que fueron necesarios para realizar las pruebas de envío de mensajes, finalmente en el Anexo I se encuentra la carta en la cual se certifica por parte de la red de servicios que los objetivos de este trabajo han sido cumplidos.

Con las soluciones presentadas en este trabajo de grado se busca ofrecer un servicio de correo electrónico con menor *spam* y más robusto por parte de la Institución, basándose en la seguridad, integridad y confiabilidad del sistema.

CAPÍTULO 1.

1 SISTEMA DE CORREO ELECTRÓNICO INICIAL DE LA UNIVERSIDAD DEL CAUCA

En este capítulo se presenta el sistema de correo electrónico actual de la Institución y las diferentes herramientas que lo componen, también se evidencia la problemática que se tiene en el servicio de correo electrónico identificadas por la administración del área de servidores de la División TIC de la Universidad del Cauca y de acuerdo a las falencias y necesidades en el sistema de correo se realizó la captura de requerimientos. Para un mayor entendimiento de los componentes de un sistema de correo se generó el Anexo A donde se encuentran las generalidades de un sistema de correo, la descripción del funcionamiento básico y de los protocolos necesarios.

1.1 DIAGNÓSTICO DEL ESTADO DEL SISTEMA DE CORREO DE LA UNIVERSIDAD DEL CAUCA

En esta sección se hace una descripción de los componentes del sistema de correo que se encuentra en funcionamiento en la Institución, para lo cual se ha elaborado un diagrama en bloques ilustrando el funcionamiento y las herramientas que se han considerado en cada uno de estos.

De acuerdo a diversas reuniones efectuadas en conjunto con el director del trabajo de grado, el coordinador Jefe del área de servidores y los desarrolladores de este proyecto, se obtuvo un esquema del sistema de correo electrónico actual de la Institución detallado en la Figura 1.1.

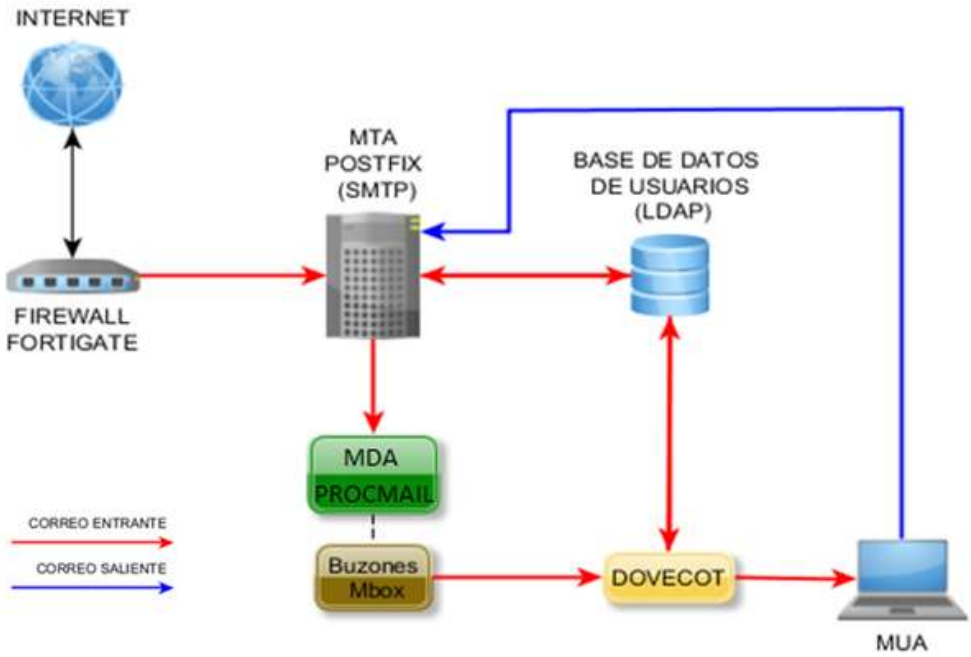


Figura 1.1 Sistema de correo actual de Unicauca.

A continuación se describe el funcionamiento del sistema representado en la Figura 1.1.

El control de *spam* en el sistema de correo de la Universidad del Cauca se realiza a través de la herramienta **FortiGate**[2], esta herramienta es la que recibe en primera instancia el correo enviado hacia el dominio de la Universidad del Cauca.

De acuerdo con [1], **FortiGate** es una plataforma de seguridad que ofrece protección y mayor rendimiento a la red en la que se encuentra operando. Presenta diversas funciones, algunas de ellas son:

- Antispam
- Firewall
- Antivirus
- Sistema de prevención de intrusión (IPS, *Intrusion Prevention System*)
- Soporte para IPv6

La plataforma utilizada en la Universidad del Cauca es la **FortiGate 310b**[3]**.** Esta contiene un sistema de Gestión Unificado de Amenazas (UTM, *Unified Threat Management*) [2], el cual se configura para hacer reconocimiento de múltiples amenazas en un único dispositivo. Para combatir estas amenazas, el UTM incluye *antispam*, antivirus y prevención de intrusión. Esta herramienta realiza control se *spam* para el correo que entra

[2] http://www.fortinet.com/products/fortigate/
[3] http://www.fortinet.com/products/fortigate/310B.html

al dominio de la Universidad, pero no para el correo saliente y tampoco para el correo interno de la Institución.

Aunque esta plataforma ofrece funciones de *antispam* y de antivirus, el área de Servidores y Servicios de Internet partió de una hipótesis que ha sido comprobada con el desarrollo de este proyecto, la cual era que con herramientas de Software Libre se pudiera aumentar la efectividad del control de *spam* ayudando a disminuir la cantidad de correo no deseado que se presenta en el servicio de correo electrónico. Por este motivo en el presente trabajo de grado se realizó la evaluación de herramientas de software libre para seleccionar y poner a funcionar de tal forma que se convirtiera en un mecanismo adicional para detectar y rechazar los mensajes *spam* que se le pasan al **Fortigate**

Si el mensaje que llega no se detecta como *spam*, pasa al Agente de Transporte de correo (MTA, *Mail Transport Agent*) para realizar la transferencia del mensaje al usuario final. El MTA que se utiliza en la Institución es **Postfix**[4], éste se comunica con la base de datos de usuarios para verificar la información de usuario. El almacenamiento de la información de usuarios se soporta en un servidor de Protocolo de Acceso Ligero a Directorios (LDAP, *Lightweight Directory Access Protocol*).

Cuando se encuentra el usuario correspondiente, se envía el mensaje a su buzón el cual maneja un formato *Mbox* para su almacenamiento, pero antes de esto, el mensaje pasa por el Agente de Reparto de Correo (MDA, *Mail Delivery Agent)* **Procmail**[5] que al mismo tiempo actúa como filtro de *spam,* realizando una última revisión antes de que el mensaje sea ingresado al buzón.

Para la lectura de los mensajes por parte del usuario se necesita de un servidor que maneje Protocolo para Acceso a Mensajes de Internet (IMAP, *Internet Message Access Protocol*) que normalmente se refiere como servidor IMAP. Este permite la recuperación del correo desde el buzón, verificando antes que el usuario que solicita la lectura del mensaje sea un usuario del dominio y su información se encuentre en el servidor de directorio LDAP. El servidor IMAP que utiliza el sistema de correo de la Universidad del Cauca es **Dovecot**[6]**.**

Para el correo saliente, el cliente se comunica por medio del Agente de Usuario de Correo (MUA, *Mail User Agent*), directamente con el servidor de correo sin antes hacer una revisión previa en el contenido de los mensajes con fines de realizar control de *spam*. El servidor de correo se encarga de realizar la transferencia del mensaje hacia otros dominios.

A continuación se realiza una descripción acerca de LDAP y del almacenamiento de usuarios mediante directorios. El almacenamiento de la información de los usuarios del

[4] http://www.postfix.org/
[5] http://www.procmail.org/
[6] http://www.dovecot.org/

servicio de correo electrónico de la Universidad de Cauca, se encuentra basado en el esquema de directorios LDAP.

Un directorio LDAP es semejante a tener una base de datos que contiene información de usuario de forma descriptiva, esto quiere decir que almacena los datos del usuario con algunos atributos que caracterizan a este mismo. Una de las particularidades de los directorios LDAP es que son utilizados normalmente para realizar consultas acerca de la información que estos contienen y muy pocas veces para hacer modificaciones de la misma. Una de las principales características que tiene LDAP es que permite acceder de manera estándar y rápida a la información, esto debido a la forma en que ésta es almacenada y la forma en que puede ser consultada, ya que se puede realizar la búsqueda de diferentes maneras de acuerdo a las especificaciones del usuario que se encuentren en el directorio. En cuanto a flexibilidad de manejar LDAP, se encuentra la posibilidad de que la información almacenada en los directorios LDAP sea utilizada en otros servicios y aplicaciones.

Las bases de datos que se usan comúnmente para guardar los datos de usuario pueden soportar muchas modificaciones en su contenido, mientras que los directorios LDAP que son un tipo de base de datos, realizan muy lentamente las funciones de modificación de la información, ya que estos están diseñados para lectura de los datos a los cuales se necesita acceder y no tanto para realizar cambios en ella.

Cuando un usuario quiere acceder al servicio de correo electrónico, primero debe realizar el proceso de autenticación (nombre de usuario y contraseña). Cuando se utiliza autenticación a través de LDAP descrita en [3], quiere decir que existe un servidor LDAP, en el cual se encuentra almacenada información como nombres de usuarios y sus claves. El servidor LDAP es consultado por el servidor de autenticación para verificar la veracidad de los datos cuando el cliente envía su información de usuario para acceder al servicio.

1.2 FALENCIAS MÁS CRÍTICAS QUE SE PRESENTAN EN EL SERVICIO DE CORREO ELECTRÓNICO DE LA UNIVERSIDAD DEL CAUCA

En esta sección se presentan las falencias determinadas por el administrador del servicio de correo electrónico, quien solicitó que esta problemática fuera atendida para darle solución a través de un trabajo de grado en la modalidad de desarrollo y es la motivación para el trabajo realizado del cual se rinde informe a través del presente documento. Estas falencias se exponen a continuación y se realiza una breve descripción para poder comprender mejor de que se trata cada una de ellas.

1.2.1 Spam

El término *spam* [4] es utilizado para referirse a los mensajes de correo no deseado que son enviados de forma masiva a los usuarios y que además de ser incómodos, ya que los usuarios no realizan ninguna solicitud para que estos mensajes lleguen a su bandeja de

entrada, también afectan los recursos del sistema debido a que estos mensajes ocupan gran cantidad de espacio, influyendo en la capacidad de almacenamiento y el desempeño de los servidores de correo.

El envío de *spam* se ha venido incrementando cada vez más en el transcurrir de los últimos años afectando a toda clase de usuarios, tanto a nivel individual como a nivel empresarial, ya que en las empresas se realiza el envío de gran cantidad de información a través del correo electrónico, haciendo que muchos de los mensajes legítimos que se están enviando sean tomados como *spam*, de tal forma que la información que llevan estos mensajes se pierda o no sea revisada ya que está clasificada como no deseada, causando una situación perjudicial para las empresas.

Este es uno de los problemas más críticos que se presentan en el servicio de correo de la Universidad del Cauca. A pesar de que las herramientas que se utilizan en el sistema actual de la Universidad ayudan a combatir este problema, se hizo necesario la implantación de nuevas posibilidades que contribuyan a la solución en cuanto al envío y recepción de correo no deseado.

En el servicio de correo de la Institución no se tiene ningún control de mensajes no deseados para el correo saliente hacia otros dominios, ni para correo dirigido hacia cuentas del propio dominio (correo interno), por esta razón y como se verá mas adelante durante el desarrollo de este trabajo de grado se estudiaron y pusieron en funcionamiento herramientas que contribuyen con la solución de estos problemas.

1.2.2 Inexistencia de autenticación de usuario y cifrado

La autenticación consiste en que el usuario debe ingresar sus datos (nombre de usuario y contraseña) antes de realizar el envío de un mensaje de correo. Este aspecto es de gran importancia, ya que la autenticación permite verificar la validez del remitente certificando los datos que se envían a través de internet. La autenticación evita la falsificación de cuentas y que se envíe correo malicioso y no deseado a nombre de estas cuentas.

El proceso de solicitud de autenticación en un sistema de correo electrónico surge por la necesidad de combatir la falsificación que se presenta en el contenido de los mensajes debido al *spam,* como por ejemplo, decir que un mensaje proviene de una dirección, sabiendo que el origen de este es otro.

Cuando un mensaje es enviado desde un origen a un destino a través de la red, éste puede tomar caminos distintos, pasando por diferentes equipos y por diversas redes. Esta gran cantidad de redes y equipos implicados en la transferencia del mensaje causa que la información se haga más susceptible a ser interceptada por terceros en algún lugar de su trayecto siendo más crítico en los extremos que es donde se genera y llega el correo.

La seguridad en Internet debe tener en cuenta aspectos como la autenticación de usuario, la integridad de la información enviada y la confidencialidad la cual se refiere a que los datos que se envían no sean interceptados en su trayecto por terceros no autorizados.

El servicio de correo electrónico de la Universidad del Cauca no tiene incluido el proceso de autenticación por parte de los usuarios al momento de enviar un mensaje, este sistema permite utilizar el servidor para enviar correo desde cuentas falsas, cuentas de otros dominios o cuentas de usuarios de la Institución por parte de un tercero ajeno a estas cuentas, por lo tanto se hace necesario implantar un módulo que permita evitar la suplantación de remitentes. También es importante realizar cifrado del canal de comunicación para proteger la información que se transmite a través de éste, de lo contrario se puede capturar los datos de autenticación de usuario y suplantar su identidad para efectuar operaciones como el envío de *spam*.

Para evidenciar que el sistema de correo electrónico actual no tiene implementado el proceso de solicitud de autenticación, se realizaron pruebas mediante el envío de mensajes de correo.

1.2.2.1 Evidencias de inexistencia de solicitud de autenticación

A continuación se presentan las pruebas de envió de correo desde el servidor de correo de la Universidad del Cauca realizadas con el fin de mostrar que el servidor de correo electrónico de la Universidad del Cauca, afrodita.unicauca.edu.co, no solicitaba autenticación para poder realizar el envío de correo y se puede utilizar cualquier cuenta para poder hacerlo.

- **Evidencia 1: Emisor de Hotmail-Receptor de Unicauca**

Esta prueba fue realizada el día miércoles 14 de marzo de 2012. La cuenta que se utilizó para enviar el mensaje, fue la cuenta ferchodas@hotmail.com perteneciente a otro dominio, en ningún momento se solicitó el ingreso de información de autenticación por parte del usuario, permitiendo enviar el mensaje al usuario davidandrade@unicauca.edu.co, esto quiere decir que la cuenta del usuario “ferchodas” fue suplantada por un remitente falso, además el servidor no solicita al cliente el ingreso del comando HELO/EHLO, el cual sirve para identificar el nombre del dominio de quien intenta realizar la conexión y de este modo iniciar la sesión SMTP. El comando HELO/EHLO se requiere para resolver en el DNS el nombre del dominio o la dirección y de esta manera verificar si es un servidor correctamente registrado.

Lo descrito en el párrafo anterior se observa en la Figura 1.2:

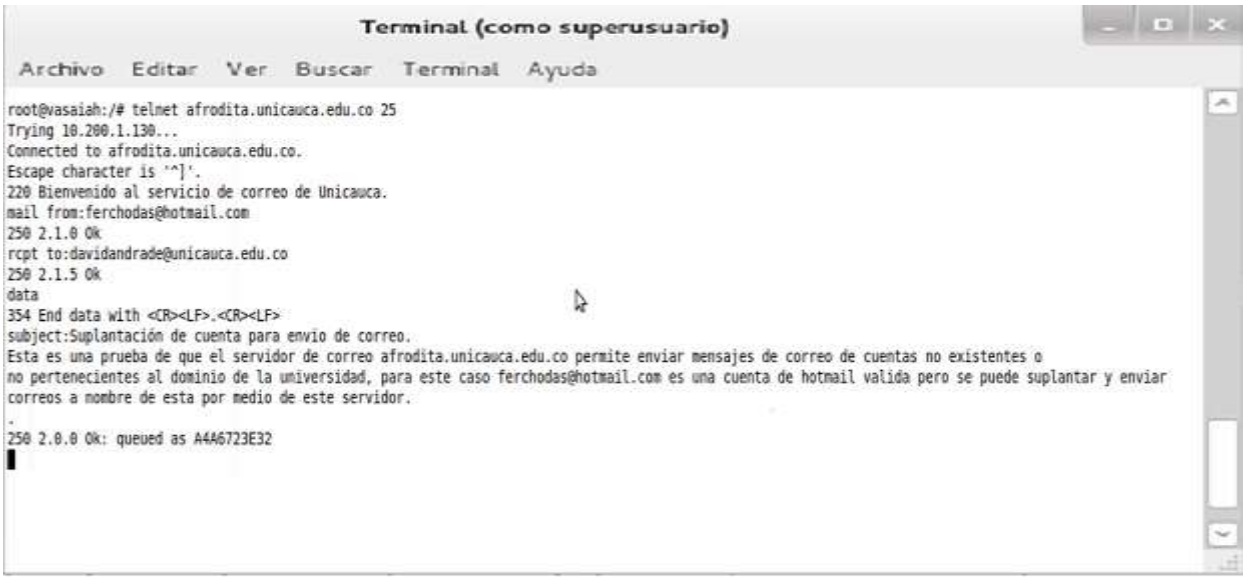


Figura 1.2 Envío de correo, emisor de Hotmail-receptor de Unicauca

Luego de entrar a la cuenta de usuario de “davidandrade”, en la Figura 1.3 se observa la bandeja de mensajes para verificar la recepción del anteriormente enviado.

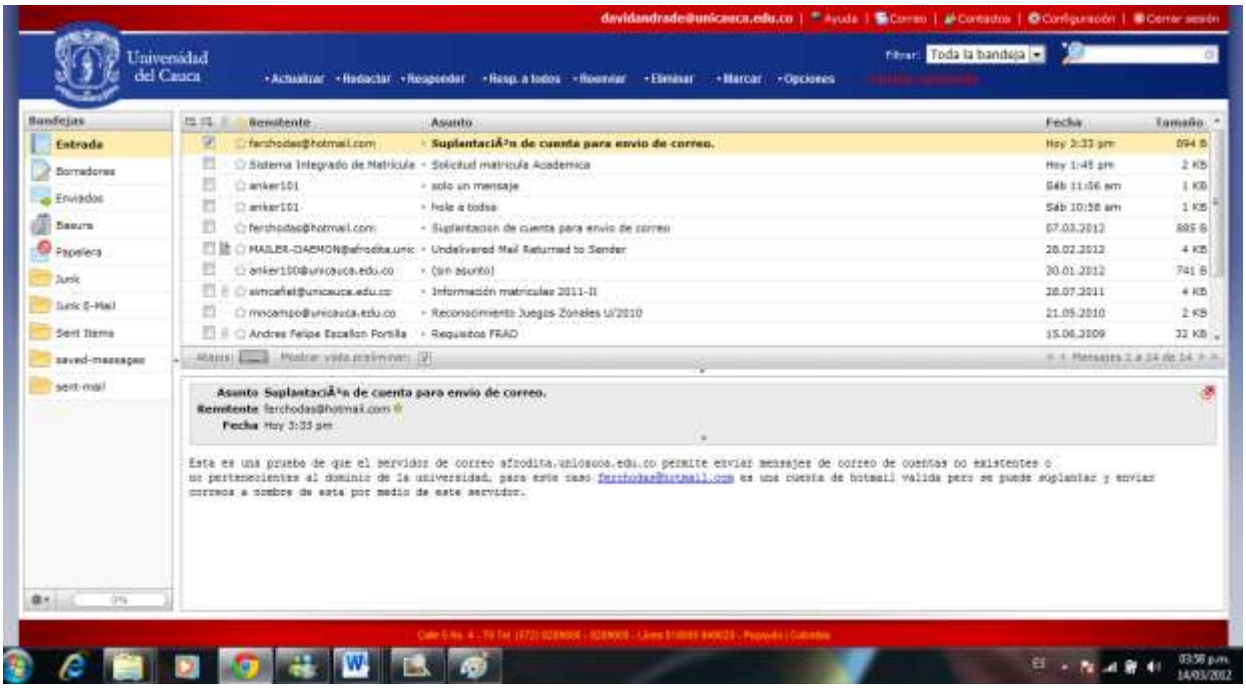


Figura 1.3 Cuenta de usuario Unicauca

Se puede ver claramente en la bandeja de mensajes del usuario que el remitente del mensaje es ferchodas@hotmail.com, haciendo creer que la procedencia del mensaje es del usuario real y desconociendo que el mensaje recibido proviene de un remitente falso.

- **Evidencia 2: Emisor de Hotmail-Receptor de Hotmail**

Esta prueba fue realizada el día martes 20 de marzo de 2012, con el fin de evidenciar que el servidor de correo de la Universidad del Cauca puede enviar correo desde cualquier cuenta y hacia cualquier dominio, sin importar que el destino sea una cuenta que no pertenezca al propio. El envío del mensaje se realizó desde la cuenta luisleam@hotmail.com hacia la cuenta del dominio de Hotmail ferchodas@hotmail.com, como se observa en la Figura 1.4.

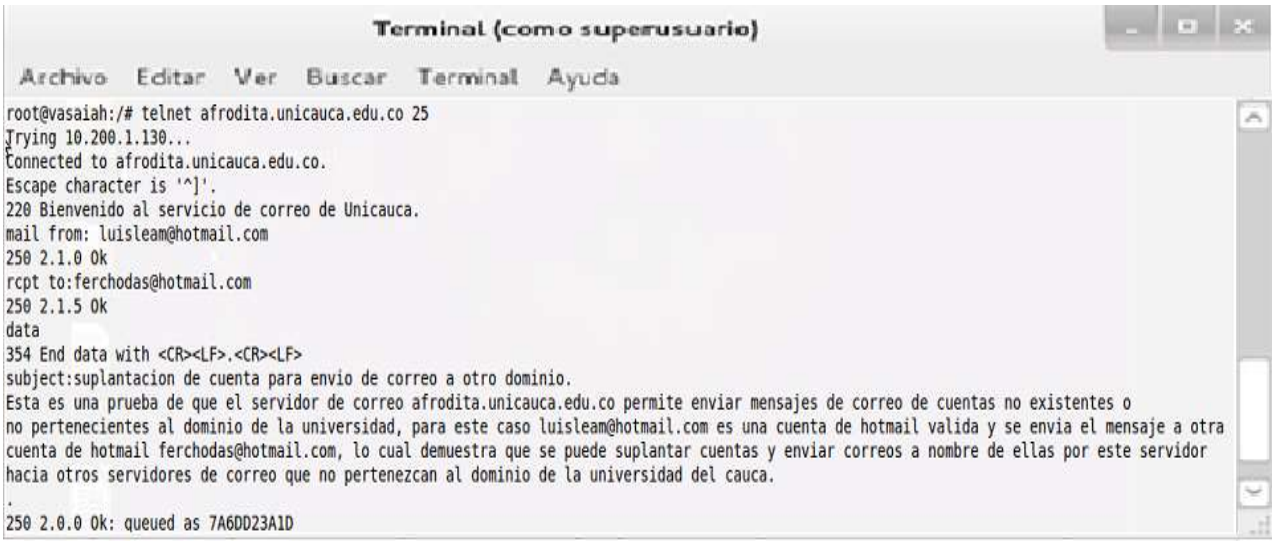


Figura 1.4 Envío de correo, emisor de Hotmail - receptor de Hotmail

La Figura 1.5 muestra la bandeja de mensajes del usuario de destino, aquí se puede verificar que el mensaje fue recibido, sin poder darse cuenta de que el mensaje no proviene de la cuenta real de Hotmail sino de un falso remitente.

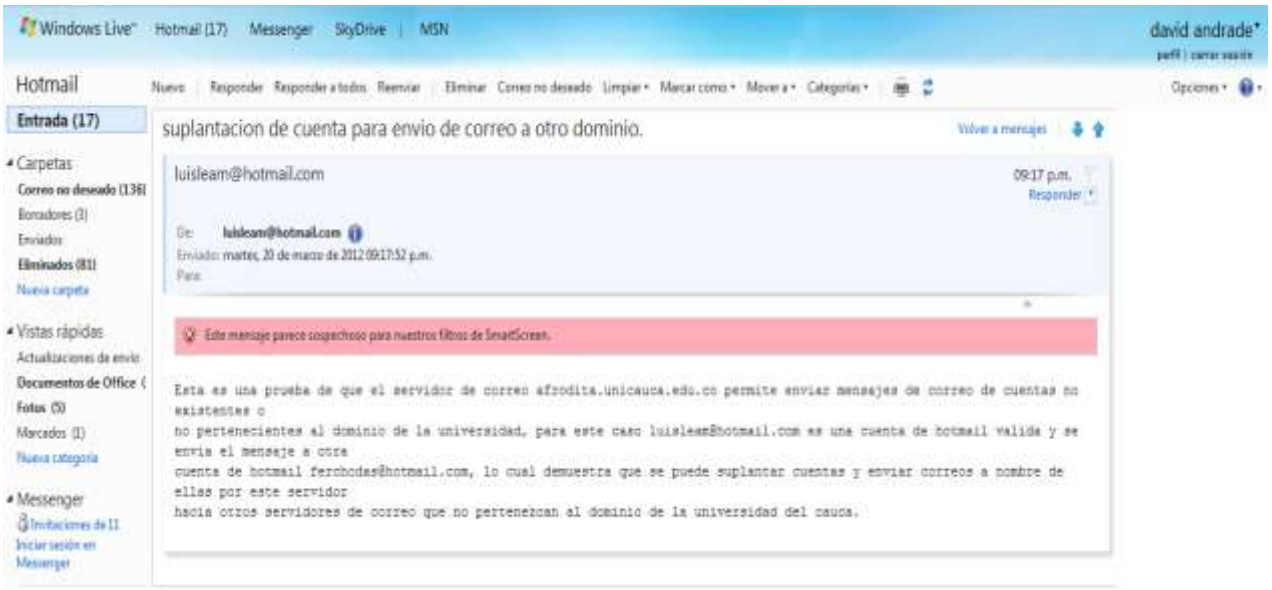


Figura 1.5 Cuenta de usuario de Hotmail

1.2.3 Ausencia verificación de robustez de contraseña

Robustez de contraseñas se refiere al nivel de seguridad que se le da a las contraseñas que los usuarios crean para utilizar el servicio de correo electrónico.

Las cuentas de los usuarios pueden ser suplantadas a partir de que la contraseña haya sido descubierta, por lo tanto se hace importante que la cuenta de cada usuario se encuentre respaldada por una contraseña robusta.

La verificación de robustez de contraseñas [5], está relacionada con la posibilidad que los usuarios del sistema de correo electrónico puedan crear contraseñas seguras para sus cuentas, generalmente estas contraseñas son creadas de tal forma que son sencillas de descifrar, esto trae como consecuencia que las cuentas de usuario puedan ser utilizadas por parte de terceros ajenos a estas, debido a que ya se conoce su contraseña de acceso.

Aunque este no sea un requerimiento indispensable para el funcionamiento del servicio de correo electrónico, es importante que se tenga en cuenta, ya que este permite darle un nivel de seguridad a las contraseñas de los usuarios y así proteger sus cuentas.

En la Universidad del Cauca no se cuenta con un sistema de verificación de contraseñas en cuanto a la seguridad que presentan éstas para proteger las cuentas de cada usuario, por lo tanto en el desarrollo de este proyecto se determinó implantar un módulo que permita cumplir con este requerimiento.

1.2.3.1 Evidencia de ausencia de verificación de robustez de contraseñas

El sistema de correo electrónico de la Universidad del cauca, no cuenta con un módulo que permita realizar la verificación de la seguridad de las contraseñas que los usuarios están utilizando para autenticarse en sus cuentas. En la Figura 1.6 se puede observar el *webmail* de la Universidad en la sección de configuraciones y se ve que no brinda la posibilidad de realizar esta comprobación.

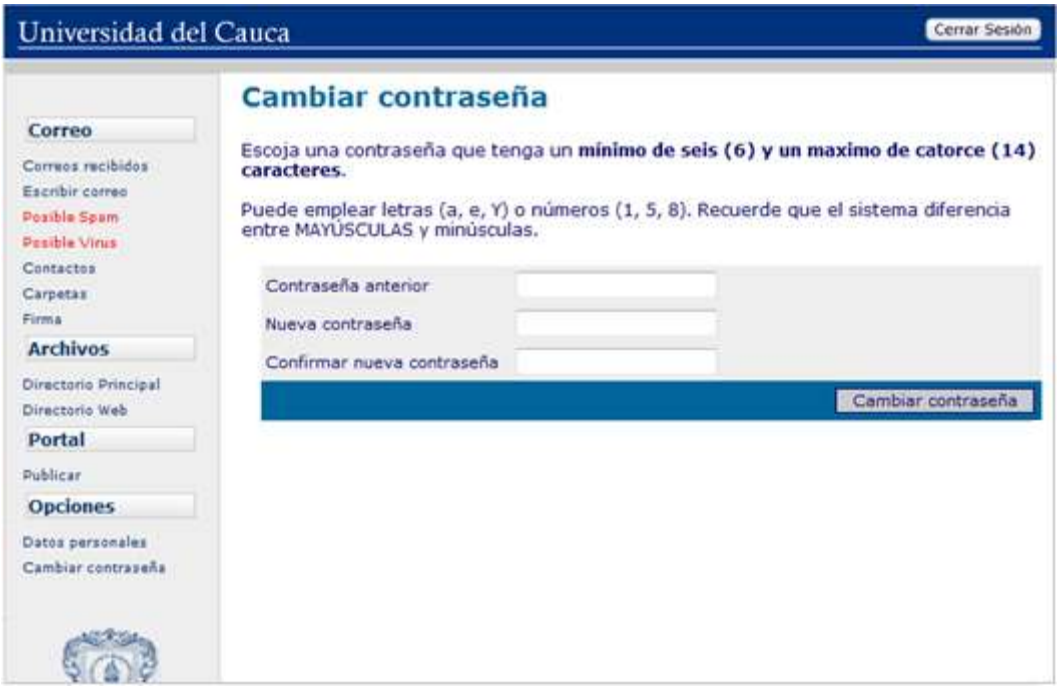


Figura 1.6 Sistema sin verificación de robustez de contraseñas

1.3 CAPTURA DE REQUERIMIENTOS

De acuerdo a las falencias y necesidades del sistema de correo de la Universidad del Cauca, presentadas en la sección anterior de este capítulo, se hizo la captura de requerimientos para contribuir a la solución de esta problemática y también se determinaron los requerimientos funcionales y los no funcionales de las herramientas a utilizar y de las configuraciones a realizar. Los requerimientos no funcionales aunque son visibles por el usuario, no se encuentran relacionados directamente a la funcionalidad de las herramientas, mientras que los funcionales definen el comportamiento de las mismas.

Estos requerimientos surgieron como una necesidad de la División de Gestión de Tecnologías de la Información y la Comunicación, específicamente del jefe del Área de Servicios y Servidores de internet de la Universidad del Cauca.

Con el fin de darle formalidad a la fase de captura de requerimientos y visualizar de una manera estándar las funcionalidades que se requieren en el sistema de correo, la descripción se realizó tomando como referencia los diagramas del Lenguaje Unificado de Modelado (UML, *Unified Modeling Languaje*) [6], el cual proporciona una notación estándar para representar y abstraer las funcionalidades de un sistema. En específico en esta sección se utilizan los diagramas de casos de uso y de secuencias. Las figuras que aparecen se obtuvieron a partir de la herramienta **EDraw Max**[7]. Debe tenerse en cuenta que la naturaleza de este trabajo es de selección y configuración de software y no de desarrollo, por tanto, el uso de UML es con fines de presentar una abstracción con notación estándar y no se deben utilizar todos sus tipos de diagramas.

Los requerimientos son los siguientes:

1. Disponer de herramientas para el control de *spam* que hagan revisión de los mensajes *spam* que se le pasan a la plataforma **Fortigate** y además que hagan control de mensajes de correo saliente y de correo interno de la Institución.

A continuación se mencionan algunos requerimientos funcionales y no funcionales de las herramientas que pueden contribuir con la problemática acerca de control de *spam.*

Requerimientos No Funcionales

- ✓ **Desempeño**: debe minimizarse el impacto que sobre el desempeño del sistema realice la integración de estas herramientas.
- ✓ **Facilidad de obtención**: poder acceder fácilmente a las herramientas para su utilización.
- ✓ **Compatibilidad con otros programas**: interconexión con otros programas para complementar las herramientas.

Requerimientos Funcionales

- ✓ **Control de *spam***: realizar control de *spam* tanto para correo entrante como para correo saliente.
- ✓ **Registros de *spam***: generar registros de mensajes detectados como *spam.*
- ✓ **Análisis de contenido**: analizar el contenido de los mensajes.
- ✓ **Acciones a realizar**: eliminar mensaje, poner en cuarentena, y marcar como *spam*.

- **Caso de Uso Controlar *spam* (correo entrante)**

Realizar control de correo no deseado para mensajes que llegan al servidor de correo de la Institución.

[7] http://www.edrawsoft.com/products.php

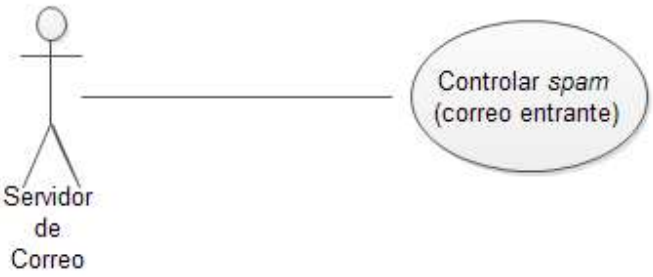


Figura 1.7 Caso de uso Controlar spam (correo entrante).

Tabla 1.1 Descripción Caso de uso Controlar *spam* (correo entrante).

Caso de Uso:	**Controlar *spam* (correo entrante).**
Actores:	Servidor de Correo
Tipo:	Primario
Descripción:	Los mensajes que llegan al servidor de correo son enviados a los filtros *antispam* para analizar su procedencia y su contenido, si el mensaje no se detecta como *spam*, este pasa al buzón del usuario.

La Figura 1.8 es el diagrama de secuencia que permite ver los objetos involucrados para poder llevar a cabo el caso de uso. El MTA envía el mensaje que llega a los filtros *antispam* para ser analizado y poder determinar si es o no *spam* antes de que el mensaje sea enviado al buzón del usuario.

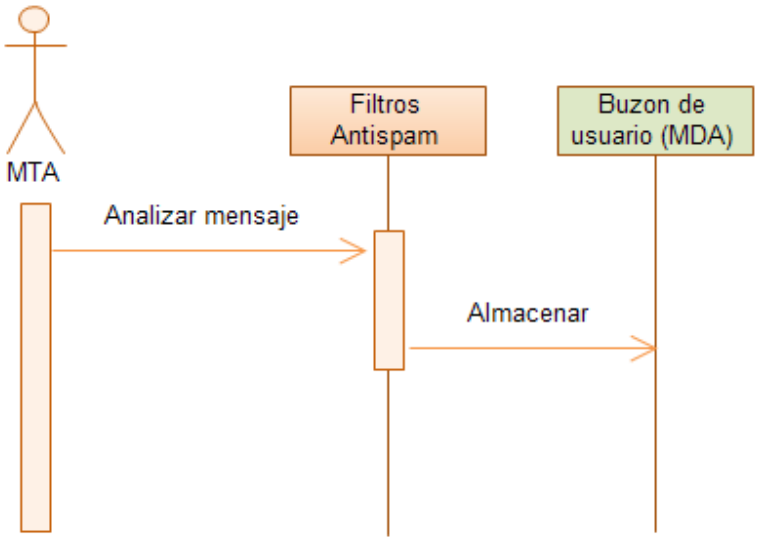


Figura 1.8 Diagrama de Secuencia Controlar spam (correo entrante).

- **Caso de uso Controlar *spam* (correo saliente)**

Realizar control de *spam* para los mensajes que los usuarios envían, ya sea hacia otro dominio o dentro del mismo.

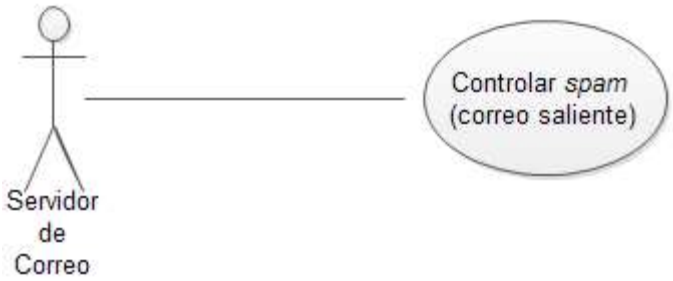


Figura 1.9 Caso de uso Controlar spam (correo saliente)

Tabla 1.2 Descripción Caso de uso Controlar *spam* (correo saliente).

Caso de Uso:	**Controlar *spam* (correo saliente)**
Actores:	Servidor de Correo
Tipo:	Primario
Descripción:	El usuario solicita el envío de un mensaje de correo electrónico, entonces se comunica con el agente de transferencia (MTA) para poder hacerlo. El MTA envía el mensaje hacia los filtros de contenido para ser analizados y de esta manera se realiza control de *spam* para el correo saliente y para el correo interno de la Institución a través del análisis de contenido y con restricciones aplicadas a los usuarios para el envío de mensajes. Si el mensaje no se detecta como *spam* este es enviado a su destino.

La Figura 1.10 es el diagrama de secuencia en el cual se observan los objetos comprometidos para realizar las acciones mostradas en el caso de uso.

La dinámica de la Figura 1.10 es iniciada por el MTA el cual envía el mensaje a los filtros *antispam* para ser analizados y determinar si el mensaje que el usuario desea enviar es calificado como *spam*.

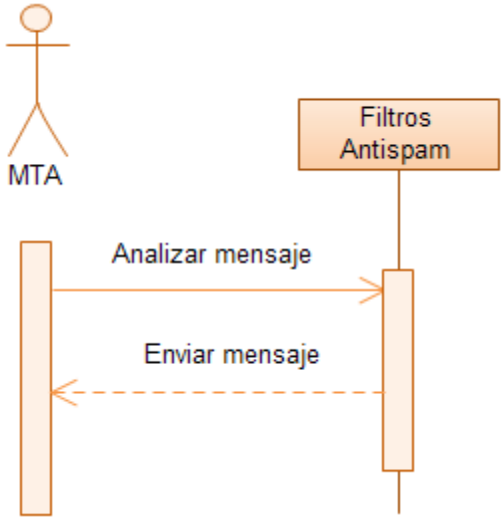


Figura 1.10 Diagrama de secuencia Controlar spam (correo saliente)

2. Configurar el servicio de correo electrónico para manejar autenticación de usuarios al momento de enviar mensajes y realizar cifrado de la conexión para proteger la información, de esta manera se puede tener un servicio de correo más seguro, evitando accesos no autorizados y protegiendo la información de los usuarios.

Esto también contribuye a que el dominio de la Institución no sea catalogado como emisor de *spam*.

A continuación se mencionan algunos requerimientos funcionales y no funcionales del servicio de autenticación.

Requerimientos Funcionales

- ✓ **Solicitar información de usuario:** solicitar al usuario el ingreso de sus datos (Nombre de usuario y contraseña) al momento de enviar un mensaje de correo.
- ✓ **Configurar cifrado**: configuración para manejar conexión cifrada y sin cifrar.

Requerimientos No funcionales

- ✓ **Recursos consumidos**: carga que se genera en el servidor al configurar el servicio de autenticación.

- **Caso de uso Enviar correo y Autenticar Usuario**

Para realizar el envío de un mensaje se deben ingresar los datos de usuario. La notación <<include>> se utiliza cuando un caso de uso necesita de otro caso de uso, este se dibuja con una flecha punteada hacia el caso que será usado [7].

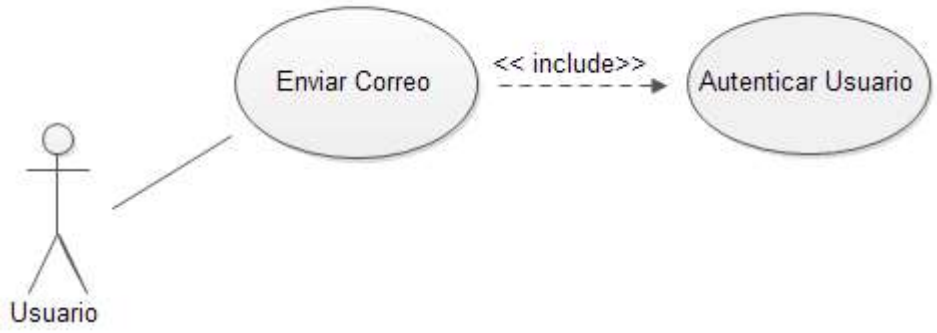


Figura 1.11 Caso de uso Enviar correo y Autenticar Usuario.

Tabla 1.3 Descripción Caso de uso Enviar correo

Caso de Uso:	**Enviar Correo**
Actores:	Usuario
Tipo:	Primario
Descripción:	El usuario intenta el envío de correo desde su cuenta hacia otro usuario, ya sea del mismo dominio o a una cuenta de otro dominio.
Precondición:	Realizar autenticación de usuario

Tabla 1.4 Descripción Caso de uso Autenticar Usuario

Caso de Uso:	**Autenticar Usuario**
Actores:	Usuario
Tipo:	Primario
Descripción:	El usuario debe ingresar sus datos de autenticación (Nombre de usuario y Contraseña) para poder realizar el envío de mensajes de correo electrónico.

La Figura 1.12 es el diagrama de secuencia que muestra los elementos implicados para realizar la autenticación de usuario. El usuario desea enviar un mensaje hacia otra cuenta, cuando el usuario intenta el envío del mensaje, el servidor le solicita al usuario ingresar su información de autenticación (Nombre de usuario y contraseña), el usuario ingresa sus datos y luego de esto el sistema ya le permite al usuario realizar el envío.

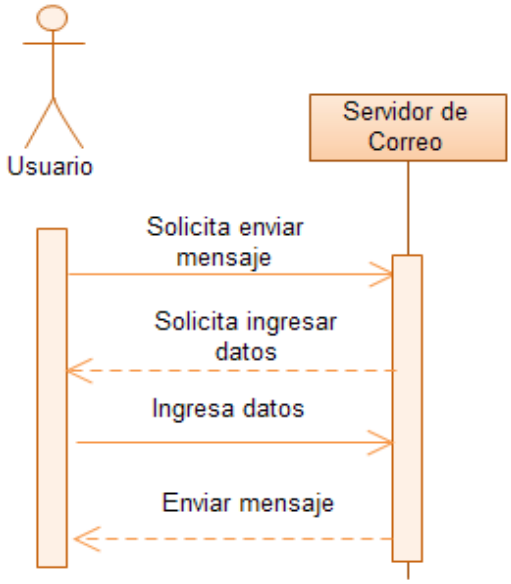


Figura 1.12 Diagrama de secuencia Enviar Correo y Autenticar Usuario.

3. Contar con un sistema que permita verificar la robustez de las contraseñas que los usuarios crean para utilizar el servicio de correo electrónico, brindando mayor nivel de seguridad a las mismas y de esta manera tener mayor protección de su información.

A continuación se mencionan algunos requerimientos funcionales y no funcionales para la verificación de robustez de contraseñas.

Requerimientos Funcionales

- ✓ **Mostrar nivel de seguridad de contraseña:** que el usuario pueda conocer el nivel de seguridad de la contraseña que esta creando.

Requerimientos No funcionales

- ✓ **Recursos consumidos**: que la codificación realizada no genere carga en el servidor.
- ✓ **Lenguaje de programación:** lenguaje en el que se lleve a cabo la implementación.

- **Caso de uso Verificar Robustez de Contraseñas**

Realizar la verificación de robustez de las contraseñas que los usuarios utilizan para acceder al servicio de correo electrónico.

Figura 1.13 Caso de uso Verificar Robustez de Contraseñas

Tabla 1.5 Descripción Caso de uso Verificar Robustez de Contraseñas

Caso de Uso:	**Verificar Robustez de Contraseñas**
Actores:	Usuario
Tipo:	Primario
Descripción:	El usuario puede darle un nivel de seguridad a la contraseña que esta creando para utilizar el sistema de correo electrónico a través de un modulo en el portal web que permita verificar la robustez de las mismas.

La Figura 1.14 es el diagrama de secuencia en el cual se observan los elementos involucrados para realizar la verificación. El usuario ingresa al portal web de la Institución y en este se encuentra un módulo que permite verificar la robustez de la contraseña que está creando para su cuenta de correo, a medida que el usuario va ingresando su contraseña, el sistema va mostrando el nivel de seguridad de la misma.

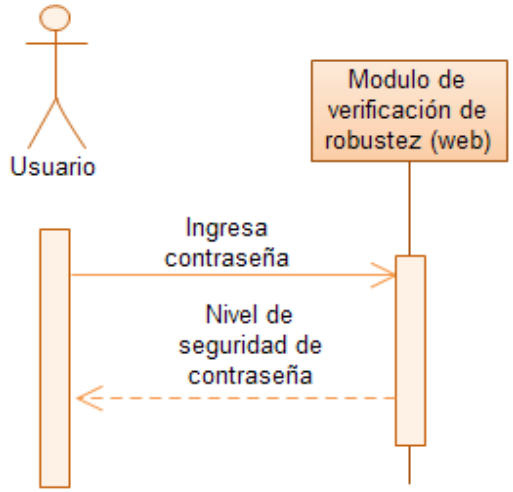


Figura 1.14 Diagrama de secuencia Verificar Robustez de Contraseñas

CAPITULO 2.

2 MEJORAS INTRODUCIDAS AL SISTEMA DE CORREO DE LA UNIVERSIDAD DEL CAUCA

En este capítulo se evidencian las diferentes formas, mecanismos y herramientas que contribuyeron con la solución a los problemas que se tenían en el sistema de correo de la Universidad del Cauca. Se presentan los parámetros de selección y la evaluación de las herramientas de acuerdo a estos parámetros. Para realizar la selección de las herramientas *antispam* de acuerdo con un proceso orientado a este propósito y así garantizar rigurosidad académica, se aplicó una metodología que permitiera realizar la evaluación de software, además por la gran cantidad de alternativas que existen para realizar las funciones de detección y control de *spam.* Por último se evidencian las mejoras introducidas al sistema de correo de acuerdo a las herramientas escogidas y las configuraciones realizadas.

2.1 PARÁMETROS DE SELECCIÓN

En esta sección se describen los parámetros utilizados para llevar a cabo la evaluación y selección de las herramientas con las cuales se busca mejorar el sistema de correo electrónico de acuerdo a las falencias presentadas en la sección **1.2**.

En la elección de las herramientas para llevar a cabo las configuraciones de autenticación y cifrado no se tomaron en cuenta parámetros de selección, ya que la configuración dependía del tipo de servicio y del servidor de correo que se esté utilizando. Para este caso se esta configurando el servicio SMTP con el servidor Postfix, el cual maneja esta autenticación a través del Protocolo de Autenticación Simple y Nivel de Seguridad (SASL, *Simple Authentication and Security Layer*) [8].

Para la configuración de la verificación de robustez de contraseñas tampoco fueron tenidos en cuenta parámetros de selección, ya que se busca es que las contraseñas cuenten con ciertas características que ofrecen niveles de seguridad para que estas no sean fáciles de descifrar y no se trataba de hacer una selección entre diferentes aplicaciones software. Una contraseña puede tener un mayor nivel de robustez si cuenta con las características que se exponen a continuación [5]:

- **Cantidad de caracteres de la contraseña**: entre más caracteres tenga una contraseña mucho mejor, esto disminuye considerablemente el peligro que la contraseña sea descifrada por software malicioso, es favorable que la contraseña tenga más de 8 caracteres.

- **Diversidad de caracteres**: La contraseña debe estar compuesta por una combinación de letras, números, caracteres especiales y letras mayúsculas, para que no pueda ser interpretada fácilmente.

De esta manera, aunque “a priori” se consideró que para todas las capacidades se debería realizar un proceso de selección de un herramienta de software libre, una vez se estuvo en el desarrollo del proyecto y se conoció la naturaleza y funcionamiento del sistema, se encontró que solamente se debía seleccionar un *antispam* que detectara el *spam* que se le lograba pasar al Fortigate.

Para realizar la selección de las herramientas *antispam*, se utilizó una metodología de evaluación de software libre en la cual se tienen los parámetros a ser evaluados y de esta manera determinar cuales con las más adecuadas para ser integradas en el sistema de correo de la Institución. Los parámetros son las métricas que se evalúan en la metodología aplicada y de acuerdo a ésta, el usuario puede incluir sus propias métricas de acuerdo al contexto. Según la metodología utilizada, ésta permite que el usuario pueda escoger las métricas de funcionalidad de acuerdo a la función de las herramientas a evaluar. Para las herramientas *antispam* se seleccionan los parámetros o métricas de funcionalidad teniendo en cuenta las funciones de control de *spam*. Las métricas que no tienen que ver con la funcionalidad son establecidas por la metodología y se muestran mas adelante en la etapa de aplicación de la metodología de evaluación de software libre. Los parámetros funcionales para el control de *spam* se detallan a continuación.

2.1.1 Parámetros de selección de herramientas *antispam*

La definición de los parámetros se realizó teniendo en cuenta la funcionalidad de las herramientas de acuerdo al contexto en el que se esta trabajando, que para este caso es cumplir con las funciones de control de *spam* y los métodos que se utilicen para hacerlo.

Para la elección de parámetros se tomo como referencia lo descrito en [9] la cual expresa que la eficiencia de una herramienta *antispam* se puede medir siguiendo lo enunciado en el siguiente apartado.

> *“En un entorno de funcionamiento real, podemos medir la calidad del filtro mediante dos indicadores:*
>
> - *El porcentaje de mensajes no spam calificados como spam erróneamente (“tasa de falsos positivos”).*
> - *El porcentaje de mensajes spam filtrados correctamente (“precisión”).*
>
> *El parámetro más importante desde el punto de vista del usuario real es el porcentaje de falsos positivos. En efecto, si un mensaje Spam evade el filtro es fácil hacer click en el botón de borrar. Sin embargo, si se marca con etiqueta de Spam a un mensaje normal, el usuario no lo verá y éste quedará perdido.”*

También se tuvo en cuenta lo que aparece en la referencia [10] para evaluar las herramientas antispam: analizan los resultados aplicando la siguiente fórmula:

> *“Tasa de detección de spam = (spam marcado como spam/total de spam)*100*
> *Tasa de falsos positivos= (genuinos marcados como spam/total de genuinos)*100”*

Según las citas anteriores, los principales parámetros que se tienen en cuenta para evaluar una herramienta *antispam* son:

- **Efectividad en el rechazo de correo *spam***: cantidad de mensajes que son detectados como *spam*.

- **Efectividad en la aceptación de correo legítimo**: cantidad de falsos positivos detectados por la herramienta, estos son correos legítimos detectados como *spam.*

También se definieron otros parámetros relacionados con la funcionalidad de las herramientas antispam, estos son:

- **Manejo de redes bayesianas**: las redes bayesianas consisten en que la herramienta se encarga de revisar el contenido del mensaje y determinar a través de métodos probabilísticos y de unas políticas establecidas si se cataloga como *spam,* basado en un entrenamiento previo.

- **Manejo de métodos heurísticos**: estos métodos consisten en buscar patrones que suelen repetirse en el contenido de los mensajes.

- **Uso de redes colaborativas**: estas son redes que complementan el funcionamiento de las herramientas *antispam*. Estas son bases de datos que se utilizan para la detección y notificación de *spam.*

- **Software libre**: este parámetro se tiene en cuenta ya que el desarrollo del proyecto se basa en herramientas de software libre.

Para estos últimos se tomaron referencias a partir del conocimiento y la experiencia por parte del Jefe del área de servicios de Internet de la Universidad del Cauca, el director del presente trabajo de grado y también del estudio y aprendizaje obtenido en el desarrollo de este proyecto acerca del *spam,* como por ejemplo que existen redes colaborativas que pueden complementar el filtro *antispam* y otros parámetros que dependen mas de la funcionalidad y de los métodos utilizados para el control de correo no deseado como el manejo de redes bayesianas y de métodos heurísticos. El parámetro de que la herramienta fuera de software libre fue seleccionado, ya que el desarrollo de este proyecto se dirige a ofrecer una mejora basada en herramientas de software libre.

En el Anexo B se evidencia un soporte escrito por parte del Ingeniero Jefe del área de Servidores y de Servicios de Internet de la Universidad del Cauca en la cual confirma que los parámetros escogidos son los necesarios para la evaluación de herramientas *antispam*.

2.2 HERRAMIENTAS UTILIZADAS Y EVALUACIÓN

En esta sección se describen las diferentes herramientas y los métodos que éstas utilizan para realizar el filtrado de *spam,* también se expone la evaluación de las mismas para saber cuáles se tienen en cuenta para atender a las necesidades en el sistema de correo de la Universidad del Cauca.

2.2.1 Herramientas utilizadas

Antes de realizar esta evaluación, es importante mostrar cuáles son los métodos con los que se realiza control de *spam* y las características de las posibles herramientas con las que se va a llevar a cabo el mejoramiento en el servicio de correo de la Institución. Para realizar el control de *spam* se utilizan dos diferentes formas de filtrado, estos son: los filtros de reputación y los filtros de contenido [11], que se describen a continuación.

2.2.1.1 Filtros de Reputación

La función de los filtros de reputación es evitar que lleguen mensajes no deseados y virus al servidor de correo, verificando la procedencia del mensaje. A continuación se describen algunas de las técnicas más utilizadas para el control de *spam* con el uso de este tipo de filtros.

- **Listas Negras (*Black List*):** este es un método en el cual se encuentran en una lista los servidores que han sido reseñados como emisores de *spam.* Si alguno de estos servidores realiza una petición de conexión, ésta es rechazada por los servidores que implementen esta técnica.

- **Listas Grises (*Grey List*):** se refiere al proceso en el cual el servidor rechaza la conexión y pide que el mensaje sea reenviado. Los métodos que utilizan los *spammers* para el envío de correo no deseado no realizan funciones de reenvío cuando el mensaje ha sido rechazado. Una desventaja de este método es que presenta una demora agregada en la recepción de correo electrónico, por lo tanto no se toma en cuenta para la utilización en los filtros de reputación.

- **Listas Blancas (*White List*):** es una lista en la cual se encuentran los servidores que son conocidos como no generadores de *spam* y que están autorizados para el envío de mensajes de correo electrónico.

- **Registros SPF (*Sender Policy Framework*):** como se define en [12], en estos registros se encuentran los servidores que un dominio ha autorizado para que se envíen sus mensajes de correo electrónico. El servidor del dominio que envía el mensaje puede no ser el mismo del que lo está entregando, entonces lo que se hace es verificar en estos registros si el servidor final está autorizado para hacerlo.

- **Verificación de remitente:** se verifica que la dirección IP del servidor que solicita la conexión corresponda al dominio que esta representa.

La configuración de estos filtros se realiza en los archivos de configuración del servidor de correo con el que se esté trabajando.

2.2.1.2 Filtros de Contenido

Son herramientas que se le integran al sistema para realizar la detección de correo no deseado. Estos filtros son los encargados de analizar el contenido de los mensajes que llegan al servidor para determinar si son mensajes *spam* o si tienen virus.

Los filtros de contenido utilizan diferentes técnicas para realizar sus funciones de detección de *spam,* entre estas técnicas se encuentran los códigos bayesianos [13] y métodos heurísticos [14], estos se describen a continuación.

- **Códigos bayesianos:** consisten en que la herramienta se encargan de revisar el contenido del mensaje y determinar a través de métodos probabilísticos y de unas políticas establecidas si se cataloga como *spam,* basado en un entrenamiento previo.

- **Métodos heurísticos:** consisten en buscar patrones que suelen repetirse en el contenido de los mensajes.

Es importante conocer las técnicas que usan los filtros *antispam,* al momento de configurar la herramienta, ya que de acuerdo al método de detección que se maneje depende dicha configuración. Por ejemplo, los filtros que manejan métodos heurísticos se configuran de acuerdo con una asignación de valores para manejar patrones comunes que tienen los mensajes *spam*, mientras que los filtros que manejan códigos bayesianos se deben entrenar para que trabajen con un conocimiento previo de acuerdo con el entrenamiento realizado y con métodos probabilísticos.

Adicional a las técnicas de análisis de *spam* que manejan los filtros de contenido, estos pueden tener métodos complementarios en los cuales se pueden apoyar para realizar la detección de *spam* como lo son las redes colaborativas [15], las cuales son bases de datos en las que se realiza la notificación de mensajes que ya han sido catalogados como *spam.*

En cuanto a configuración, también hay herramientas que manejan el control de flujo de mensajes, esto brinda la posibilidad de configurar la cantidad de mensajes que un usuario puede enviar y recibir en un tiempo determinado y también se puede restringir el número de usuarios por mensaje, esto ayuda a controlar el envío y recepción de correo no deseado en un sistema de correo electrónico. Estos filtros brindan la posibilidad de configurarse de acuerdo a las necesidades que se tengan.

2.2.2 Metodología de evaluación

Después de definir los parámetros y de saber en qué consisten, estos son aplicados a las herramientas para realizar la evaluación y selección.

De acuerdo con las características que presenta la autenticación, el cifrado y la verificación de robustez de contraseñas en las que no se tienen en cuenta parámetros de selección, tal y como se describe en la sección **2.1,** no se realiza evaluación de herramientas por medio de una comparación, ya que lo que se tiene en cuenta es que estos se integren al sistema de correo, por lo tanto la comprobación que se realiza es que no se contaba con un sistema que manejara autenticación de usuarios, cifrado de la conexión y verificación de robustez de contraseñas y de acuerdo a las falencias planteadas y a la contribución de este trabajo de grado, ya se cuenta con un sistema que tiene implantadas estas capacidades.

Para las herramientas *antispam* se definieron parámetros de selección y de acuerdo a estos se realiza la evaluación para saber cuales de las herramientas van a ser utilizadas para el mejoramiento del sistema.

La evaluación de las herramientas *antispam* se llevó a cabo con la utilización de una metodología para evaluar software libre debido a la gran cantidad de opciones que existen para combatir el correo no deseado, pero antes de empezar con la evaluación es necesario saber cual metodología se va a utilizar ya que existen distintos modelos con los cuales se puede evaluar software libre.

2.2.2.1 Selección de la metodología para evaluar las herramientas *antispam*

La selección de software puede convertirse en una tarea bastante complicada, ya que pueden existir diversas opciones para cubrir las necesidades que se tengan, por lo tanto se requiere de un proceso que facilite tomar una decisión de seleccionar un software teniendo en cuenta diferentes aspectos como por ejemplo: costos, seguridad, compatibilidad, soporte, entre otros y de esta manera analizar las limitaciones del software.

Para la selección de software se requiere llevar un proceso detallado y justificado acerca de la escogencia de las herramientas que se van a utilizar. Existen diversos métodos que permiten realizar el análisis y evaluación de software en el caso de ser libre, entre los más conocidos y de mayor acogida por la comunidad de Software de Código Abierto y de Software Libre (FLOSS, *Free/Libre and Open Source Software*) [16], se encuentran las metodologías de primera generación que surgieron entre el año 2003 y 2005 aproximadamente como la de Puntuación para la Preparación de Negocios Abiertos (OpenBRR[8], *Open Business Readiness Rating*), la metodología de Calificación y

[8] http://www.openbrr.org/

Selección de Software de Código Abierto (QSOS[9], *Qualification and Selection of Open Source software*) y el Modelo de Madurez de Código Abierto (OSMM[10], *Open Source Maturity Model*) [17], también se encuentran los modelos de segunda generación como por ejemplo el Modelo de Calidad de Software de Código Abierto (QualOSS[11], *QUALity of Open Source Software*) y el Modelo de Madurez de Código Abierto (OMM[12], *QualiPSo Open Source Maturity Model*), los cuales están basados en las metodologías de primera generación [16]. Estas metodologías tienen sus propias estructuras de evaluación y su sistema de puntuación basado en diferentes criterios, algunas de estas metodologías se basan en aspectos como madurez del software, la durabilidad y otras tienen en cuenta aspectos funcionales para realizar la evaluación [18].

Para la elección de la metodología de evaluación se analizaron las características que presentan las metodologías mencionadas. El modelo OSMM [19] se basa más que todo en la madurez de las herramientas que se están evaluando y en el contexto que se está trabajando en este proyecto. Esta no es una característica esencial para la evaluación y son de mayor importancia otros aspectos como por ejemplo, la funcionalidad de las herramientas a evaluar, por lo tanto este modelo no se tendrá en cuenta para realizar la evaluación. Los modelos de segunda generación todavía no están maduros y presentan inconvenientes con las métricas que estas proponen, además las herramientas de medición para la evaluación aun se encuentran en su etapa de prototipo [16].

De acuerdo a [20], las metodologías OpenBRR y QSOS son muy similares y proponen seguir los mismos pasos para la evaluación de software. La diferencia se encuentra en el orden en que estos se aplican. A continuación se presentan los pasos en el orden que se aplican en la metodología QSOS:

1. Plantear un conjunto de criterios de evaluación ya definidos.

2. Asignar una puntuación a los diferentes criterios sobre una puntuación definida por cada metodología.

3. Asignar un nivel de importancia a cada criterio de acuerdo al contexto del proyecto.

4. Tomar una decisión de acuerdo a los resultados obtenidos.

La metodología OpenBRR invierte los pasos 2 y 3 de tal forma que primero se realiza la selección de los criterios que el usuario considera relevantes, sin tener la necesidad de dar una puntuación a los criterios que no se hayan considerado.

[9] http://www.qsos.org/?page_id=7
[10] http://qualipso.org/omm
[11] http://libresoft.es/research/projects/qualoss
[12] http://www.qualipso.org/trustworthy_process

Según la metodología QSOS, los resultados obtenidos son universales ya que la evaluación se define para una versión particular del software [20], mientras que con OpenBRR los resultados pueden variar ya que la evaluación se realiza dependiendo del contexto y de como éste sea asumido por el usuario.

Debido a que su nivel de aceptación no fue el que se esperaba y no tuvo una comunidad que realizara grandes aportes, el proyecto OpenBRR no continuó desde de Julio del 2010 [20]; sin embargo, en el desarrollo de este proyecto se hace bastante viable la utilización de esta metodología OpenBRR para la evaluación de herramientas, ya que permite la adaptación de nuevas características en la evaluación, por lo tanto se opta por realizar la evaluación de las herramientas *antispam* con esta metodología. Además de esto, QSOS no maneja las características de funcionalidad como parte del método de evaluación, mientras que OpenBRR si lo hace y de acuerdo al contexto del proyecto en desarrollo el aspecto de funcionalidad es muy importante para la evaluación, ya que las principales características de las herramientas *antispam* se encuentra en las funciones que estas realicen en cuanto al control y detección de correo no deseado como fue sustentado en la sección **2.1.1**.

2.2.2.2 Aplicación de la metodología de evaluación OpenBRR

En esta etapa se presenta el proceso realizado al aplicar la metodología OpenBRR para la evaluación de las herramientas *antispam*, este proceso se encuentra detallado en el Anexo C en donde se muestra paso a paso las acciones realizadas según la metodología.

Es importante mencionar que los resultados que se obtengan de la evaluación no se utilizan para juzgar a ninguna herramienta sino para conocer sus características y de esta manera poder dar una puntuación para realizar la selección.

A continuación se presenta una descripción de las etapas que se llevaron a cabo para realizar la evaluación con la metodología OpenBRR.

1. Se realizó la evaluación rápida: esta se hace con ciertas características que presenten las herramientas y se hace para reducir el número de alternativas que se tengan. La evaluación rápida se evidencia en la sección **1** del Anexo C, en donde se muestran las características que fueron tenidas en cuenta para efectuar dicha evaluación y se expone una tabla con las herramientas que fueron evaluadas en esta etapa y cuáles de estas pasaron esta evaluación.

   De acuerdo a OpenBRR, de todas las herramientas que se consideraron en la evaluación rápida, las que cumplieron con las características que en esta se evalúan, fueron **Spamassassin**[13] y **Dspam**[14], entonces con estas dos herramientas son con las que se lleva a cabo el proceso completo de evaluación como lo define la metodología

[13] http://spamassassin.apache.org/
[14] http://dspam.nuclearelephant.com/

y de esta manera obtener una puntuación BRR como resultado final para cada una de ellas.

Para realizar la evaluación de estas herramientas es importante conocer las características que presentan y así tener información que sirva como referencia, para esto a continuación se realiza una breve descripción de cada una de ellas.

- **SpamAssassin**

De acuerdo con [21], es una de las herramientas de software libre más utilizadas en el mercado para el análisis de correo no deseado, hace uso de listas negras y de bases de datos donde se publica el *spam* que llega a los usuarios, maneja métodos heurísticos en los cuales se buscan pautas o conductas que suelan repetirse en los mensajes no deseados y realiza análisis probabilístico de acuerdo con un entrenamiento previo con mensajes clasificados como *spam*. Es un programa que se puede configurar de acuerdo con las preferencias del usuario, se le pueden definir nuevas reglas y se puede integrar con el servidor de correo (MTA) para realizar filtrado automático de todo el correo de un sitio.

- **Dspam**

Como se describe en [22], es una herramienta de código abierto usada para controlar *spam* mediante filtros estadísticos. Puede integrarse con cualquier MTA o también con MDAs como **Procmail**.

Cuando se recibe un mensaje de correo no deseado, se puede enviar a una cuenta de correo previamente configurada por el administrador para que esta herramienta conozca y analice automáticamente y tenga como base los *spam* que se han recibido. Esta herramienta puede utilizar listas negras y se puede complementar con redes colaborativas donde se publican los mensajes catalogados como *spam*.

2. Se inició con la evaluación de las herramientas que pasaron la evaluación rápida, escogiendo los criterios a evaluar, según los establecidos por la metodología. En la sección **2** del Anexo C se encuentran cuáles son los criterios establecidos por la metodología y cuáles de estos fueron seleccionados para ser evaluados.

Los criterios escogidos fueron:

- Funcionalidad
- Calidad
- Rendimiento
- Comunidad
- Documentación
- Soporte
- Escalabilidad

3. Se asignó un porcentaje a cada uno de los criterios escogidos para la evaluación, de acuerdo a la importancia que se determino dar a cada uno. En la sección **3** del Anexo C se muestra a través de una tabla, cada uno de los criterios con su respectiva ponderación y luego una descripción de cada uno para tener mayor claridad de lo que se está haciendo.

4. Se escogieron las métricas que se van a evaluar para cada criterio y se les asignó un porcentaje de importancia a cada una de ellas.

   Cada uno de los criterios tiene asociadas unas métricas para realizar la evaluación. De acuerdo a la metodología OpenBRR el criterio de funcionalidad se maneja de forma distinta a los otros criterios, de tal forma que a éste se le pueden asignar las métricas de acuerdo al contexto del proyecto.

   Una vez que se encuentra un proceso estandarizado como la metodología de evaluación, los parámetros son llamados *métricas*, por lo tanto en esta etapa de evaluación de las herramientas *antispam,* para los parámetros definidos se usará este término.

   Las métricas escogidas para la evaluación del criterio de funcionalidad son los parámetros que se definieron en la sección **2.1.1**. Las métricas de los otros criterios son establecidas por la metodología.

   Esta etapa se evidencia detalladamente en la sección **4** del Anexo C, en donde también se muestra a través de una serie de tablas, cómo se realiza la evaluación de las métricas para cada criterio. La evaluación de las métricas de funcionalidad puede ser definida por el usuario, mientras que la evaluación de las métricas de los otros criterios está determinada por la metodología. La evaluación de las métricas de funcionalidad se llevo a cabo como se muestra a continuación:

   - La evaluación de la primera métrica que es la **Efectividad en el rechazo de *spam*** se realizó como se muestra en la Tabla 2.1.

Tabla 2.1 Evaluación Métrica de Efectividad en el rechazo de spam

Efectividad en el rechazo de *spam*	
Porcentaje de Rechazo (%)	**Puntuación**
0% - 30%	1
30% - 70%	2
70% - 100%	3

   - La métrica de **Efectividad en la aceptación de correo legítimo** (falsos positivos), se evalúa como se muestra en la Tabla 2.2.

Tabla 2.2 Evaluación Métrica de Efectividad en la aceptación de correo legitimo

Efectividad en la aceptación de correo legitimo	
Reconocimiento de falsos positivos	**Puntuación**
No	3
Si	1

- Para las métricas **Manejo de redes bayesianas, Manejo de métodos heurísticos** y el **Uso de redes colaborativas**, por ser características de funcionamiento adicionales que pueden presentar o no las herramientas, según lo establecido por OpenBRR la evaluación se realiza premiando a la herramienta que cumpla con estas métricas, de tal forma que se suma el valor del peso que se le dio a dicha métrica, o castigándola restándole este mismo valor en caso de que no cumpla. La evaluación de la métrica de **Software Libre** se hace de la misma manera.

5. Se evaluaron las métricas de cada criterio de acuerdo con lo definido en la metodología. Esta etapa se evidencia en la sección **5** del Anexo C.

En esta etapa se les asigna una puntuación a cada una de las métricas de acuerdo al cumplimiento de cada una de éstas. A excepción del criterio de funcionalidad, para realizar la calificación de las métricas cada uno de los criterios escogidos se utiliza una escala que asocia unos valores de 1 a 5 a una calificación, como se observa en la Tabla 2.3.

Tabla 2.3 Calificación para Criterios

Valor	Concepto
1	Inaceptable
2	Pobre
3	Aceptable
4	Muy bueno
5	Excelente

Para la puntuación de las métricas de funcionalidad se usa una escala de 1 a 3, en donde 1 es la de menor importancia y 3 la de mayor importancia.

Primero se analizan las métricas de funcionalidad. Para verificar el cumplimiento de la primera métrica que es la **Efectividad en el rechazo de *spam***, se realizan pruebas de

las herramientas con el fin de verificar cuál es la que mejor cumple con este parámetro, que es la que mayor cantidad de *spam* rechace. Para graficar los resultados de estas pruebas se utilizó el programa llamado **Mailgraph**[15] el cual genera una gráfica basándose en el sistema de registro de mensajes del servidor de correo, mostrando la cantidad de correo que se recibió en un periodo de tiempo y cuales de estos son detectados como *spam.*

A continuación se evidencian las pruebas realizadas con los filtros **Spamassassin** y **Dspam**.

- **Prueba con Spamassassin**

  Para esta prueba se enviaron 484 correos *spam* para observar cuantos de estos son rechazados. La Figura 2.1 muestra la cantidad de mensajes *spam* enviados y cuantos de estos fueron rechazados.

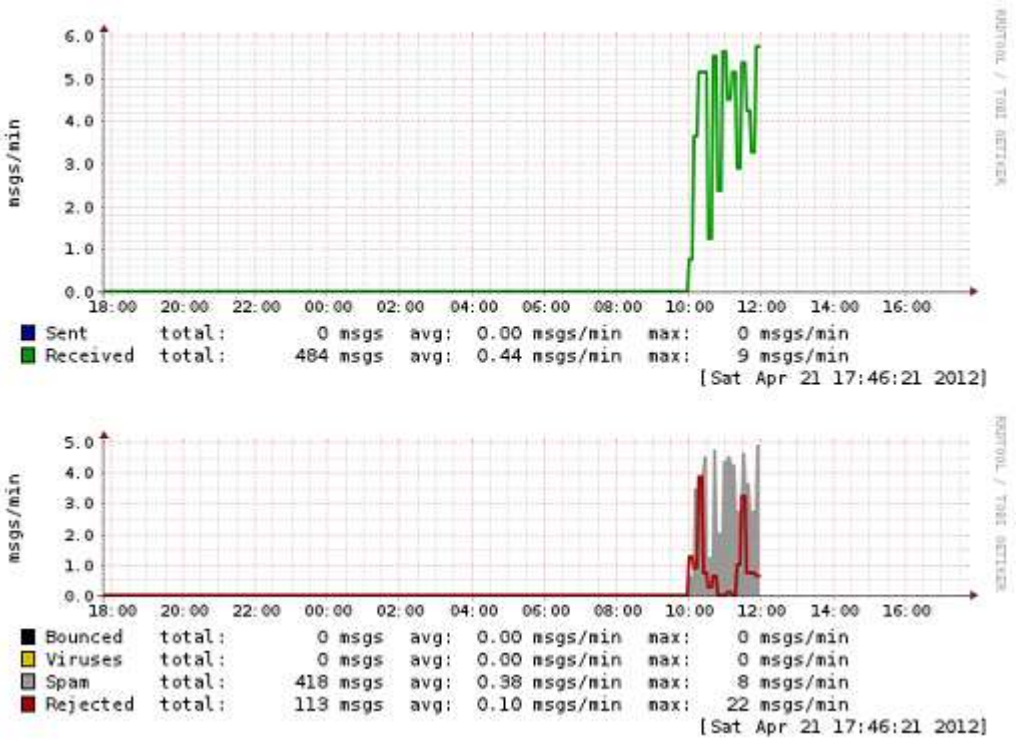


Figura 2.1 Prueba de Spamassassin con mensajes spam

La primera parte de la gráfica representa con una línea verde los mensajes recibidos por minuto y la hora en que estos se recibieron, se observa que el filtro recibió 484 mensajes.

[15] http://mailgraph.schweikert.ch/

En la segunda parte, el color gris representa los mensajes clasificados como *spam*, se observa que **Spamassassin** detectó 418 mensajes como *spam*, de los 484 recibidos, esto quiere decir que el filtro rechazó el 86% de los mensajes *spam*. La línea roja representa otras conexiones por parte de otros servidores hacia este servidor de correo. Como este servidor tiene configurado los filtros de reputación, estos rechazan estas conexiones de servidores desconocidos.

- **Prueba con Dspam**

Para esta prueba se llevó a cabo el envío de los mismos 484 mensajes *spam*, para observar que acciones realizaba el **Dspam** al recibirlos, esto se muestra en la Figura 2.2.

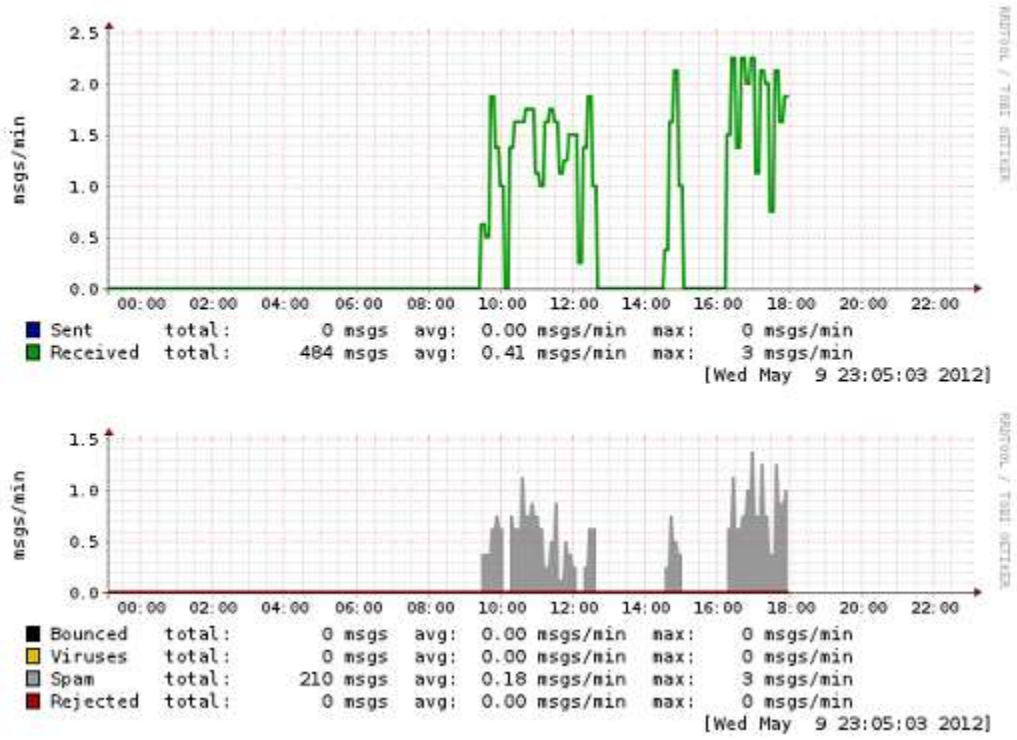


Figura 2.2 Prueba de Dspam con mensajes spam

Se puede observar que de los 484 mensajes recibidos que se representan con la línea verde, 210 fueron detectados como *spam*, esto quiere decir que el 44% de los mensajes fueron detectados como *spam*.

En cuanto a la evaluación, la herramienta *antispam* que mejor cumple con este parámetro es **Spamassassin,** esta herramienta tuvo un rechazo de correo *spam* del 86% de acuerdo al número de mensajes *spam* enviados, mientras que **Dspam** solamente tuvo un rechazo del 44% en el rechazo de mensajes no solicitados, esto quiere decir que la efectividad en el rechazo de mensajes no deseados por parte

de **Spamassassin** es mucho mayor a la efectividad que presenta **Dspam** realizando esta misma función.

La segunda métrica evaluada en el criterio de funcionalidad es la **Efectividad en la aceptación de coreo legítimo**, para ésta se realizan pruebas de las herramientas con el fin de verificar cual es la que mejor cumple con este parámetro, que será la que menor número de falsos positivos identifique. Para graficar los resultados se utilizó **Mailgraph**.

A continuación se evidencian las pruebas realizadas con los filtros **Spamassassin** y **Dspam.**

- **Prueba con Spamassassin**

Luego de probar con correo *spam*, se realizaron pruebas con correo legítimo para observar cuántos de estos deja pasar y observar si se detecta alguno de éstos como *spam*. Esto se muestra en la Figura 2.3.

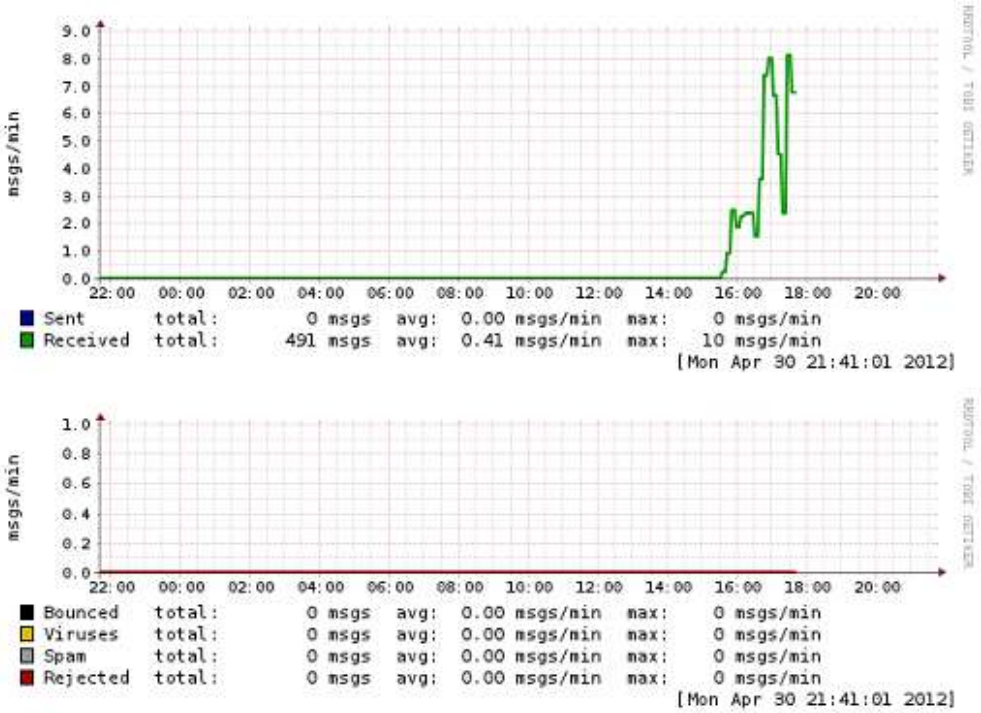


Figura 2.3 Prueba de Spamassassin con mensajes legítimos

La línea verde representa los mensajes recibidos por el filtro, se recibieron 491 mensajes. En la segunda parte de la gráfica se observa que ninguno de los mensajes fue detectado como *spam*. Esto quiere decir que no hubo falsos positivos.

- **Prueba con Dspam**

  De los 491 mensajes recibidos representados con la línea verde, **Dspam** reconoció un falso positivo, esto quiere decir que de los supuestos 491 mensajes legítimos, esta herramienta detectó uno (1) de ellos como *spam*.

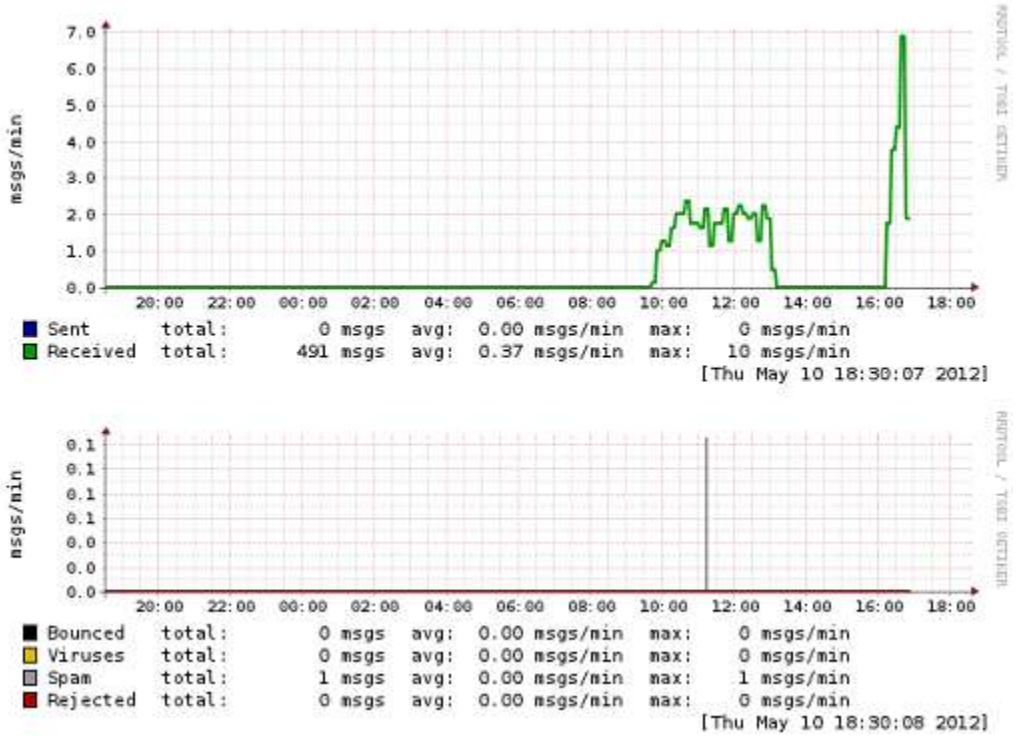


Figura 2.4 Pruebas de Dspam con mensajes legítimos

En la Figura 2.4 se muestra que se enviaron 491 mensajes legítimos que fueron recibidos por el filtro **Dspam**, para verificar que acciones realizaba.

En cuanto a la evaluación, la herramienta *antispam* que mejor cumple con este parámetro es **Spamassassin,** el número de falsos positivos de esta herramienta fue igual a cero o sea de un 0%, mientras que **Dspam** detectó un falso positivo que equivale a un 0.2%. Esto quiere decir que la efectividad en aceptación de correo legítimo por parte de **Spamassassin** es mayor que la de **Dspam**.

La siguiente métrica es el **Manejo de redes bayesianas** y tanto **Spamassassin** como **Dspam** manejan este método, pero la única que cumple con la métrica del **Manejo de métodos heurísticos** es **Spamassassin**. Las dos herramientas cumplen con el **Uso de redes colaborativas** como complemento para la detección de correo no deseado y también cumplen con la ultima métrica ya que ambas son de **Software Libre.**

A continuación se observan una serie de tablas, que presentan la evaluación de cada uno de los criterios y sus métricas en las herramientas.

Tabla 2.4 Evaluación de Funcionalidad

Funcionalidad	Peso	Puntuación	
		Spamassassin	Dspam
Efectividad en el rechazo de *spam*	3	3	2
Efectividad en la aceptación de correo legitimo	3	3	1
Manejo de redes bayesianas	2	2	2
Manejo de métodos heurísticos	2	2	-2
Uso de redes colaborativas	2	2	2
Software libre	1	1	1
Total	**13**	**13**	**6**
Porcentaje total (%) = Puntuación Total / Peso total		**100.00 %**	**46.15 %**

Al porcentaje obtenido como resultado de la evaluación del criterio de funcionalidad se le asigna una puntuación, como se muestra en la Tabla 2.5.

Tabla 2.5 Puntuación Asignada al Porcentaje Obtenido

Porcentaje obtenido	Puntuación	Descripción
Menor a 65 %	1	Inaceptable
Entre 65 % y 80 %	2	Pobre
Entre 80 % y 90 %	3	Aceptable
Entre 90 % y 96 %	4	Muy Bueno
Mayor a 96 %	5	Excelente

De acuerdo con esa puntuación (Puntuación total no ponderada) se obtiene el resultado final de la puntuación de cada una de las herramientas evaluadas de acuerdo al peso que se le dio al criterio de funcionalidad que para este caso fue del 25%, como se muestra en la Tabla 2.6.

Tabla 2.6 Resultado de Evaluación de Funcionalidad

Funcionalidad (25%)	Spamassassin	Dspam
Puntuación total no Ponderada (PNP)	5	1
Calificación Ponderada= PNP * 25%	**1.25**	**0.25**

La Tabla 2.7, muestra la evaluación del criterio de Calidad, para la puntuación de las métricas de este criterio se tomo como referencia [23] para **Spamassassin** y para **Dspam** se tomaron como referencia a [24] y [25].

Tabla 2.7 Evaluación de Calidad

Calidad (20%)	Ponderación	Spamassassin		Dspam	
		Puntuación no Ponderada (PNP)	Puntuación Ponderada (PP)	PNP	PP
Número de errores abiertos en los últimos 6 meses (desde 1/1/2009 hasta 30/6/2009)	20%	5	1	5	1
Número de errores corregidos en los últimos 6 meses (en comparación con el número de errores abiertos)	30%	4	1.2	3	0.9
Cantidad de errores críticos/P1 abiertos. (Se toman como críticos errores de prioridad 9 en escala del 1 al 10),	30%	4	1.2	4	1.2
Promedio de tiempo en que se solucionan los errores críticos / P1 en los últimos 6 meses	20%	4	0.8	1	0.2
Calificación No Ponderada (CNP)			4.2		3.3
Calificación Ponderada= CNP * 20%		**0.84**		**0.66**	

En la Tabla 2.8, se observa la evaluación de Rendimiento. Para la información de pruebas de rendimiento de **Spamassassin** se tomó como referencia a [26] y para **Dspam** a [27].

Tabla 2.8 Evaluación de Rendimiento

Rendimiento (20%)	Ponderación	Spamassassin		Dspam	
		Puntuación no Ponderada (PNP)	Puntuación Ponderada (PP)	PNP	PP
Pruebas de rendimiento e informes de referencia disponibles	50%	3	1.5	3	1.5
Ajuste de rendimiento y configuración	50%	5	2.5	5	2.5
Calificación No Ponderada (CNP)			4		4
Calificación Ponderada= CNP * 20%		**0.8**		**0.8**	

La Tabla 2.9, muestra la evaluación del criterio Comunidad. Para **Spamassassin** se tomó como referencia [28] para la lista de correo general y [29] para el número de contribuyentes. Para conseguir la información de **Dspam** se tomó como referencias a [30] y [31].

Tabla 2.9 Evaluación de Comunidad

Comunidad (15%)	Ponderación	Spamassassin		Dspam	
		Puntuación no Ponderada (PNP)	Puntuación Ponderada (PP)	PNP	PP
El volumen medio de la lista de correo general en los últimos 6 meses	50%	4	2	1	0.5
Número de contribuyentes de código en los últimos 6 meses	50%	4	2	2	1
Calificación No Ponderada (CNP)			4		1.5
Calificación Ponderada= CNP * 15%		**0.6**		**0.225**	

En la Tabla 2.10, se muestra la evaluación del Criterio de Documentación, para evaluar este criterio, la información de **Spamassassin** se obtuvo de [32], [33] y [34]; la información de documentación de **Dspam** se obtuvo de [35] y [36].

Tabla 2.10 Evaluación de Documentación

Documentación (10%)	Ponderación	Spamassassin		Dspam	
		Puntuación no Ponderada (PNP)	Puntuación Ponderada (PP)	PNP	PP
Existencia de varios tipos de documentación	50%	5	2.5	5	2.5
Marco de contribución de usuario	50%	5	2.5	5	2.5
Calificación No Ponderada (CNP)			5		5
Calificación Ponderada= CNP * 10%		**0.5**		**0.5**	

La Tabla 2.11, muestra la evaluación del criterio de soporte, para obtener esta información de **Spamassassin** se tomó como referencia [37], [38], [39] y [40] y para **Dspam** se tomó como referencia a [41] y [42].

Tabla 2.11 Evaluación de Soporte

Soporte (5%)	Ponderación	Spamassassin		Dspam	
		Puntuación no Ponderada (PNP)	Puntuación Ponderada (PP)	PNP	PP
El volumen promedio de la lista de correo general en los últimos 6 meses	50%	5	2.5	4	2
Calidad de apoyo profesional	50%	5	2.5	5	2.5
Calificación No Ponderada (CNP)			5		4.5
Calificación Ponderada= CNP * 5%		**0.25**		**0.225**	

La Tabla 2.12, muestra la evaluación de Escalabilidad, para obtener la información de este criterio, para **Spamassassin** se tomó como referencia a [43] y para **Dspam** a [35].

Tabla 2.12 Evaluación de Escalabilidad

Escalabilidad (5%)	Ponderación	Spamassassin		Dspam	
		Puntuación no Ponderada (PNP)	Puntuación Ponderada (PP)	PNP	PP
Despliegue de referencia	50%	3	1.5	3	1.5
Diseñado para escalabilidad	50%	5	2.5	5	2.5
Calificación No Ponderada (CNP)			4		4
Calificación Ponderada= CNP * 5%		**0.2**		**0.2**	

6. Se obtuvo el resultado de la evaluación, para saber que herramienta utilizar. este punto también se encuentra evidenciado en la sección **6** del Anexo C.

El resultado final de la evaluación de cada criterio en cada una de las herramientas y la puntuación BRR se muestra en la Tabla 2.13.

Tabla 2.13 Puntuación BRR

Posición	Categoría	Spamassassin	Dspam
1	Funcionalidad	1.25	0.25
2	Calidad	0.84	0.66
3	Rendimiento	0.8	0.8
4	Comunidad	0.6	0.225
5	Documentación	0.5	0.5
6	Soporte	0.25	0.225
7	Escalabilidad	0.2	0.2
	Puntuación BRR	**4.44**	**2.86**

De acuerdo a los resultados obtenidos se puede realizar un análisis que permite llegar a las siguientes conclusiones:

- En cuanto a funcionalidad se puede decir que la herramienta que mayor puntuación tuvo en este criterio es **Spamassassin**, esto se debe a que es la herramienta que presenta mayor rechazo de mensajes *spam* y porque no tuvo detección de falsos positivos. A **Spamassassin** y **Dspam** se les premia por usar redes colaborativas y a **Dspam** se le castiga por no manejar métodos heurísticos.

- De acuerdo a la evaluación y resultado de calidad, se puede observar que las dos herramientas presentan una buena calificación debido a que los errores que estas han presentado, se les ha dado una rápida solución.

- Se puede observar que la documentación y el soporte que tienen las herramientas permiten tener una alta puntuación, ya que éstas tienen diversos tipos de documentación en los cuales los usuarios se pueden apoyar y además de esto los grupos de trabajo de cada herramienta brindan un gran soporte en cuanto a la solución de problemas.

- En cuanto a escalabilidad, las herramientas fueron pensadas para que fueran escalables, por lo tanto tienen una puntuación similar.

- La puntuación del criterio de Comunidad, varía entre las dos herramientas debido a que el número de contribuyentes en el desarrollo de las herramientas en los últimos meses difiere bastante.

De acuerdo a la puntuación BRR, la herramienta con mayor calificación es **Spamassassin,** por lo tanto es la herramienta *antispam* de software libre que se va a tener en cuenta para ser puesto en funcionamiento en el desarrollo de este proyecto.

2.3 SISTEMA DE CORREO MEJORADO

En esta etapa se presentan por medio de esquemas las mejoras implantadas y la integración de herramientas para atender a las necesidades del sistema de correo de la Institución. Se genera un esquema del sistema de correo mejorado con la integración de herramientas para el control de *spam*, con un sistema que cuente con autenticación y cifrado y en el cual se pueda realizar la verificación de robustez de las contraseñas que los usuarios crean para utilizar el servicio de correo electrónico.

2.3.1 Sistema mejorado con módulo *antispam*

Para poner en funcionamiento un servicio de correo electrónico, se deben tener en cuenta una gran cantidad de aspectos para ofrecer un servicio seguro y de confianza para los usuarios. Según las referencias [44], [45] y [46], se encuentran los siguientes aspectos:

- **Alta disponibilidad:** se busca que el servicio esté disponible en todo momento, evitando situación de colapso.

- **Reglas anti_relay:** con estas reglas se busca que se garantice un uso legítimo del servicio de correo, aceptando mensajes cuyo destino sea la propia organización o bien dominios delegados.

- **Autenticación:** que el sistema pida credenciales de acceso, la finalidad es que el sistema de correo sea utilizado solo por usuarios que pertenezcan al servicio evitando que los servidores sean utilizados por personas ajenas a éste.

- **Seguridad de transporte:** cifrar la conexión para proteger los datos de autenticación.

- **Control sobre el origen de los mensajes:** verificar la procedencia de los mensajes

- **Análisis sobre el contenido de los mensajes:** la verificación se realiza para determinar si un mensaje es *spam*.

- **Control sobre el correo saliente:** permite controlar el flujo de mensajes que salen del servidor en caso de que una cuenta del sistema sea utilizada como emisor de *spam*

- **Política de Logs:** permiten identificación de problemas y también que se generen datos estadísticos acerca del funcionamiento del servicio de correo.

Estos aspectos se deben tener en cuenta cuando se va a poner en funcionamiento un servicio de correo electrónico. Los puntos anteriores en donde se especifican los aspectos que son los más relevantes, también se encuentran sugeridos en el documento de la RedIris[16]. De acuerdo a esto se opta por escoger como base para el diseño del sistema de correo electrónico de este proyecto, las sugerencias e indicaciones que se exponen en este documento.

La RedIris, entidad certificadora del nivel de calidad de un sistema de correo electrónico, ha generado un documento conocido como *Racev2 (Red Avanzada de Correo Electrónico)* [11], el cual expone los criterios para la creación de una red de confianza, brinda diferentes recomendaciones para el diseño y configuración del servicio de correo electrónico, teniendo en cuenta la calidad del servicio ofrecida a usuarios locales y también a los dominios con los que se intercambia tráfico SMTP. Basándose en controlar y disminuir el *spam* que llega y que genera una institución, algunos de los aspectos básicos que se deben tener en cuenta son los siguientes [47] :

[16] RedIRIS: Red española para la interconexión de los recursos Informáticos de las universidades y centros de investigación.
http://www.rediris.es/

- Documento oficial y normas del servicio
- Filtro en el puerto SMTP de la organización, tanto para entrada, como para el correo saliente.
- Uso de comunicación cifrada entre servidores (TLS)
- Revisión de antivirus y *antispam* de los mensajes que salen del dominio de la institución.

De acuerdo a aspectos de diseño y configuración para el servicio de correo electrónico se tienen en cuenta algunas consideraciones [11]. Las de mayor interés para el desarrollo de este proyecto se describen a continuación:

- **Enrutamiento SMTP:** normas que se deben tener en cuenta de acuerdo a la infraestructura con la cual se cuenta.

- **Autenticación y cifrado:** autenticación centralizada, protección de la información.

- **Antivirus:** para correo entrante y saliente.

- **Antispam:** para correo entrante y saliente

- **Cambio de contraseñas:** que el usuario pueda realizar esta tarea sin intervención de terceros.

- **Manejo de listas de distribución:** para facilidad en la comunicación dentro de la institución.

Teniendo como guía lo anterior se realiza la configuración y la integración de herramientas para obtener un sistema mejorado que cumpla con las características para atender a las necesidades del sistema de correo de la Institución. Para mostrar la integración de las herramientas y configuraciones al sistema de correo utilizando una notación estandarizada se toma nuevamente como referencia UML y se genera un diagrama de implantación, el cual es un esquema basado en bloques que permite observar cuáles son las componentes del sistema mejorado, Figura 2.5.

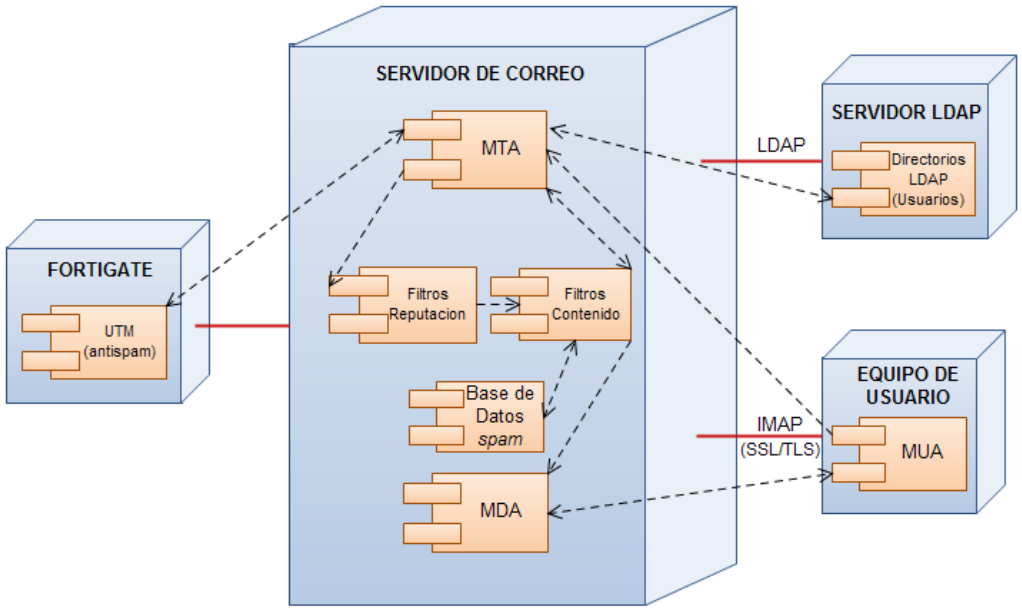


Figura 2.5 Diagrama de implantación- sistema de correo mejorado

En la Figura 2.5 se observan cuatro nodos que son el servidor de correo, el servidor de directorios LDAP, la plataforma Fortigate y el equipo de usuario, cada uno de ellos con sus componentes y las conexiones existentes entre éstos.

Para mostrar la interacción entre los componentes y el flujo de eventos que se presenta entre ellos, se hizo una adaptación con los elementos que ofrece la herramienta **EdrawMax** para generar esquemas, específicamente los que se utilizan para representar los diagramas de secuencia y se hizo un diagrama que pudiera mostrar el proceso de comunicación y de acciones realizadas entre estos componentes. Cabe aclarar que se utilizan los elementos gráficos que UML ofrece para visualizar de una manera más clara y estandarizada la secuencia que seguiría el análisis de *spam*. La Figura 2.6 muestra este proceso para el correo entrante.

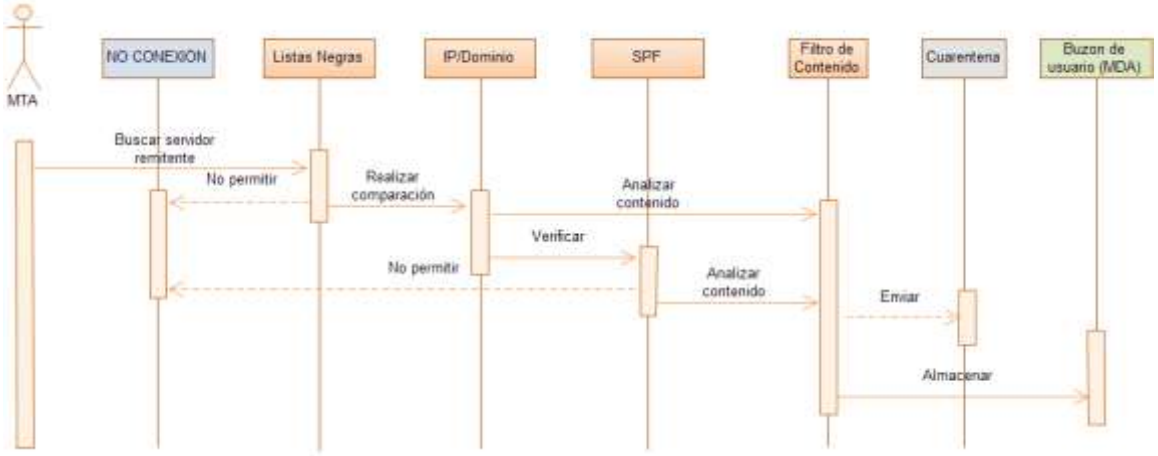


Figura 2.6 Comunicación componentes - sistema de correo mejorado (Correo entrante)

La Figura 2.7 muestra el proceso de comunicación y acciones realizadas entre los componentes para el correo saliente.

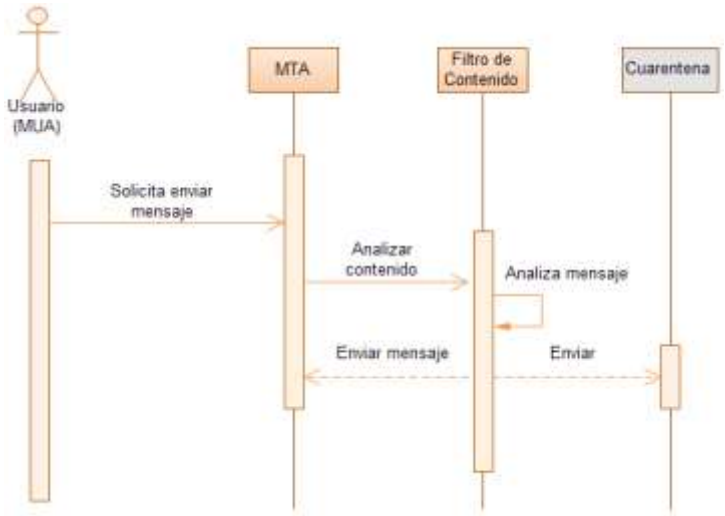


Figura 2.7 Comunicación componentes - sistema de correo mejorado (Correo saliente)

De acuerdo a las instalaciones y configuraciones realizadas en el sistema de correo de la Institución se genera un esquema que aparece en la Figura 2.8 en el que se integran las mejoras que contribuyen a solucionar las falencias que en éste se presentan. Se pueden observar los elementos que conforman un sistema de correo electrónico, teniendo en cuenta un módulo *antispam* en el que se encuentran los filtros encargados de hacer una revisión y verificación de los mensajes cuando éstos pasan por cada uno de sus componentes y de esta manera realizar las acciones necesarias también descritas en este esquema. En este módulo *antispam* se tienen en cuenta varias acciones para las cuales se pueden necesitar diversas herramientas y también varias modificaciones en los archivos de configuración de cada uno de los programas requeridos. Se puede ver claramente cómo se hace la comunicación entre estos elementos cuando se va a enviar correo hacia otros dominios y también cuáles de estos están implicados cuando se reciben mensajes de correo que provienen de dominios externos.

De tal forma, el esquema de la Figura 2.8 muestra diversos recursos que fueron implantados como resultado de este trabajo de grado en el sistema de correo de la Universidad del Cauca, al compararlo con el esquema de la Figura 1.1.

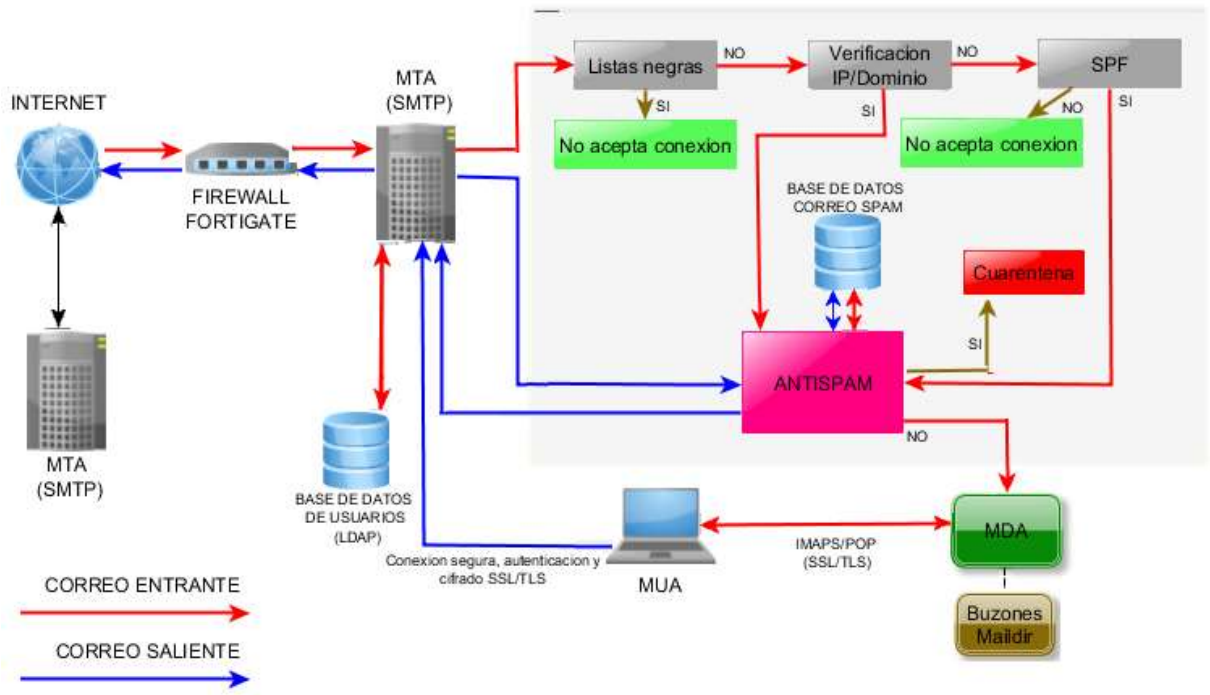


Figura 2.8 Sistema de correo electrónico y módulo antispam

A continuación se describe el esquema de la Figura 2.8.

Para el funcionamiento de un sistema de correo electrónico se requiere de diversos módulos los cuales necesitan estar correctamente configurados y conectados entre si para realizar las tareas que se requieren en el sistema. En las secciones siguientes se describe el sistema de correo mejorado y las herramientas utilizadas en cada uno de sus componentes.

2.3.1.1 Correo entrante

Cuando llega correo externo al servidor de correo electrónico (MTA), éste consulta hacia quien va dirigido el mensaje en la **Base de datos de los usuarios (LDAP)**. Luego de que se conoce el destinatario se empieza por realizar las revisiones del mensaje para el control de *spam* y de código malicioso dentro de estos a través de los filtros de reputación. El primer filtro del módulo *antispam* son las **Listas negras,** en estas listas se encuentran las direcciones IP y dominios de los servidores que envían *spam*. En caso de que el cliente esté reseñado en la lista negra no se acepta la conexión. Si el cliente no se encuentra en esta lista, el servidor envía al cliente un mensaje de aceptación, entonces el cliente responde con el nombre de su dominio. Luego de esto se pasa a la **verificación IP/dominio**, el servidor verifica que la IP sea la misma que se obtiene resolviendo el dominio, si es así, el servidor del cliente envía la dirección de correo del remitente. Si la dirección IP no coincide con el dominio, pasa al siguiente filtro que está conformado por el Entorno de Políticas del Remitente (SPF, *Sender Policy Framework*) conocidos como

registros SPF. El dominio del remitente del mensaje no necesariamente es el mismo dominio del servidor que está enviando el mensaje, entonces, éstos registros sirven para verificar qué servidores están autorizados por el dominio para enviar mensajes de correo electrónico, si no es así no se acepta la conexión. La cuarta etapa son los filtros de contenido **Antispam,** en éste se encuentra el analizador de s*pam*, si se cataloga como *spam* es adicionado a una **Base de datos de correo *spam*** manejada por los filtros de contenido y en la que se encuentran mensajes *spam* que han llegado al servidor. Si el mensaje no es clasificado como *spam* pasa al buzón del usuario para finalmente poder ser recuperado y leído por el usuario (MUA).

2.3.1.2 Correo saliente

Inicialmente el usuario a través del MUA envía el mensaje comunicándose con el servidor (MTA) para que los mensajes puedan ser enviados hacia el exterior. Esta comunicación se realiza de forma segura mediante autenticación y cifrado. Antes de que los mensajes salgan, estos son analizados por el filtro **Antivirus/Antispam** para saber si el mensaje que se quiere enviar está clasificado como correo no deseado o si contiene código malicioso, el filtro de contenido realiza una verificación en la **Base de datos de *spam*** para saber si el mensaje se encuentra reseñado como *spam.* Para los mensajes de salida se analiza la cantidad de mensajes enviados por cada usuario y el número de mensajes que se envían en cierto intervalo de tiempo, esto se hace para evitar que el dominio se encuentre transmitiendo *spam.* Finalmente después de analizados los mensajes, el servidor de correo transmite el mensaje hacia el exterior del dominio. La comunicación entre servidores también se realiza de forma segura mediante autenticación y cifrado.

2.3.1.3 Agente de transferencia de correo (MTA)

El MTA que se debe utilizar para el sistema de correo mejorado es el servidor **Postfix.** Este servidor es el que se utiliza para ofrecer el servicio de correo en la Universidad del Cauca y para el desarrollo de este proyecto no se hace necesario cambiar a otro servidor. En el Anexo A de generalidades del correo electrónico se mencionan otros servidores de correo como **Exim**[17], **Sendmail**[18] y **Qmail**[19]. Aunque el servidor de correo que se va a seguir utilizando es **Postfix**, también se llevo a cabo la instalación y configuración del servidor **Exim** durante el desarrollo del presente proyecto, con el fin de probar y observar un servidor de correo diferente en atención a considerar un posible cambio, pero una vez se trabajó con **Postfix** las ventajas del mismo indicaron que no era necesario. La instalación y configuración de estos servidores de correo se detalla en el Anexo D.

A continuación en la Tabla 2.14 se presenta una comparación que permite observar las características de los servidores de correo, tomando como referencia el grupo GNU/Linux de la Universidad del Cauca [48].

[17] http://www.exim.org/
[18] http://www.sendmail.com
[19] http://www.qmail.org/

Tabla 2.14 Comparación entre servidores de correo

	Qmail	Sendmail	Postfix	Exim
Soporte al software y documentación	El soporte es bajo ya que no es mantenida por una comunidad	La documentación es buena y abundante. Cuenta con una compañía dedicada a sus servicios	Abundante documentación disponible y cuenta con una comunidad activa que lo respalda	Abundante documentación disponible y tiene una comunidad de respaldo.
Seguridad	Alto nivel de seguridad. Pensado en seguridad de los usuarios	Presenta vulnerabilidades en su seguridad [49].	Fue construido poniendo especial atención en seguridad para ofrecer un servicio confiable	Fue diseñado pensando en la seguridad del servicio.
Configuración	Su configuración es sencilla.	Una de las características de Sendmail es la complejidad de su configuración.	Facilidad de configuración y fácil administración. Sus configuraciones por defecto son muy completas y seguras.	Su configuración es sencilla y sus configuraciones por defecto son muy completas.
Escalabilidad	Su escalabilidad es media ya que no apoya estándares modernos como el direccionamiento IPv6 y no tiene un grupo oficial encargado de su gestión.	Fue diseñado para ser escalable.	Su diseño modular hace que fuera pensado para ser escalable	Fue diseñado para ser escalable. Puede ser ajustado a las necesidades del usuario.
Otras características	Necesita de otros módulos que no son gratuitos para desarrollar funciones especiales.	Es instalado por defecto en la mayoría de sistemas operativos de Unix comercial.	Surgió debido a la complejidad de Sendmail. Fue diseñado pensando en la simplicidad y la compatibilidad. En caso de querer sustituir Sendmail por Postfix, este último puede utilizar los archivos de configuración de Sendmail.	Diseñado para manejar grandes cantidades de correo.

2.3.1.4 Servidor IMAP/POP

Para poder realizar la lectura de los mensajes se necesita del protocolo IMAP o del Protocolo de Oficina de Correo Postal (POP, *Post Office Protocol*), estos permiten acceder a los mensajes almacenados en el servidor. Existen diversos servidores POP e IMAP, entre ellos se encuentran **UW**[20], **Courier**[21], **Dovecot** y **Cyrus**[22] [50]. A continuación se presenta en la Tabla 2.15 una comparación de los servidores IMAP, para poder observar algunas de sus características.

Tabla 2.15 Comparación de servidores IMAP

	Dovecot	Courier	Cyrus	UW
Soporte de formato Mbox y Maildir	El sistema fue desarrollado para trabajar con ambos formatos	Inicialmente el sistema manejaba solo Maildir pero las versiones recientes manejan los dos formatos	El sistema fue desarrollado para manejar Maildir pero las versiones recientes manejan ambos formatos	Inicialmente el sistema manejaba solo Mbox pero las versiones recientes manejan los dos formatos
Facilidad de configuración	Simplicidad de funcionamiento y configuración	Simplicidad de funcionamiento y configuración	Dificultad de configuración y administración.	Simplicidad de funcionamiento y configuración
Compatibilidad con TLS	Total compatibilidad	Total compatibilidad	Total compatibilidad	Total compatibilidad
Software Libre.	si	si	si	si

Como estos servidores no presentan mayor diferencia en su funcionalidad, se optó por continuar con el servidor **Dovecot**, ya que además de ser diseñado pensando en la seguridad como característica principal, es el servidor IMAP con el que se trabaja en el sistema de correo de la Universidad del Cauca, además, es compatible con otros servidores como **UW** y **Courier** en caso de querer migrar a estos.

Se probaron los servidores **Courier-pop** y **Courier-imap** para realizar envío de correo ya que se quería conocer su funcionamiento en un sistema de correo electrónico. Las instalaciones y descripción de estos servidores se encuentran en el Anexo D. La configuración que traen estos por defecto, es suficiente para comunicarse con **Postfix** y LDAP. Para la administración de servicios a través de la web se hace la instalación del

[20] http://www.washington.edu/imap/
[21] http://www.courier-mta.org/imap/
[22] http://cyrusimap.web.cmu.edu/

Webadmin de **Courier**, este se utiliza para configurar todos los parámetros del servidor LDAP sin necesidad de hacerlo por consola. Para revisar los mensajes de correo que se instaló y configuró, se hizo necesaria la instalación de una interfaz de correo o webmail, para este caso se utilizó **Squirrelmail**[23] que puede trabajar con cualquier navegador.

2.3.1.5 Almacenamiento de usuarios mediante LDAP

El uso de directorios trae como beneficio poder tener un modelo de autenticación centralizado, esto quiere decir que los datos de usuario se encuentran en un solo lugar y que pueden ser utilizados por diversos servicios y aplicaciones. Este es uno de los aspectos que se desea seguir manejando en el sistema de correo de la Universidad del Cauca, por lo tanto en la configuración de las herramientas tenidas en cuenta en el presente trabajo, se utilizó el esquema de directorios LDAP para almacenar los datos de usuario del servicio de correo.

De acuerdo con [51], el manejo de LDAP brinda ciertas utilidades que sobresalen en comparación con las bases de datos comunes, como que permite crear múltiples directorios y también se puede utilizar la misma base de datos LDAP para distintos servicios y aplicaciones, ya que la mayoría tienen soporte para manejar el servicio de directorios, esto trae como beneficio en que la administración de los usuarios esté centralizada y no se necesite gestionar esta información en un lugar diferente para cada servicio.

Los servidores LDAP son de fácil instalación y mantenimiento, el almacenamiento de la información se hace de forma jerárquica o de árbol, esto quiere decir que existe una raíz por la cual se inicia la búsqueda y a partir de esta se desprenden varias ramas las cuales pueden ser otros directorios o archivos y las cuales pueden tener atributos. Otra ventaja que presenta LDAP es que fácilmente se pueden hacer réplicas de los servidores.

Existen muchos servidores LDAP y mayoría de ellos funcionan correctamente bajo Linux, algunos de los más utilizados son **OpenLDAP**[24], **Sun SunONE 5.2**[25]*,* **Microsoft ADS – Active Directory Server**[26]**, Novell eDirectory**[27] **y Red Hat Directory Server**[28]**.**

El servidor de directorios utilizado es **OpenLDAP**, esto es debido a que es de software libre y puede operar bajo Linux. Otro requerimiento que cumple **OpenLDAP** es que se puede configurar de modo maestro-maestro, esto se hace cuando se quiere tener como respaldo otros servidores LDAP en caso de perder el servidor principal. Lo importante de esta configuración es que el servidor de respaldo va a tener las mismas características y se pueden realizar las mismas tareas que se realizaban con el servidor maestro, se

[23] http://squirrelmail.org/
[24] http://www.openldap.org/
[25] http://docs.oracle.com/cd/E19199-01/816-6703-10/index.html
[26] http://www.microsoft.com/en-us/server-cloud/windows-server/active-directory-overview.aspx
[27] http://www.novell.com/products/edirectory/
[28] http://www.redhat.com/products/identity-management/directoryserver/

pueden realizar modificaciones de la información, mientras que con una configuración maestro- esclavo solo se podría hacer lectura de la información en el servidor esclavo.

Para la utilización de **OpenLDAP** no se llevo a cabo un proceso de selección de software ya que éste es el que se encuentra funcionando en el sistema de correo de la Universidad del Cauca y no se hace necesario cambiar el método de almacenamiento, ya que esto no influye con los objetivos de este trabajo de grado.

En el Anexo D se evidencian las diversas instalaciones y configuraciones que se realizaron para observar las características de algunas de las herramientas antes mencionadas, detallando la instalación y configuración de los servidores de correo **Postfix** y **Exim**, también la instalación de **Openldap** para manejar el servicio de directorios, configurándose para poder comunicarse con el servidor de correo.

2.3.1.6 Filtros de reputación

Los filtros de reputación son los que se encargan de verificar la procedencia de los mensajes. Los filtros tenidos en cuenta fueron: listas negras, verificacion IP/dominio, registros SPF.

Para el manejo del servicio de listas negras se escogieron las listas **Spamcop**[29] y **Spamhaus**[30]. Para la elección de estas listas, se definió como criterios aquellas que sean actualizadas de forma permanente y que tengan la reputación de rechazar altas cantidades de *spam*, gracias a las listas de servidores reseñados como emisores de *spam* [52]. Estas listas presentan un bajo rango de falsos positivos, esto quiere decir que es muy baja la posibilidad de que el servidor que se encuentre reseñado en estas listas no sea emisor de *spam*.

Para la verificación de IP/Dominio, se realizaron algunas configuraciones en las restricciones de **Postfix**.

El último filtro son los registros SPF [53]. Una de las formas más utilizadas para enviar *spam,* es a través de la suplantación de un dominio, este método puede evitar que esto suceda ya que este verifica que el servidor que esta enviando el mensaje tenga autorización del dominio, en caso contrario este es rechazado. Para configurar este filtro se necesita de la instalación de algunos paquetes que se encuentran especificados en la sección 1.1 del Anexo E, en donde también se evidencian algunas modificaciones de los archivos de **Postfix**.

Otro mecanismo para verificar mensajes de correo es a través de las firmas de Correo Identificado por Claves de Dominio (DKIM, *Domainkeys Identified Mail*), en éstas se genera una firma digital del dominio que está enviando el correo, pero este método puede

[29] http://www.spamcop.net/
[30] http://www.spamhaus.org/

fallar en el momento que el mensaje sea retransmitido por otro servidor y éste modifique en algún sentido el mensaje, como por ejemplo que se coloque un pie de pagina del mensaje o alguna descripción del servidor.

Las funciones que realizan los filtros de reputación se configuran en los archivos de **Postfix**, agregando algunas restricciones para realizar esas tareas. Las configuraciones de los filtros de reputación son evidenciadas en el Anexo E.

2.3.1.7 Filtros de contenido y otras herramientas para el control de *spam*

Este bloque que aparece indicado como **Antispam** en el esquema de la Figura 2.8, es el encargado de realizar el filtrado de contenido de los mensajes de correo electrónico para ver si se trata de correo no deseado. Este es el último filtro presente en el módulo *antispam* del sistema de correo. Si el mensaje deja atrás todos los filtros, entonces el mensaje es clasificado como válido, transfiriéndose hacia el buzón de usuario de destino para su almacenamiento.

Se realizó la integración de **Spamassassin** como filtro de contenido para trabajar en conjunto con la plataforma **Fortigate** con la función de realizar el control de spam de los mensajes que no son detectados por **Fortigate**.

Para la base de datos de correo *spam*, se realizó la integración de redes colaborativas **Razor**[31] y **Pyzor**[32] para complementar las funciones de detección de *spam*. A continuación se hace una descripción de estas redes.

Razor y Pyzor

De acuerdo con [54], **Razor** y **Pyzor** son redes colaborativas para las herramientas *antispam*, son herramientas de software libre que mantienen una actualización constante acerca del *spam* que se esta propagando, para que puedan ser filtrados de los mensajes legítimos. Estas redes pueden trabajar de forma complementaria con otras herramientas para realizar la detección de *spam*, como por ejemplo **Spamassassin**., además de manejar sus propias técnicas. Estos filtros utilizan bases de datos de mensajes *spam* para realizar una comparación con los mensajes que ahí se encuentran y de esta manera detectar si un mensaje es *spam* o no. Estas son bases de datos en las que la comunidad de usuarios, publica y comprueba el *spam* que les llega.
Como valor agregado para realizar control de *spam*, también se configuró la herramienta **Policyd** para complementar el control de correo saliente del dominio de la Institución, ya que esta es una herramienta que presenta unas características especiales que permiten realizar funciones que son completamente diferentes a las que cumple el filtro de contenido seleccionado y ayudan a contribuir a las necesidades en el sistema de correo de la Institución. A continuación se realiza una descripción de esta herramienta.

[31] http://razor.sourceforge.net/
[32] http://sourceforge.net/apps/trac/pyzor/

Policyd

Es una herramienta de software libre descrita en [55], creada para manejar gran cantidad de flujo de correo, cumple funciones de control de *spam* y está diseñada especialmente para trabajar con el Agente de correo **Postfix**. Es una herramienta que maneja *quotas* de correo, estas son características de control de volumen de mensajes por dominio, control de mensajes por usuario y limite de usuarios por mensaje, también se caracteriza por manejar listas blancas, listas grises y listas negras. Por la gran variedad de características que posee **Policyd**[33], se convierte en una opción bastante viable para ser configurada y probada, ya que puede ofrecer grandes beneficios en cuanto al control de *spam* en el servicio de correo de la Universidad del Cauca, en especial para realizar control del correo interno y del correo que se genera desde la Institución hacia ella misma o hacia afuera.

Esta herramienta maneja el método de "*triplets*" para determinar si un mensaje es posible *spam,* este término tiene incluido tres aspectos para el envío de correo, que son:

- ✓ La dirección IP del host que intenta el envío.
- ✓ La dirección del remitente.
- ✓ La dirección del destinatario.

Policyd es utilizado para controlar el flujo de mensajes que generan los usuarios del sistema, como por ejemplo cuando un software malicioso utiliza las cuentas para el envío masivo de mensajes *spam.* Ésta se encarga de controlar el número de mensajes permitidos para ser enviados por un usuario en un periodo de tiempo y también de restringir el número de usuarios a quien va dirigido. **Policyd** no hace revisión del contenido del mensaje como tal, lo que se hace con esta herramienta es aplicar restricciones a los usuarios en cuanto al envío de mensajes, haciendo que no se superen ciertos limites que son determinados por el administrador de**l** servicio.

Aunque no es uno de los problemas a solucionar, es importante contar con un módulo antivirus para proteger el sistema. Para esto se probaron herramientas antivirus que aunque no se utilizaron, se realizó su instalación y configuración que se encuentran detalladas en el Anexo E. Entre los antivirus se encuentran **ClamAV**[34] y **Amavisd-new**[35]**.** En este anexo también se exponen los filtros de contenido **Spamassasin**, **Policyd** y **Dspam**, de los cuales se realiza la instalación y configuraciones necesarias para que puedan cumplir con sus funciones correctamente. También se detalla la instalación de las redes colaborativas **Razor** y **Pyzor**.
Con la integración de estas herramientas al sistema de correo, se atendió a la necesidad de controlar el *spam* que se le pasaba a Fortigate, dando cumplimiento a uno de los requerimientos identificados por la administración del servicio que era uno de los objetivos de este trabajo de grado.

[33] http://www.policyd.org/
[34] http://www.clamav.net/lang/en/
[35] http://www.ijs.si/software/amavisd/

2.3.2 Sistema mejorado con autenticación y cifrado

Para tratar con los problemas de seguridad mencionados en la sección **2.2.3**, existen algunos mecanismos [56], el protocolo de Nivel de Sockets Seguro (SSL, *Secure Sockets Layer*) y el protocolo de Seguridad del Nivel de Transporte (TLS, *Transport Layer Security*), que son tecnologías que realizan cifrado de la información en conexiones TCP/IP. Además ofrecen la función de autenticación entre clientes y servidores para dar seguridad de la identidad de los mismos. Existen otros mecanismos de autenticación como S/Key y Kerberos, también cabe mencionar la existencia del protocolo de Capa de Seguridad y Autenticación Simple (SASL, *Simple Authentication and Security Layer*) que cuando se encuentran disponibles varios mecanismos de autenticación, brinda la posibilidad de negociar y escoger el mecanismo entre cliente y servidor.

La autenticación SMTP se realiza por medio del protocolo SASL, se configura con el fin de evitar la suplantación de cuentas, verificando que el usuario que está enviando el mensaje es el verdadero remitente, esto hace que aumenten los niveles de seguridad en el servicio de correo electrónico, lo que además de ofrecer protección al trafico de los mensajes, también contribuye a la reducción del envío de *spam*. Cuando el servidor que se está utilizando se ha configurado con módulo de autenticación, éste solicita el ingreso del nombre de usuario y la contraseña antes de enviar el mensaje. El cifrado se llevó a cabo con la herramienta **OpenSSL**[36] que permite implementar los protocolos SSL y TLS.

Para realizar las configuraciones de autenticación y cifrado necesarias, se utilizó un servidor de correo, copia exacta del servidor de producción de la Universidad del Cauca. Como se dijo anteriormente, el servidor de correo que se maneja en la Institución es **Postfix** y utiliza **Dovecot** como servidor IMAP. Todo esto se encuentra soportado en el sistema operativo Linux **Debian**. La información de usuarios se encuentra almacenada en directorios basados en el protocolo LDAP.

En el Anexo F se evidencian las configuraciones de autenticación y cifrado utilizando las herramientas indicadas en esta sección, en éste se describen todos los archivos necesarios y sus respectivas configuraciones para lograr obtener un servicio de correo con solicitud de autenticación de usuarios y con cifrado del canal de comunicación para proteger la información. Luego de realizar dichas configuraciones se procede a realizar una prueba para verificar que el sistema solicita autenticación de usuario.

Con la integración del servicio de autenticación, se atendió a una de las necesidades en el servicio de correo de la Institución, dando cumplimiento a uno de los requerimientos establecidos en los objetivos de este trabajo de grado.

[36] http://www.openssl.org/

2.3.3 Sistema mejorado con verificación de robustez de contraseñas

De acuerdo con los problemas presentados en el servicio de correo de la Universidad del Cauca, evidenciados en la sección **1.2** y debido a la ausencia de un sistema que permita verificar la robustez de las contraseñas de los usuarios, se realiza la configuración de un módulo que ofrece estas funciones para atender a esta necesidad.

Al momento de crear las contraseñas y con la intención de no olvidarla, es normal que un usuario promedio tienda a colocar una contraseña fácil de recordar, por lo tanto utilizan claves bastante predecibles conformadas por sus nombres, iniciales, fechas importantes o cosas muy comunes, lo que puede implicar debilidad en la misma.

Es de gran importancia dar a conocer a los usuarios el nivel de seguridad de la contraseña que se esta creando, para este caso, a partir de un código en **Javascript** que fue tomado como referencia de [57], se realizó una adaptación del mismo y se integró para atender a las necesidades de este proyecto. Este código permite que el usuario conozca el nivel de seguridad de la contraseña que esta originando.

El código se encuentra especificado en el Anexo G, lo que éste hace es verificar si la contraseña que ha introducido el usuario, esta compuesta por la combinación de letras, números, caracteres especiales, letras mayúsculas y también tiene en cuenta el número de caracteres que se utilizan. A medida que el programa verifica que la contraseña cumple con cada una de estos requerimientos, va asignando a una variable un valor numérico que se ira acumulando por cada combinación que se cumpla, esta variable servirá como contador para medir el nivel de seguridad de la contraseña, también se verifica el numero de caracteres de esta palabra y se va sumando a dicha variable un valor numérico dependiendo del número de caracteres que tenga, el valor asignado puede variar si el número de caracteres esta entre, cero (0) y cuatro (4), cinco (5) y siete (7), u ocho (8) en adelante.

Existen métodos para que los usuarios puedan crear una contraseña segura automáticamente. Estos generadores crean contraseñas aleatorias bastante seguras debido a que son difíciles de descifrar. El problema con estos generadores de contraseñas, es que estas no son fáciles de recordar por parte de los usuarios, por lo tanto hace que aunque sea un buen método, sea muy poco utilizado.

En el Anexo G, se muestra un código en **Javascript** que fue encontrado y adaptado a las necesidades del proyecto realizado, el cual permite obtener este tipo de contraseña. La finalidad de este código es entregar contraseña con combinaciones de números, letras mayúsculas, caracteres especiales y longitud igual o mayor a 8 caracteres. Este código permite tomar a través de un formulario de HTML el número de caracteres con que el usuario desea que se genere la contraseña, el número que se ingrese debe ser mayor o igual a 8 de lo contrario la contraseña no se crea.

CAPITULO 3.

3 PRUEBAS Y RESULTADOS

En este capítulo se presenta el plan de pruebas desarrollado y luego se evidencian cada una de las acciones también descritas en este plan para verificar las configuraciones de autenticación, la implantación de las herramientas *antispam* y de un sistema con verificación de robustez de contraseñas. Se exponen los resultados que se obtuvieron de acuerdo con las configuraciones realizadas y con la implantación en el sistema de correo de la Institución. Se evidencian los esquemas de validación de los resultados de las configuraciones y de las herramientas utilizadas.

3.1 PLAN DE PRUEBAS

Para proceder a la etapa de pruebas de las herramientas utilizadas y de las configuraciones efectuadas, se describe el proceso que se va a llevar a cabo para su realización a través de este plan de pruebas, para esta etapa se tomó como referencia los pasos que se siguen en [58] y descripciones que se exponen en [59].

Propósito

El objetivo de las pruebas es verificar que las configuraciones realizadas se encuentren libres de errores, comprobar la eficiencia de la herramienta y por la falta de confiabilidad en caso de que la puesta en funcionamiento no se haga de forma adecuada, de esta manera lo que se busca con las pruebas es validar los resultados obtenidos con las mejoras introducidas al sistema de correo, mostrando que las herramientas que se han puesto en funcionamiento y las configuraciones realizadas se han hecho correctamente y que son las adecuadas para realizar las funciones requeridas.

Enfoque

El proceso de pruebas para la obtención de resultados se encuentra enfocado en la funcionalidad de las herramientas utilizadas y de las configuraciones realizadas, esto quiere decir que de acuerdo a lo que se tiene en el sistema de correo de la Universidad, con las herramientas y las configuraciones que se están aplicando, se espera que éstas cumplan con sus funciones y de esta manera conseguir un mejoramiento en el sistema.

Recursos

Para estas pruebas se tienen como recursos un servidor replica del servidor real de la Institución y el servidor de producción. Primero las configuraciones fueron realizadas en el servidor replica que es una copia exacta del servidor real y de acuerdo a las pruebas realizadas en este, fueron puestas en funcionamiento en el servidor de producción.

Elementos a probar

Los elementos que se van a probar son los siguientes:

- Las herramientas para el control de *spam.*
- La configuración de autenticación y cifrado
- La verificación de robustez de contraseñas

Las actividades que se van a realizar con cada uno de los elementos a probar se describen a continuación:

- Las herramientas para el control de *spam*: se probaron los filtros que se integraron al sistema de correo y que contribuyeron con la solución a las falencias en cuanto al correo no deseado, estas herramientas son **Spamassassin** y **Policyd**. En estas pruebas también se puede observar el funcionamiento de los filtros de reputación.

  Los parámetros que se probaron fueron la efectividad en el rechazo de mensajes *spam* y la efectividad en la aceptación de correo legítimo para validar el funcionamiento del filtro **Spamassassin**. También se realizaron pruebas con **Policyd** para verificar las restricciones aplicadas a los usuarios a través de las configuraciones de este filtro.

  Las gráficas para mostrar los resultados del funcionamiento de estas herramientas, se generaron con la herramienta **Mailgraph**.

- La configuración de autenticación y cifrado: se probaron las diferentes configuraciones para verificar que los procesos de autenticación y cifrado quedaron incluidos en el sistema de correo de la Institución.

  Lo que se quiere verificar con estas pruebas es que el sistema de correo mejorado ya cuenta con el proceso de autenticación de usuarios y de cifrado del canal de conexión. Para la realización de estas pruebas se utilizó la consola de Linux para enviar mensajes de correo a través de conexión con telnet. También se instalaron y configuraron clientes de correo para el envío de mensajes utilizando las características del servidor para manejar autenticación y cifrado. Se utilizaron los clientes de correo **Outlook**, **Thunderbird**, **Zimbra** y **Eudora**. Para examinar los resultados de autenticación y cifrado se utilizó el Analizador de protocolos **Wireshark** mediante el cual se pueden observar los mensajes intercambiados entre cliente y servidor.

- La verificación de robustez de contraseñas: las pruebas se realizaron para verificar el funcionamiento del módulo adaptado a partir de uno ya existente y observar el nivel de seguridad que este va mostrando mientras se va ingresando la contraseña.

  Lo que se busca es verificar el funcionamiento de este módulo cuando se esta ingresando una contraseña y además mostrar que en el sistema de correo de la Institución este ya se encuentra implantado.

Responsables y Riesgos

Los responsables de las configuraciones y de evidenciar las pruebas en el servidor réplica para luego ser pasadas a producción, fueron los desarrolladores de este proyecto y los responsables del traspaso de estas configuraciones al servidor de producción, son los ingenieros del área de Servicios y Servidores de Internet de la Universidad del Cauca.

En primera instancia se utilizó el servidor réplica del servidor real para realizar las configuraciones, debido a que si se generaban errores de cualquier índole en este servidor, no se comprometía el funcionamiento del sistema de correo de la Institución. En el proceso de configuración se pueden generar distintos problemas que hacen que el servicio pueda fallar, ya que se necesita hacer la interconexión de diferentes aplicaciones y configuraciones, por esta razón antes de realizar las configuraciones en el servidor de producción, estas se realizaron y se probaron en el servidor réplica del servidor real. A continuación se presentan las pruebas realizadas.

3.2 PRUEBAS Y RESULTADOS DE MÓDULO ANTISPAM

De acuerdo con las configuraciones de *antispam*, se hace una serie de pruebas para validar los resultados en el servidor de correo de la Institución. Se realizaron pruebas con las herramientas **Spamassassin** y **Policyd** para validar estos resultados.

Para **Spamassassin** se realizaron dos pruebas con mensajes *spam* que llegaron al servidor de correo de la Universidad y que no fueron reconocidos por la plataforma **Fortigate**; para la primera, se tomaron 78 mensajes *spam* y para la segunda 526 mensajes que fueron suministrados por la administración de la red. Para esta última se tomo una cantidad más grande de mensajes ya que se pudo recolectar un mayor número de éstos y de esta manera realizar una prueba más exigente a la herramienta.

Estas pruebas que son las más importantes porque evidencian el aporte de haber realizado este trabajo de grado en cuanto a los problemas de *spam*, fue realizada para observar qué tanto correo no deseado que ha sido permitido por el sistema de correo de la Universidad del Cauca, específicamente el módulo *antispam* de **Fortigate**, es rechazado por este filtro.

Para **Policyd** se realizan pruebas para verificar las configuraciones realizadas a esta herramienta.

3.2.1 Pruebas y resultados con Spamassassin

- **Prueba 1: prueba con 78 mensajes *spam***

Esta prueba fue realizada enviando 78 mensajes *spam* que llegaron al servidor de correo de la Institución entre el 28 de marzo y el 9 de abril de 2012 y que no fueron reconocidos

por la plataforma **Fortigate**, con el fin de detectar cuántos de estos son reconocidos por **Spamassassin**, como se muestra en la Figura 3.1.

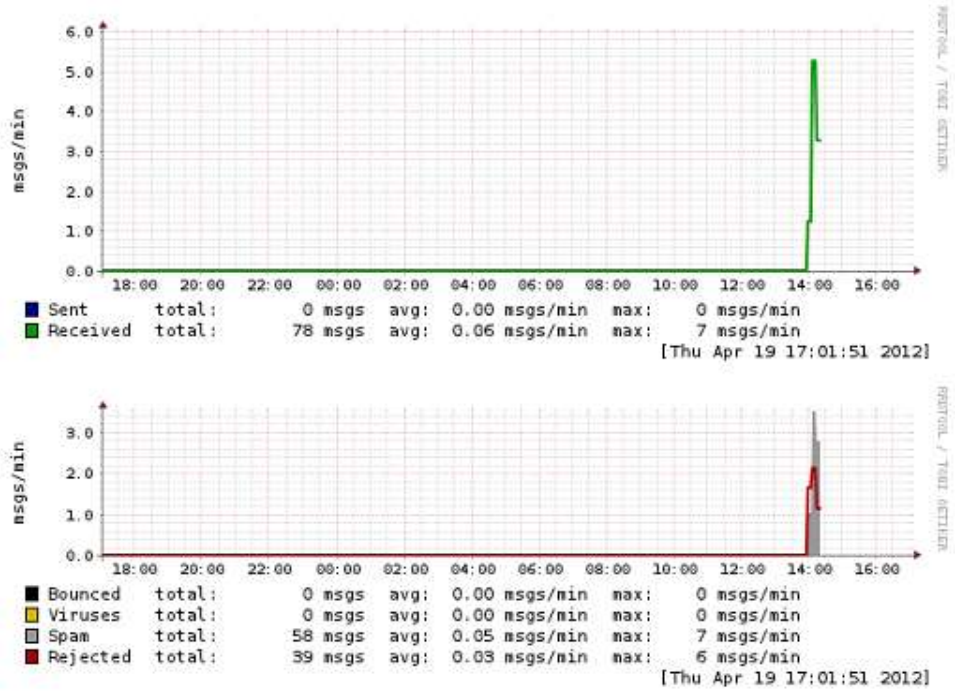


Figura 3.1 Prueba de Spamassassin con 78 mensajes *spam*

La línea verde indica los 78 mensajes recibidos por este filtro. La línea gris representa aquellos que fueron reconocidos como *spam*, para este caso fueron detectados 58 mensajes, esto quiere decir que esta herramienta tiene una efectividad del 74% en el rechazo de *spam*. Este se considera un alto porcentaje de acierto en el reconocimiento de correo no deseado, ya que la herramienta se configuró para que no fuera tan estricta en cuanto a la detección de *spam*, para evitar que se presenten falsos positivos.

La línea roja indica las conexiones rechazadas por los filtros de reputación hacia otros servidores que solicitaban conexión con el servidor de la Institución, esto demuestra que la integración de estos filtros se encuentra en correcto funcionamiento y que está contribuyendo efectivamente con el control de *spam* y con el mejoramiento del sistema.

- **Prueba 2: prueba con 526 mensajes *spam***

Esta prueba fue realizada enviando 526 mensajes *spam* que llegaron al servidor de correo de la Institución entre el mes de Julio y el mes de Octubre de 2012 y que no fueron reconocidos por la plataforma **Fortigate**, con el fin de detectar cuántos de estos son reconocidos por este filtro, como se muestra en la Figura 3.2.

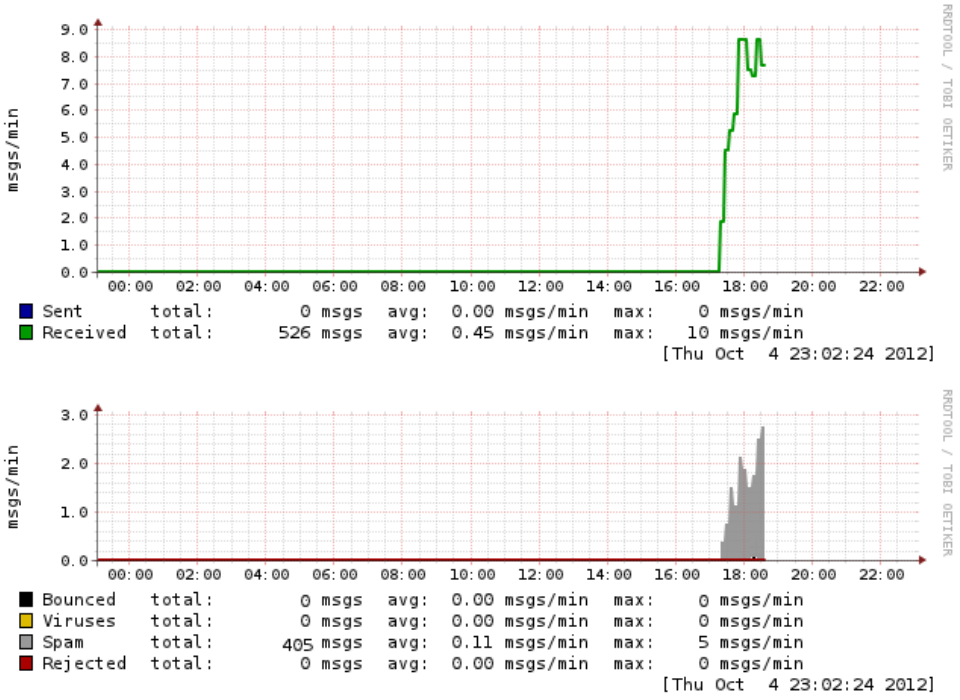


Figura 3.2 Prueba de Spamassassin con 526 mensajes *spam*

La línea verde indica los 526 mensajes recibidos por este filtro. La línea gris representa los mensajes que fueron reconocidos como *spam*, para este caso fueron detectados 405 mensajes, esto quiere decir que la herramienta tiene una efectividad del 76.99% en el rechazo de *spam*.

Como se evidencia en las Figura 3.1 y 3.2, con estas pruebas se demuestra que existe una mejora en el servicio de correo de la Universidad del Cauca, ya que permite disminuir la cantidad de *spam* que llegaría al buzón de cada usuario de la Institución, adicionando una herramienta que pueda controlar el correo no deseado que se le pasa a la herramienta **Fortigate** y que además realice control sobre el correo saliente y el correo interno de la Institución.

3.2.2 Pruebas y resultados con Policyd

Para observar el comportamiento de este filtro de acuerdo a las configuraciones previas, se llevaron a cabo pruebas de envío de correo.

- **Prueba 1: Prueba de envío de mensaje a varios usuarios**

La primera prueba con **Policyd,** fue realizada enviando un mensaje a múltiples usuarios, para este caso se definió un límite de 50 usuarios, esta cantidad se tomó promediando la información entregada por el archivo de registro del servicio de correo acerca de la cantidad de usuarios por mensaje que se envían diariamente. La cantidad de usuarios a

los que fue enviado el mensaje, excede el número de usuarios permitidos por mensaje de acuerdo a la configuración realizada. El envío del mensaje se observa en la Figura 3.3.

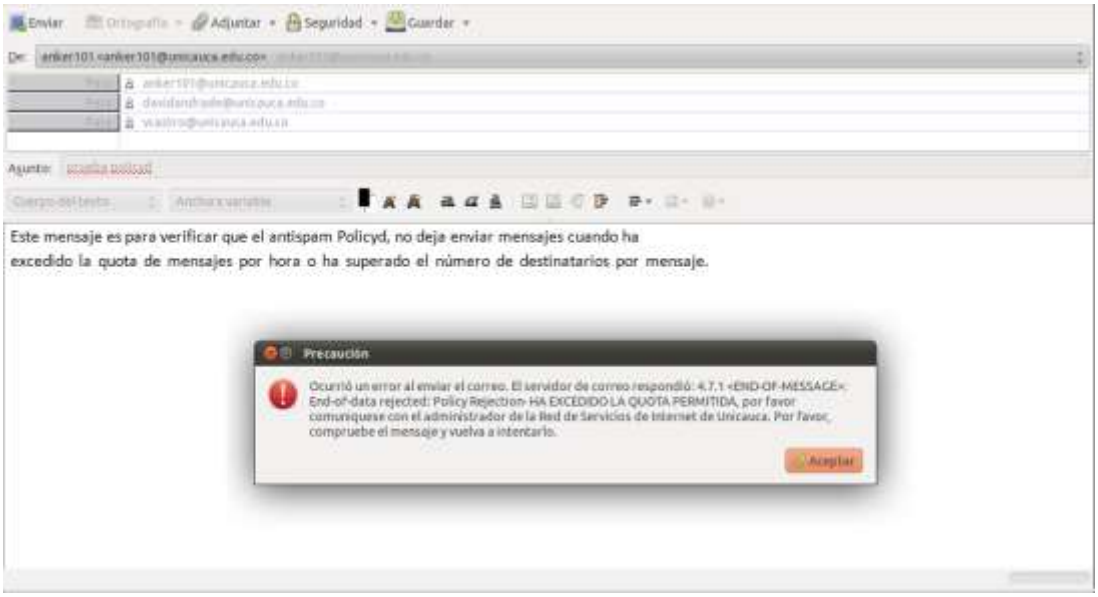


Figura 3.3 Número de usuarios excedido

Como el mensaje fue enviado a un número de destinatarios mayor al permitido, el sistema responde con un mensaje de precaución de que la *quota*[37] ha sido excedida.

- **Prueba 2: Prueba de envío de varios mensajes por usuario**

Esta prueba es para verificar que si un usuario envía un número de mensajes mayor al permitido de acuerdo a las configuraciones realizadas, éste no se puede enviar. Para esta prueba se configuraron 23 mensajes por hora, esta cantidad se tomó promediando la información entregada por el archivo de registro del servicio de correo acerca de la mayor cantidad de mensajes por hora que se envían diariamente. Esto se observa en la Figura 3.4.

[37] Quota: Restricciones impuestas a los usuarios al momento de enviar o recibir correos.

Figura 3.4 Número de mensajes excedido

El número de mensajes enviados por un mismo usuario en un periodo de tiempo es mayor al permitido, por esta razón no se autoriza el envío del mensaje mostrando un anuncio de precaución.

- **Prueba 3: Tamaño del mensaje excedido**

Para esta prueba, se realizó el envío de un mensaje que sobrepasa el tamaño permitido de acuerdo a las configuraciones realizadas. La Figura 3.5 muestra el intento de envío del mensaje.

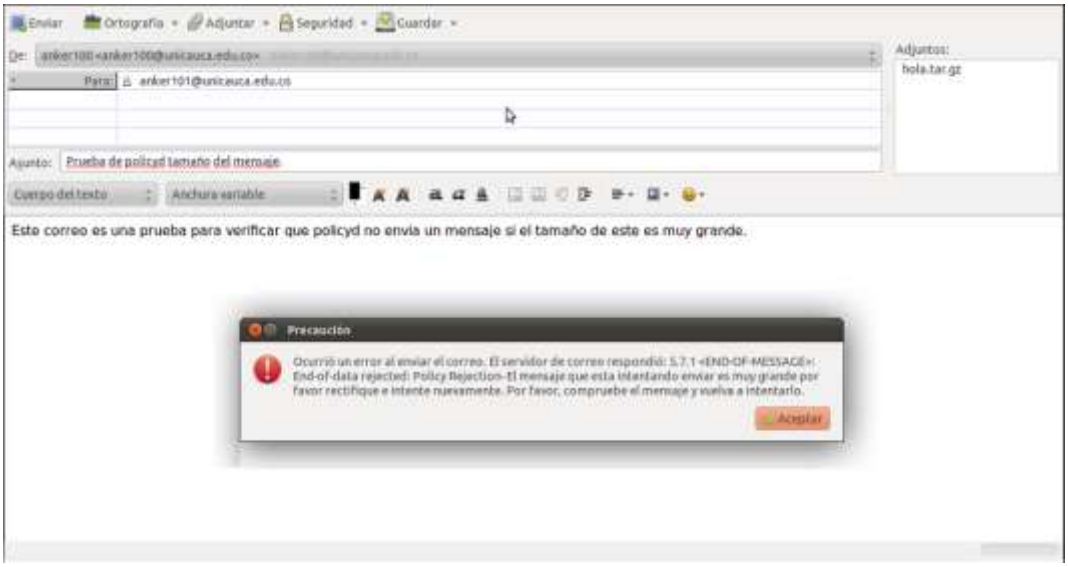


Figura 3.5 Tamaño del mensaje excedido

Al intentar enviar el mensaje aparece un mensaje de precaución que anuncia que el mensaje que se quiere envía es muy grande y excede el tamaño permitido.

De acuerdo a los resultados y a las evidencias mostradas en esta sección, se puede decir, que el servicio de correo de la Universidad del Cauca ahora cuenta con un sistema que permite reducir la cantidad de mensajes *spam* que llegan al correo de la Institución y que deja pasar la plataforma **Fortigate,** además, ahora si se cuenta con un sistema que analice el correo saliente y el correo interno de la Universidad por medio de herramientas de software libre como **Policyd** y **Spamassassin**.

3.3 PRUEBAS Y RESULTADOS DE AUTENTICACIÓN Y CIFRADO

Para la verificación de las configuraciones de autenticación y cifrado se realizaron una serie de pruebas las cuales evidencian que este requerimiento esta funcionando correctamente, se enviaron mensajes a través de telnet y por medio de clientes de correo. La configuración de autenticación se efectuó en un servidor de correo que es una réplica exacta del servidor de correo de la Universidad del Cauca, se llevaron a cabo las pruebas en este servidor y luego de verificar que todo se encontraba en correcto funcionamiento, se implantaron estas configuraciones en el servidor de producción de la Institución.

3.3.1 Pruebas y resultados en servidor réplica

Antes de poner en producción las configuraciones, éstas se realizaron en el servidor réplica. Para validar los resultados de las configuraciones de autenticación y cifrado en este servidor se realizaron una serie de pruebas.

3.3.1.1 Prueba de la configuración de autenticación mediante telnet

Esta prueba de autenticación consiste en realizar el envío de un mensaje de correo para verificar que el sistema solicita el proceso de autenticación antes de enviar el mensaje. Para realizar la prueba de autenticación se hace un telnet al Puerto 25:

```
telnet localhost 25
```

A continuación en la Figura 3.6 se observa como se hace esta prueba de autenticación:

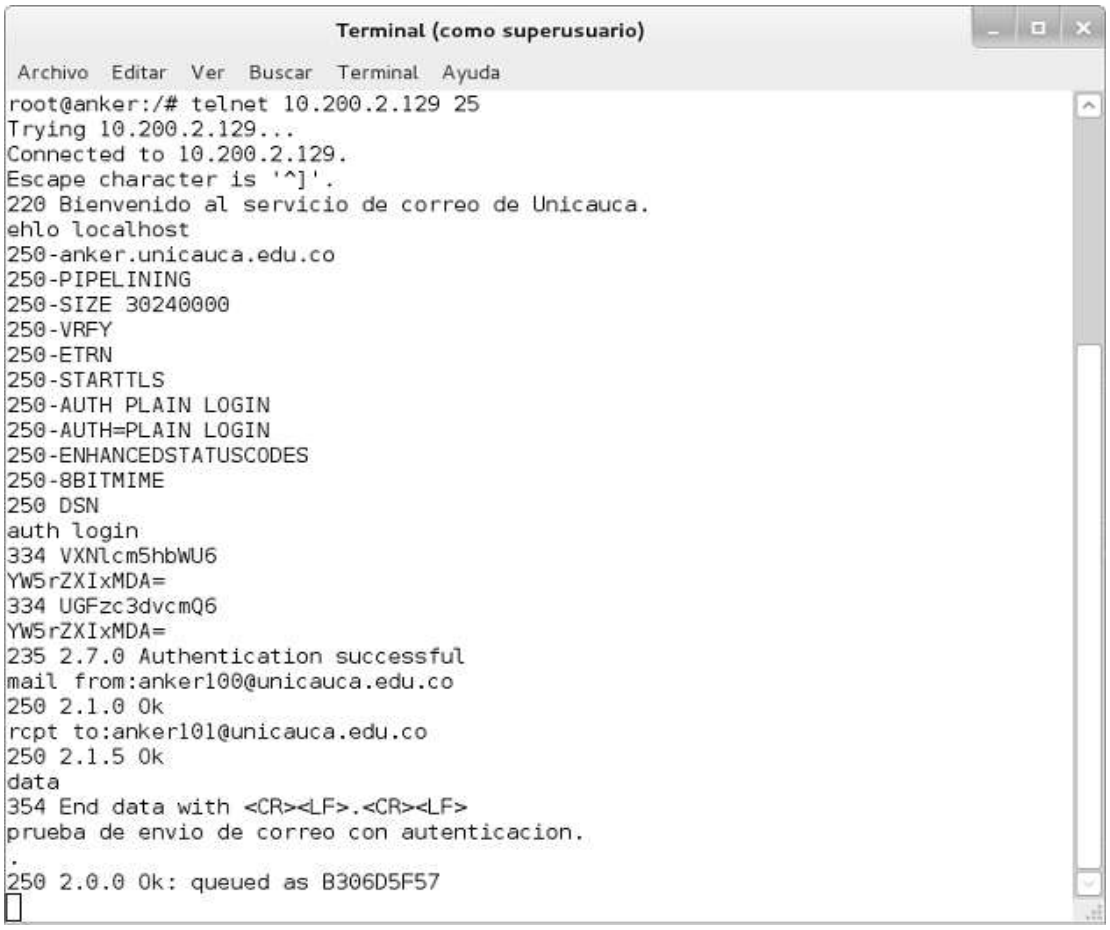


Figura 3.6 Verificación de autenticación en servidor de prueba

Se ingresa el comando `ehlo localhost` para observar las funciones que cumple el servidor:

```
ehlo localhost
```

La respuesta que da el servidor permite ver que tiene activada la autenticación y el cifrado con TLS. Luego de esto, se prueba la autenticación con `auth login` y se realiza el envío de un mensaje.

La línea `YW5rZXIxMDA=` es el nombre de usuario codificado, para este caso el nombre de usuario y la contraseña son iguales (anker100). Se observa que la autenticación es exitosa y después se envía el mensaje satisfactoriamente.

La codificación del nombre de usuario y la contraseña se realiza mediante el método de codificación base64, por medio del siguiente comando:

```
perl -MMIME::Base64 -e 'print encode_base64("contraseña a cifrar")'
```

En el espacio que dice "**contraseña a cifrar**" se pone la palabra o clave que se quiere codificar, para este caso es "anker100".

Esta prueba de envío de correo a través de este servidor se realizó utilizando dos cuentas de usuario creadas dentro de este sistema de pruebas, las cuentas son anker100@unicauca.edu.co y anker101@unicauca.edu.co. El servidor de prueba tiene como IP la dirección 10.200.2.129.

3.3.1.2 Pruebas de autenticación y cifrado con clientes de correo

Se realizaron pruebas de autenticación y cifrado, enviando mensajes de correo por medio de los clientes de correo y se utilizó el analizador de protocolos **Wireshark**[38] para verificar el tráfico SMTP y comprobar si el proceso de cifrado de la información se encontraba funcionando correctamente.

El interés principal en el desarrollo de esta etapa del proyecto, es el manejo de la comunicación cifrada por medio de TLS y la autenticación con SASL, por lo tanto para los dos primeros clientes de correo, se realizaron pruebas para que el canal de comunicación quedara cifrado mediante TLS, aunque también se tuvo en cuenta el texto plano para observar el comportamiento de la comunicación. Para los otros dos clientes se realizaron las pruebas solo con comunicación cifrada con TLS para no repetir el mismo procedimiento, ya que al hacer la interpretación de la comunicación con el analizador de protocolos se va a observar lo mismo que en las pruebas con los dos primeros clientes.
Las pruebas de envío de correo a través de este servidor se realizaron con las cuentas de usuario anker100@unicauca.edu.co y anker101@unicauca.edu.co, también se utilizaron cuentas propias de la Universidad del Cauca como vcastro@unicauca.edu.co y davidandrade@unicauca.edu.co. Se realizó la instalación de diferentes clientes de correo, entre ellos **Outlook**, **Thunderbird**, **Zimbra**[39] y **Eudora** para verificar la compatibilidad con el sistema de autenticación del servidor.

En el Anexo H se encuentran detalladas las instalaciones de los clientes de correo utilizados, configurados con la información del servidor y los usuarios de prueba.

Pruebas de envío de mensajes con cliente Outlook

A continuación se muestran algunas pruebas de envío de mensajes que se realizaron con el cliente **Outlook,** para verificar las configuraciones de autenticación y cifrado realizadas. La configuración del cliente de correo se modifica para cada una de las pruebas.

[38] http://www.wireshark.org/
[39] http://www.zimbra.com/

- **Prueba 1: Texto plano**

En esta prueba se muestra el envío de un mensaje de correo con **Outlook** como se ve en la Figura 3.7. Para esta prueba se solicita autenticación, pero se encuentra desactivado el cifrado con TLS en los archivos de configuración del servidor **Postfix** y en la configuración de **Outlook** no se trabaja con conexión cifrada, por lo tanto la transmisión del correo se realiza en texto plano.

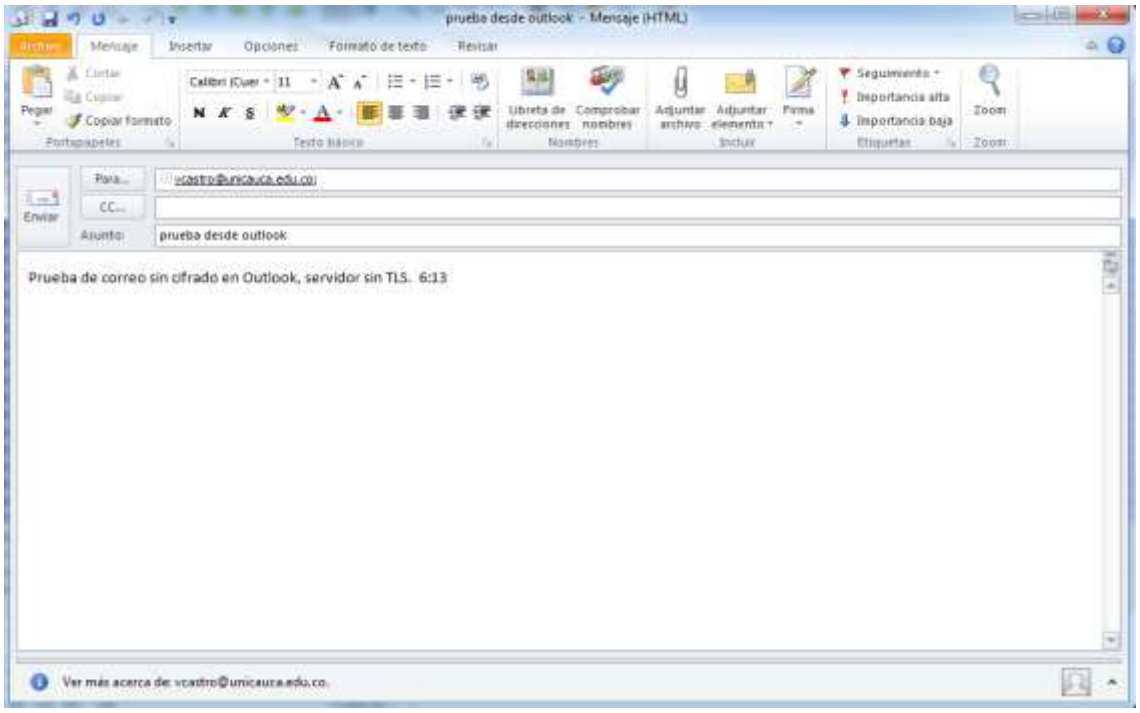


Figura 3.7 Envío de mensajes - texto plano

La Figura 3.8 es una captura de imagen realizada con **Wireshark** de la conexión y de los datos transmitidos entre el cliente con dirección IP 192.168.120.35 y el servidor 10.200.2.129. En las líneas negras se observa la comunicación desde el cliente hacia el servidor y las líneas color azul claro representan la información enviada desde el servidor hacia el cliente. Luego de iniciar la comunicación se ve claramente el proceso de solicitud de autenticación por parte del servidor y el momento en que esta es realizada por el cliente. Se puede observar el remitente del mensaje anker100@unicauca.edu.co y el destinatario vcastro@unicauca.edu.co, después de esto es enviada la información del mensaje y por último se observa el final de la conexión.

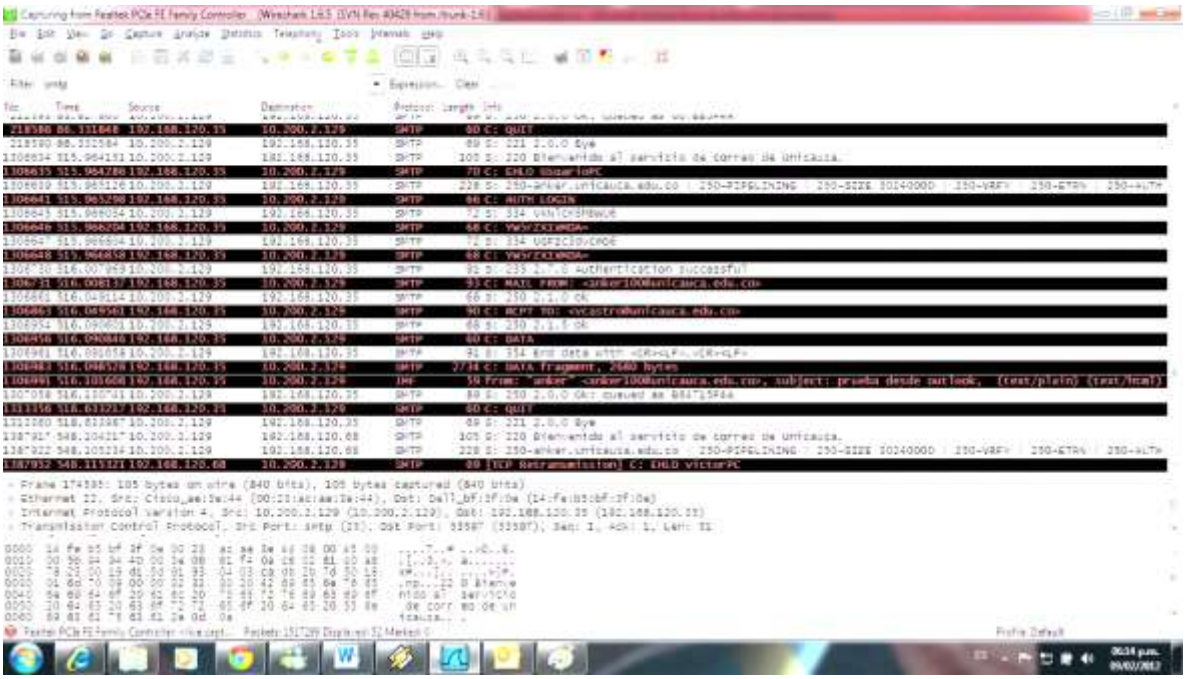


Figura 3.8 Comunicación SMTP con Wireshark - texto plano

Para verificar que el mensaje enviado ha sido recibido satisfactoriamente, se ingresa a la cuenta de correo del destinatario que es un usuario de la Universidad del Cauca. Se puede ver en la Figura 3.9 que el mensaje llegó a la bandeja de entrada.

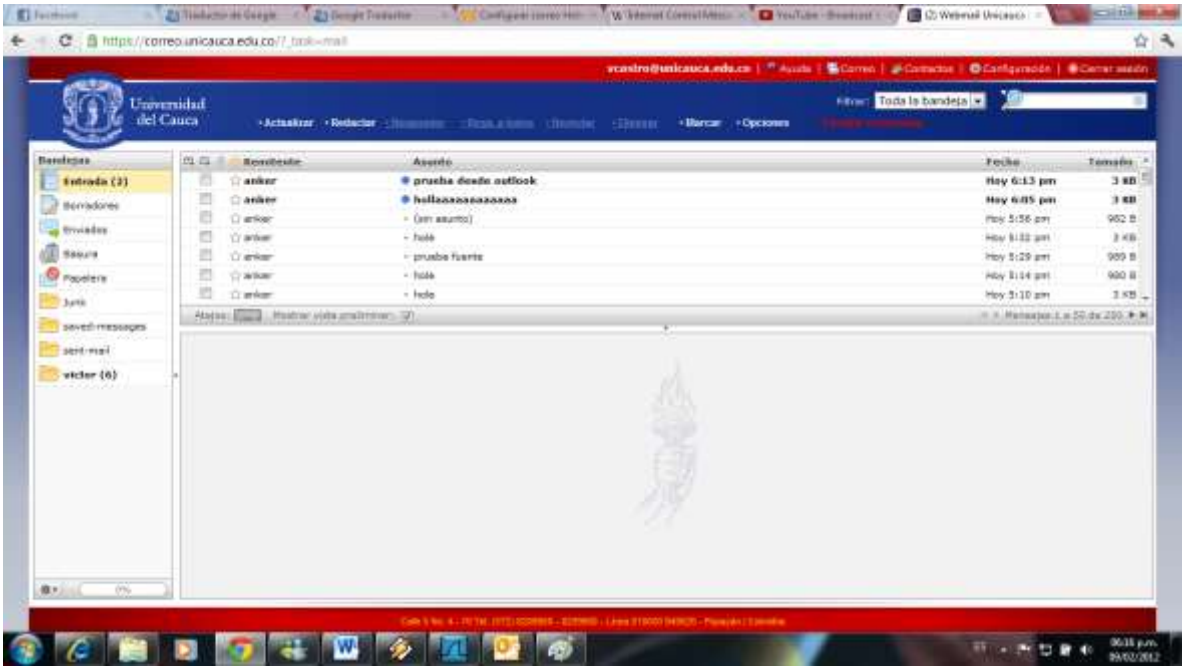


Figura 3.9 Cuenta de usuario de Unicauca - texto plano

Se ingresa al mensaje, para verificar los datos recibidos y que el remitente y la hora coincidan con la información desde donde fue enviado el mensaje, Figura 3.10.

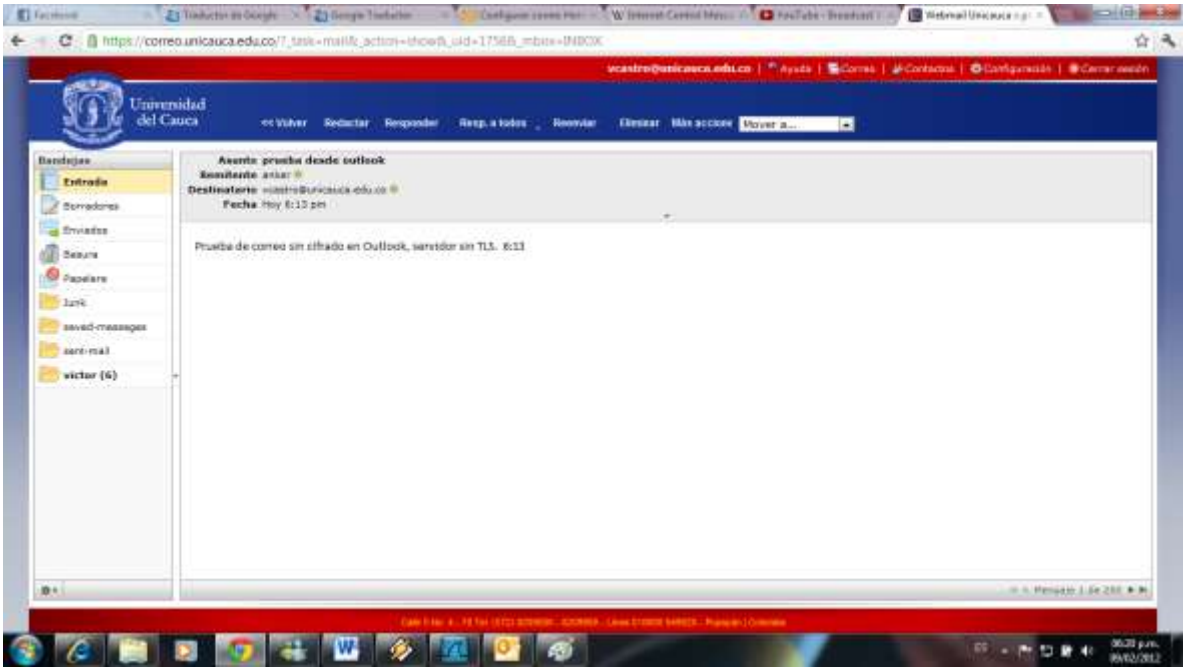


Figura 3.10 Mensaje recibido - texto plano

- **Prueba 2: Cifrado con TLS**

La configuración tenida en cuenta para esta prueba, tiene activada en el servidor la transmisión cifrada mediante TLS y en la configuración de **Outlook** también tiene como tipo de conexión cifrada, TLS. Se encuentra configurado para enviar y recibir mensajes solamente con cifrado y no en texto plano. El envío del mensaje se observa a continuación en la Figura 3.11.

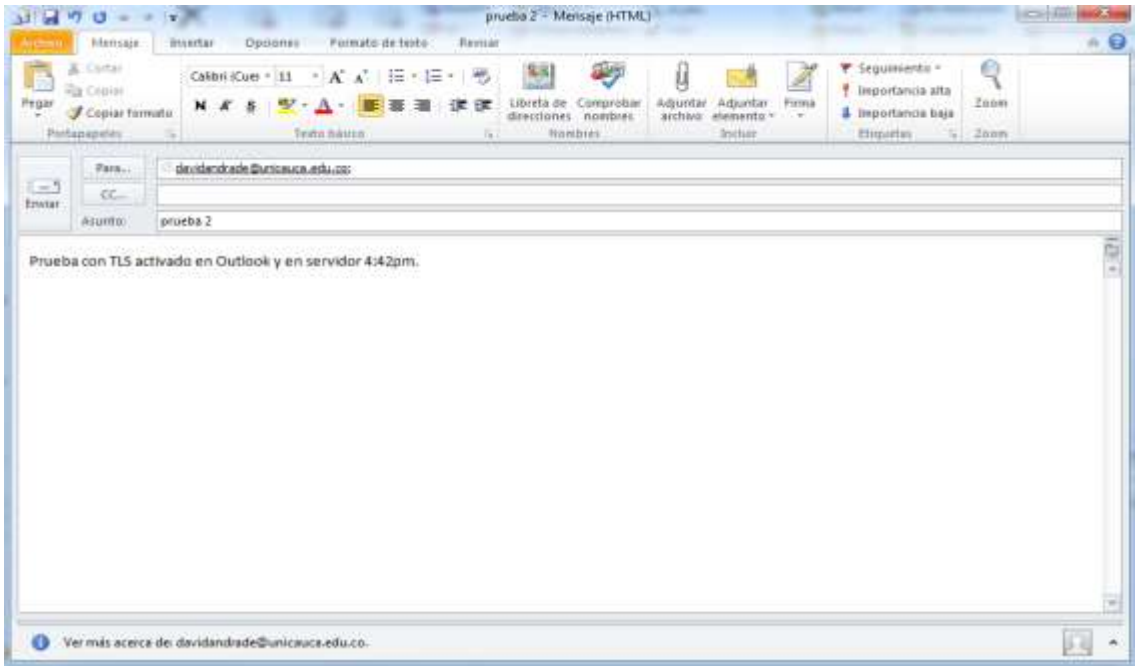


Figura 3.11 Envío de correo - cifrado con TLS

Por medio de **Wireshark**, en la Figura 3.12 de la conexión SMTP, se observa que cuando se utiliza TLS solamente permite ver el mensaje EHLO entre el cliente y el servidor, no muestra nada de la etapa de autenticación ni del mensaje que fue transmitido.

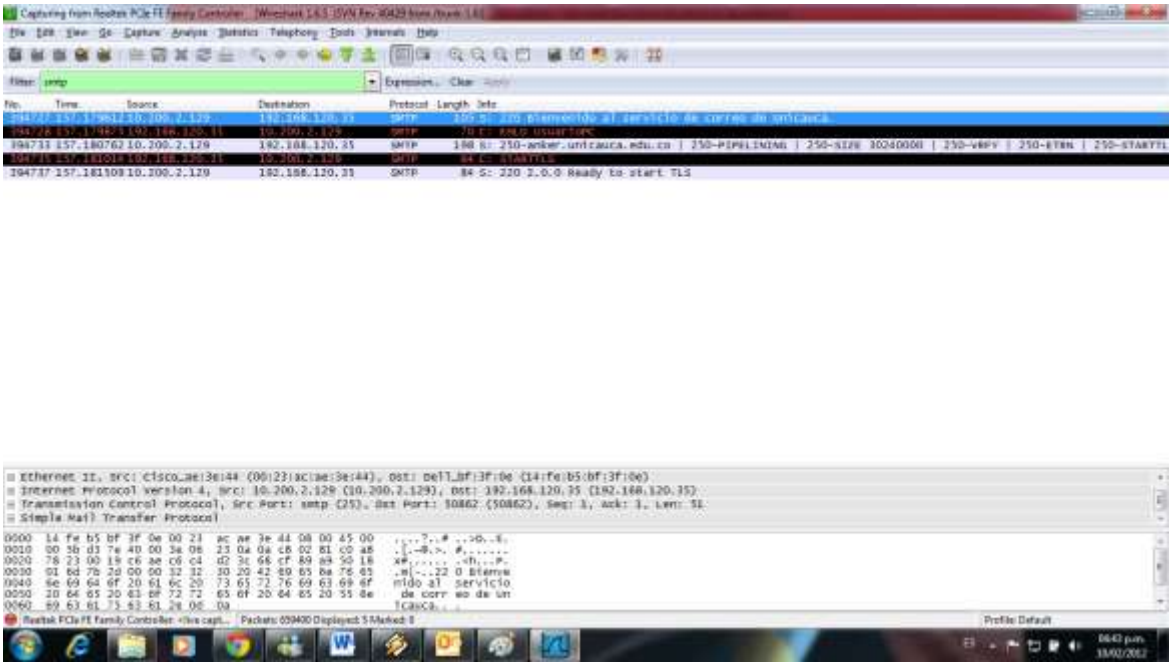


Figura 3.12 Conexión SMTP con Wireshark - cifrado con TLS

En la Figura 3.13 se muestra la conexión TLS entre el cliente y el servidor.

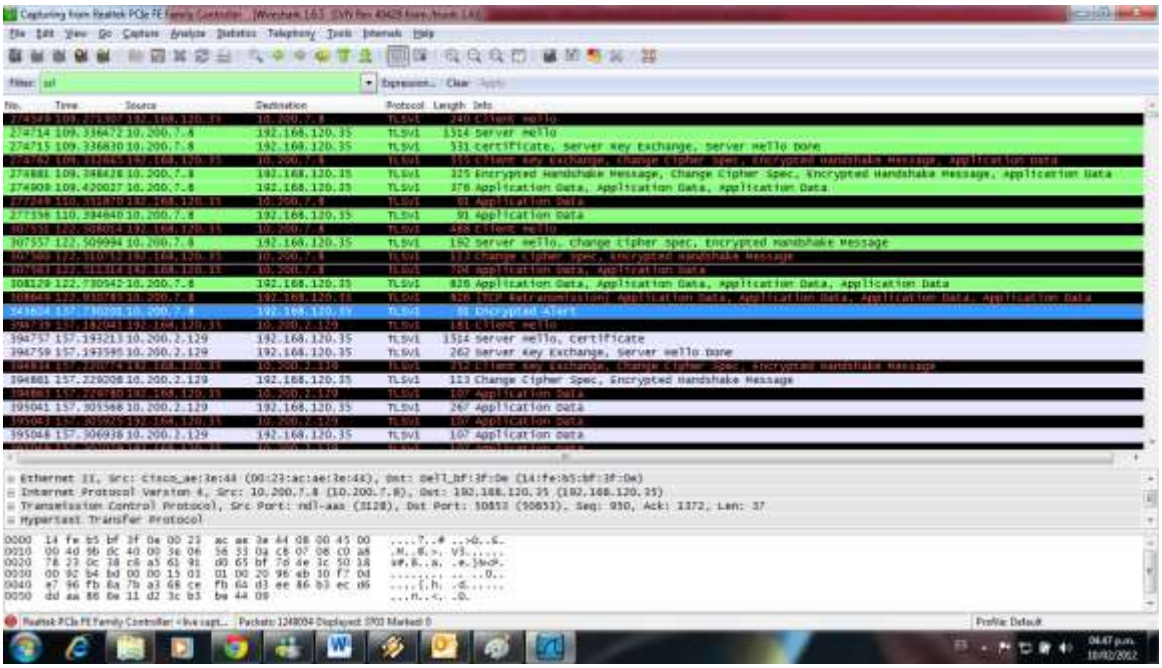


Figura 3.13 Comunicación TLS - cifrado con TLS

En la Figura 3.14 se verifica que el mensaje enviado llego a su destino, se accede a la cuenta de usuario del destinatario.

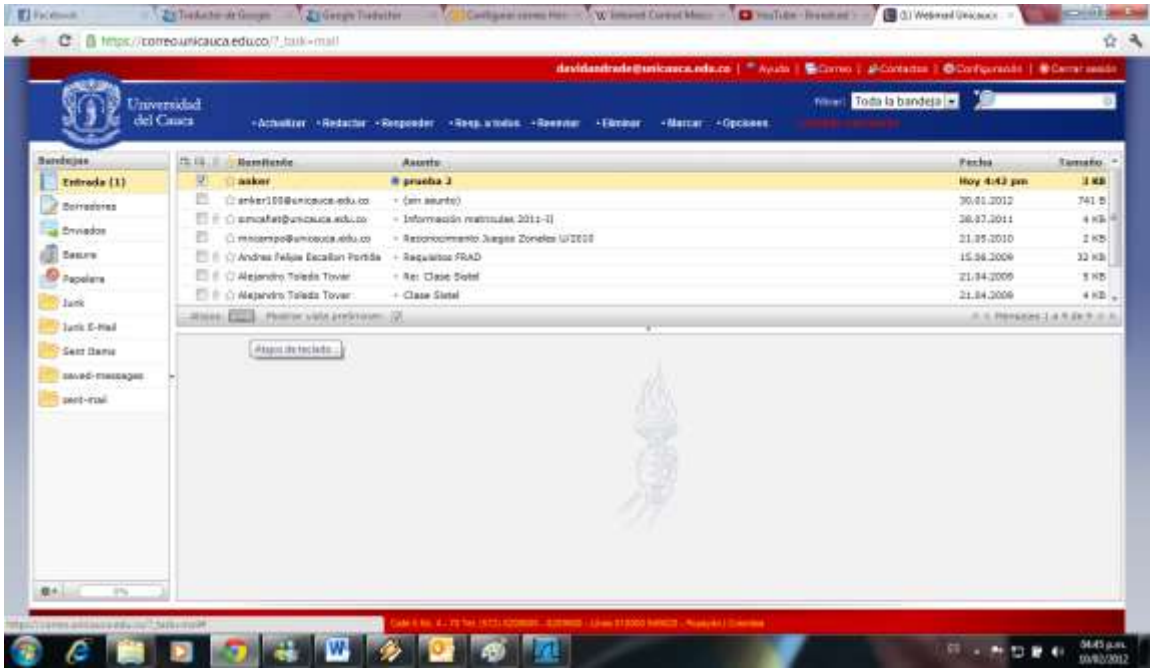


Figura 3.14 Cuenta de usuario - cifrado con TLS

Se ingresa al mensaje para verificar la información, Figura 3.15.

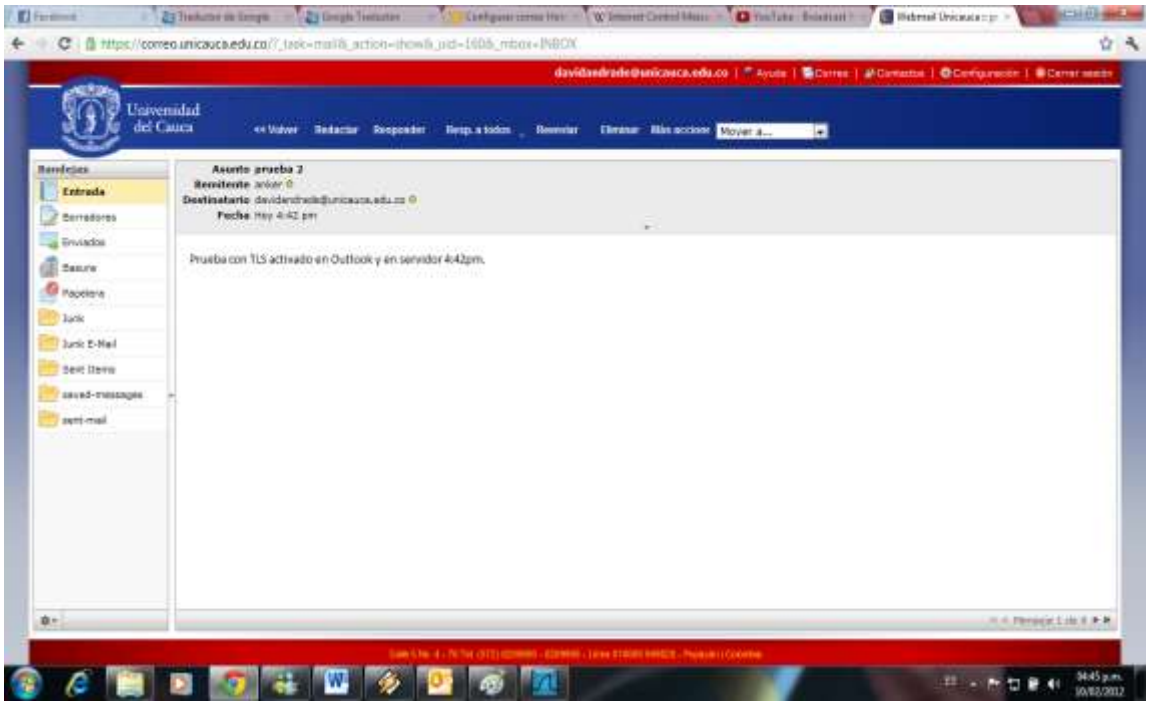


Figura 3.15 Mensaje recibido - cifrado con TLS

- **Prueba 3: Cliente con TLS – Servidor en texto plano y TLS**

Para la realización de esta prueba se configuró **Outlook** con conexión cifrada TLS. Se puede llevar a cabo comunicación cifrada y también en texto plano de acuerdo a la configuración en el servidor. El envío del mensaje se observa en la Figura 3.16.

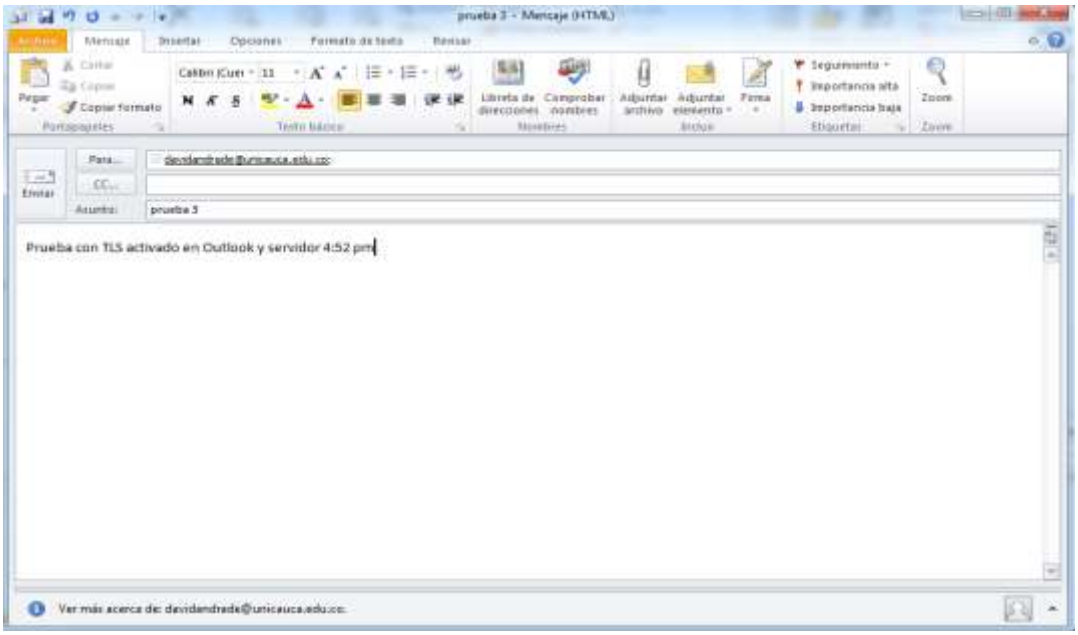


Figura 3.16 Envío de mensaje - cliente con TLS - servidor en texto plano y TLS

La comunicación SMTP se puede observar a continuación en la Figura 3.17:

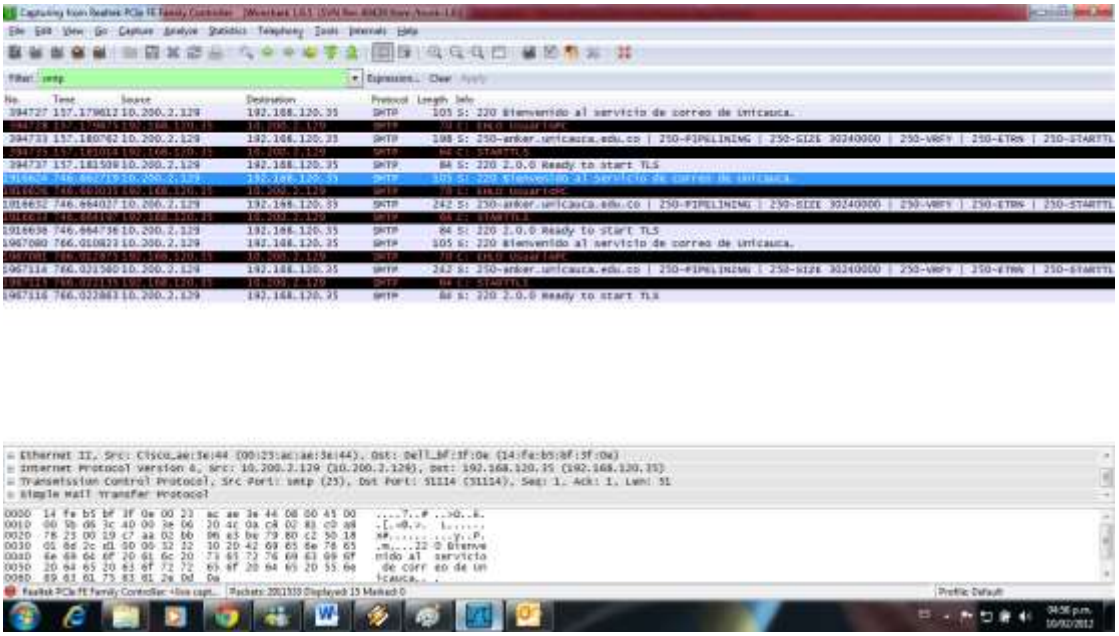


Figura 3.17 Comunicación SMTP - cliente con TLS - servidor en texto plano y TLS

En la Figura 3.18 se muestra la comunicación TLS:

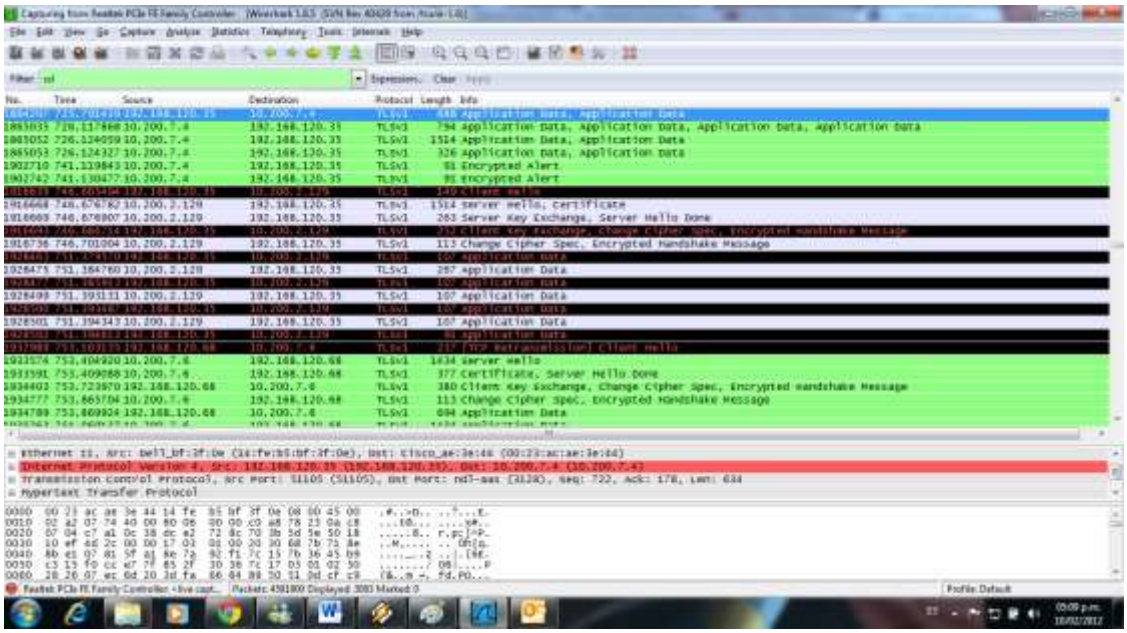


Figura 3.18 Comunicación TLS - cliente con TLS - servidor en texto plano y TLS

En la Figura 3.19 se ingresa a la cuenta de correo del usuario de destino para verificar la recepción del mensaje.

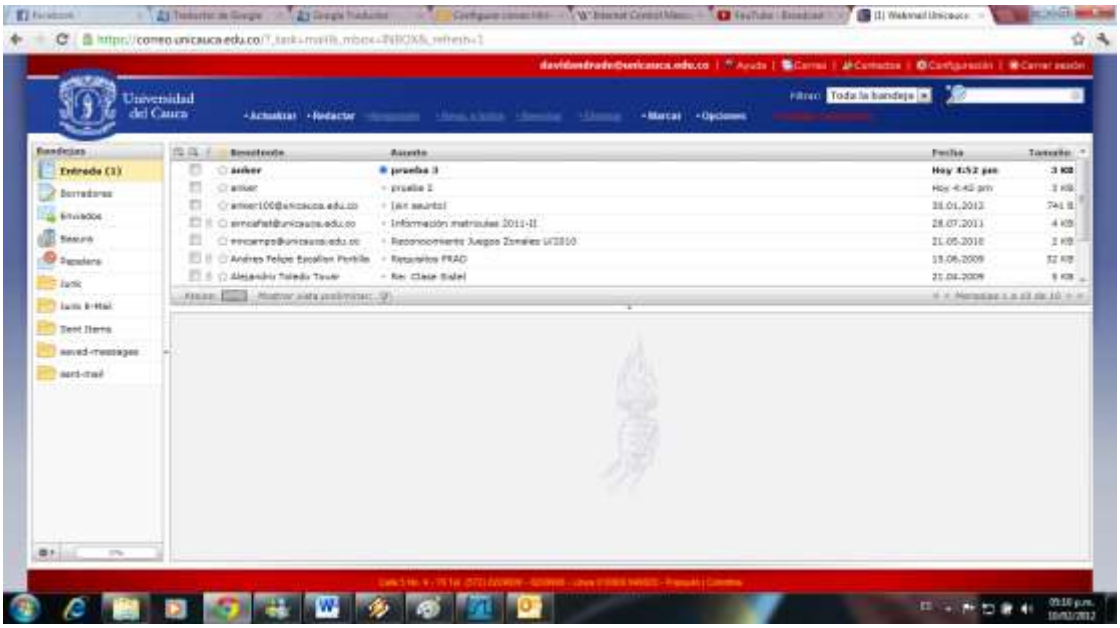


Figura 3.19 Mensajes de usuario - Cliente con TLS - servidor en texto plano y TLS

La Figura 3.20 permite ver el mensaje para ratificar la información:

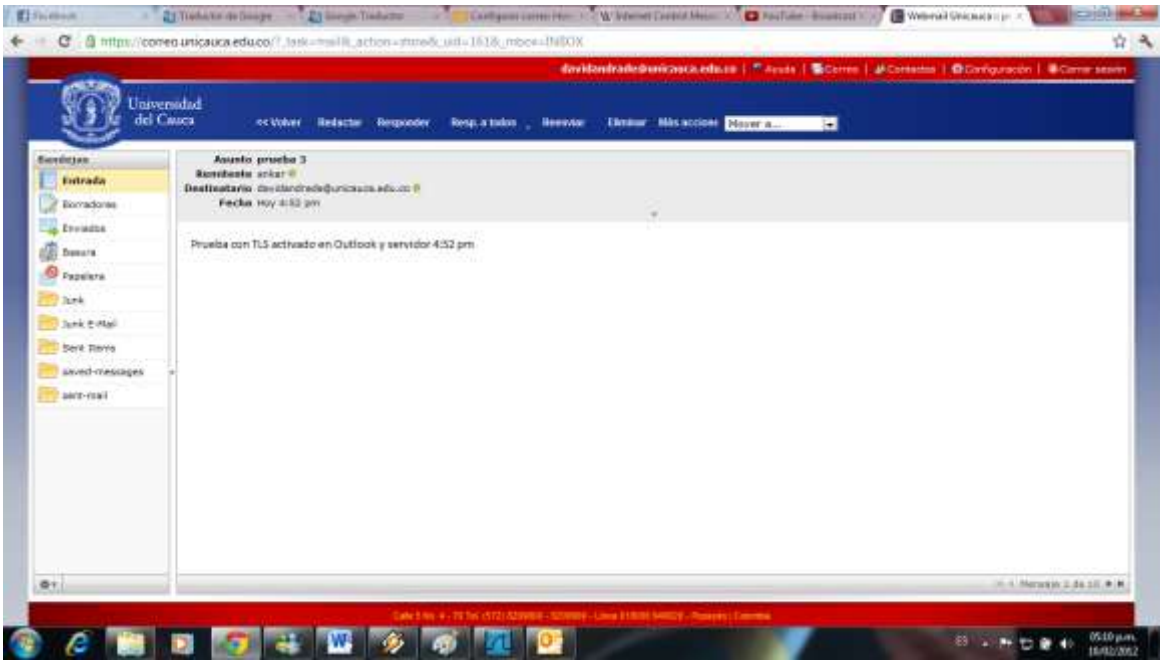


Figura 3.20 Mensaje recibido - cliente con TLS - servidor en texto plano y TLS

- **Prueba 4: Cliente sin TLS – servidor con TLS**

En la configuración del servidor **Postfix**, se encuentra habilitada la conexión cifrada mediante TLS, sin la posibilidad de realizar comunicación en texto plano. La configuración de **Outlook** esta configurada de tal manera que no se utiliza ningún tipo de conexión cifrada.

Al realizar la prueba de conexión de acuerdo a la configuración de la cuenta, se evidencia un error debido a que solo se pueden enviar y recibir mensajes con TLS y en la configuración del cliente **Outlook** no se seleccionó ningún tipo de cifrado. La Figura 3.21 permite ver el error en la conexión.

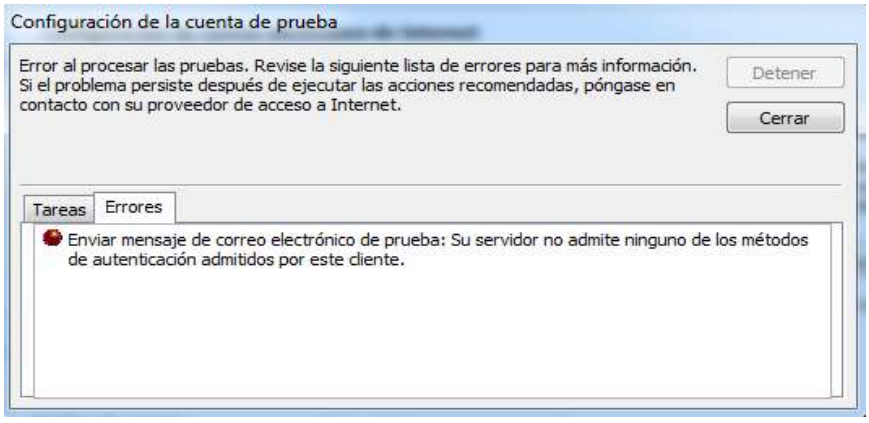
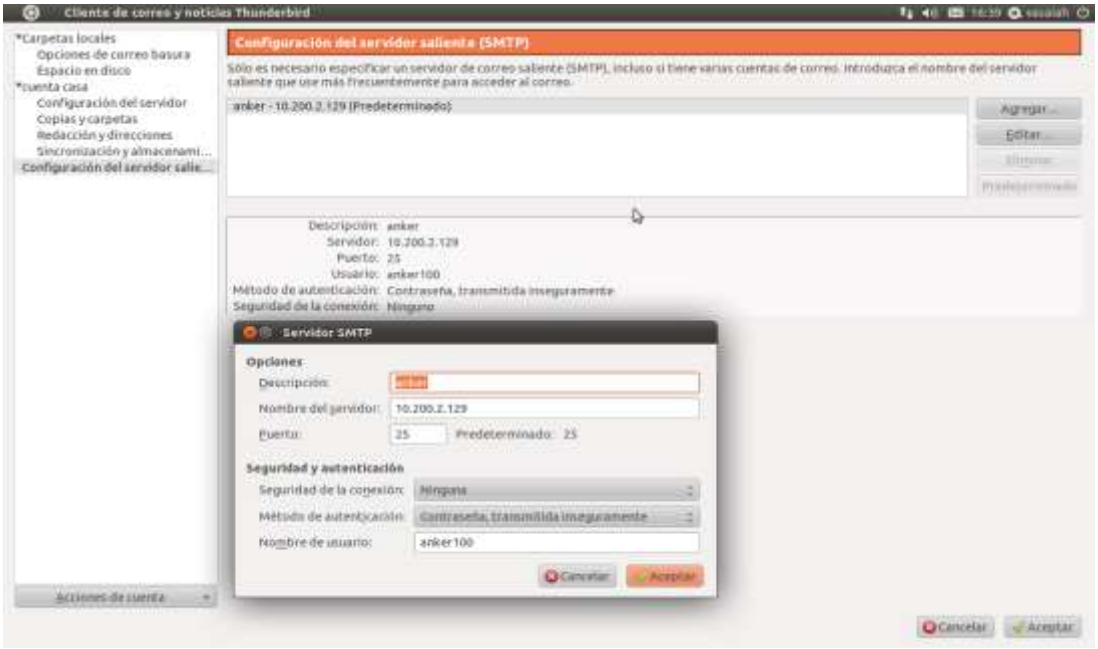


Figura 3.21 Error de conexión - cliente sin TLS - servidor con TLS

Prueba de envío de mensajes con cliente Thunderbird

- **Prueba 1: Autenticación sin soporte TLS**

En esta prueba se realiza el envío de un mensaje con el cliente de correo configurado sin soporte TLS. En la Figura 3.22 se muestra la configuración del cliente de correo **Thunderbird** para que trabaje en un sistema autenticado sin una conexión cifrada.



.

Figura 3.22 Configuración de Thunderbird sin TLS

A continuación se muestra el correo a enviar desde el cliente **Thunderbird** a un usuario de Unicauca. Este mensaje lleva en el asunto el nombre del cliente de correo que lo envía y en el cuerpo del mensaje la fecha y hora de envió. También se puede observar que antes de enviar el mensaje se pide autenticación de usuario para verificar validez del remitente.

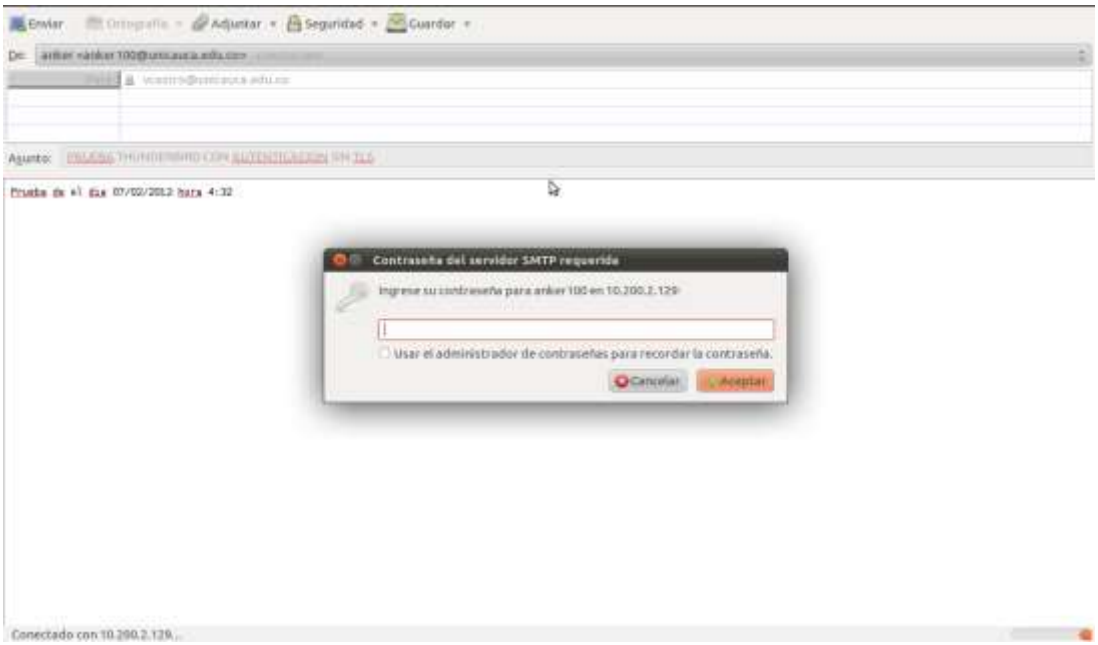


Figura 3.23 Mensaje del cliente Thunderbird con solicitud de autenticación

En la Figura 3.24 se muestra la recepción del correo en la cuenta del usuario de Unicauca.

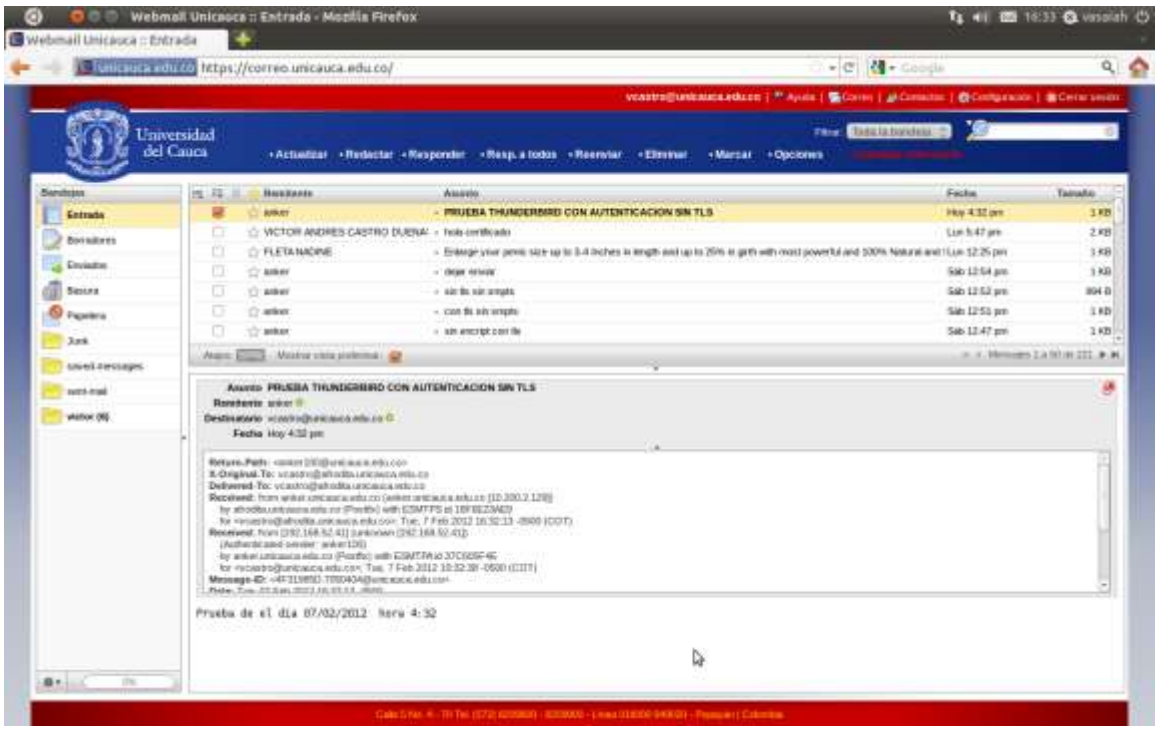


Figura 3.24 Recepción del mensaje Unicauca

La Figura 3.25 muestra a través de **Wireshark** que la transmisión del mensaje se hace en texto plano, lo cual no es conveniente para un sistema de correo ya que los datos transmitidos pueden ser capturados o vistos por sistemas ajenos al del correo electrónico de Unicauca.

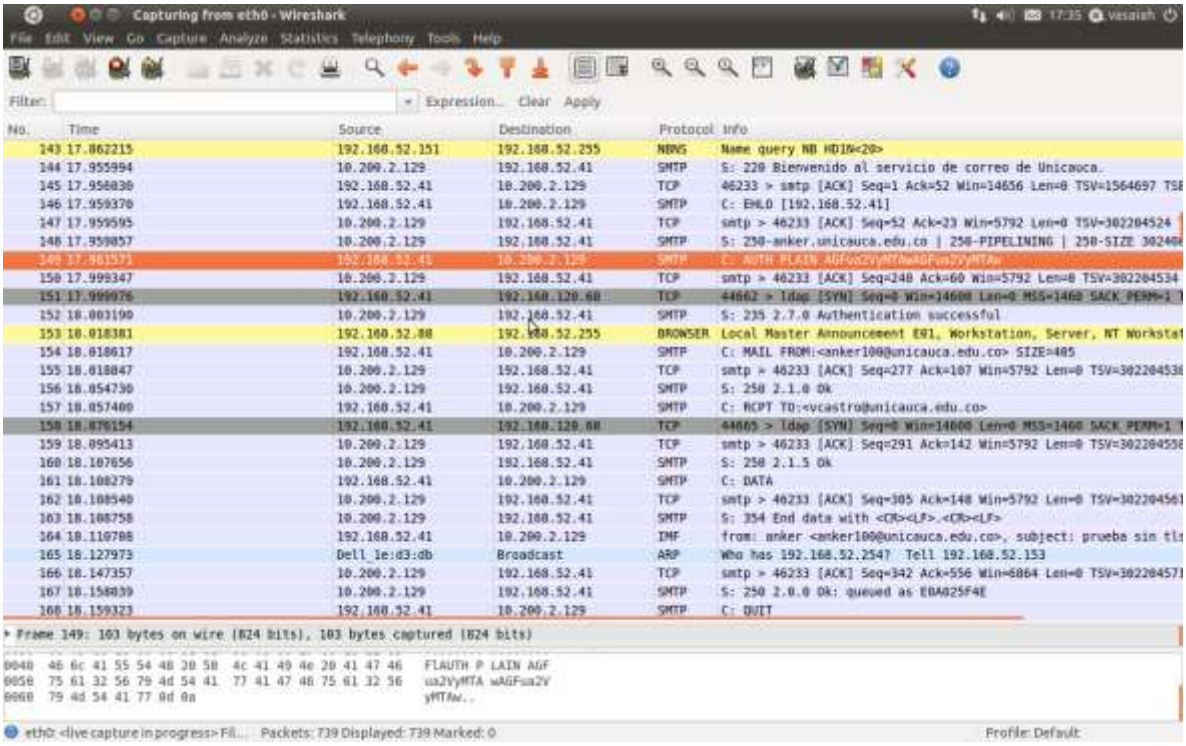


Figura 3.25 Captura de datos con Wireshark sin TLS

- **Prueba 2: Autenticación con soporte TLS**

Para esta prueba se activa en **Thunderbird** el soporte de transmisión cifrada. En la Figura 3.26, se muestra la configuración para realizar la activación.

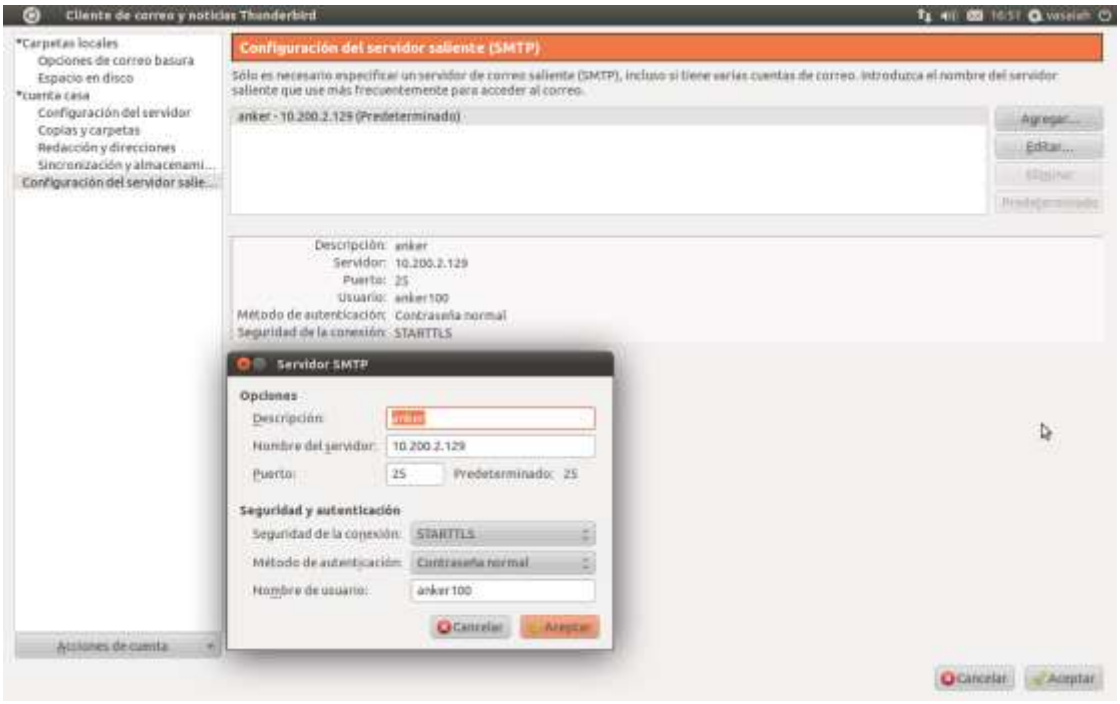


Figura 3.26 Configuración de Thunderbird con TLS

La Figura 3.27 que se muestra a continuación permite ver la transmisión del mensaje y la verificación del usuario por parte del cliente **Thunderbird**.

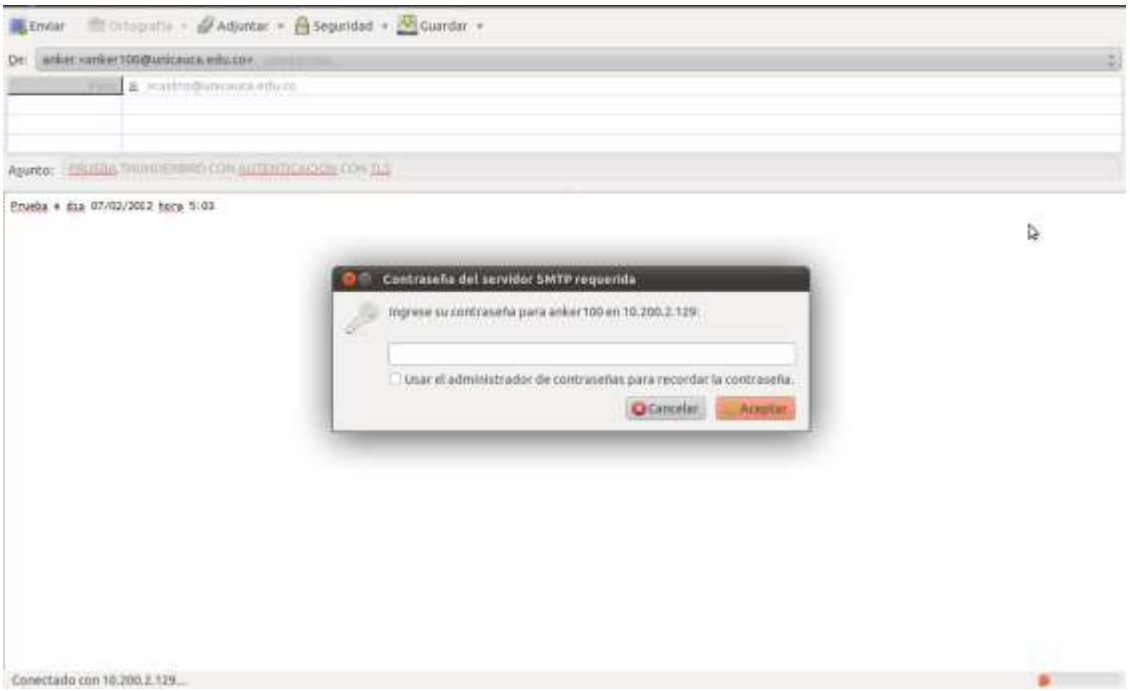


Figura 3.27 Mensaje del cliente Thunderbird

La Figura 3.28 muestra que el correo transmitido por TLS llega al usuario correspondiente.

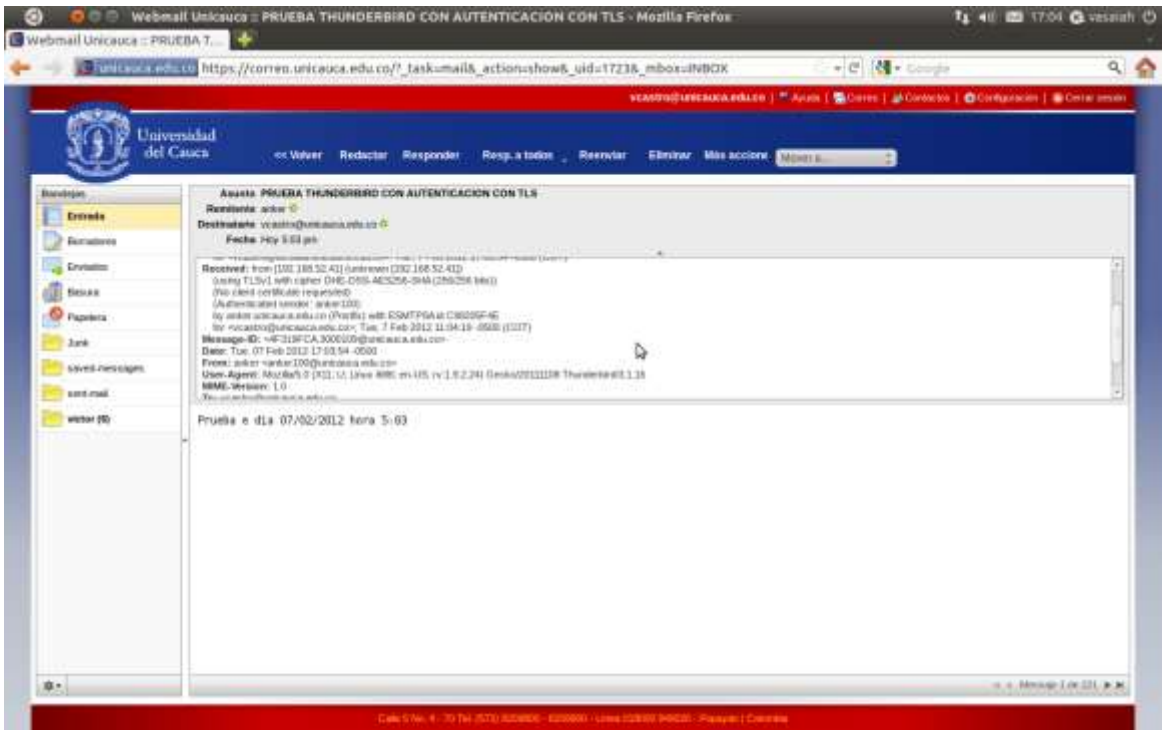


Figura 3.28 Recepción del mensaje Unicauca

La Figura 3.29 muestra que **Wireshark** captura los datos de la transmisión de correo, pero esta conexión se encuentra cifrada por lo tanto no es mucho lo que se puede observar acerca de esta transmisión.

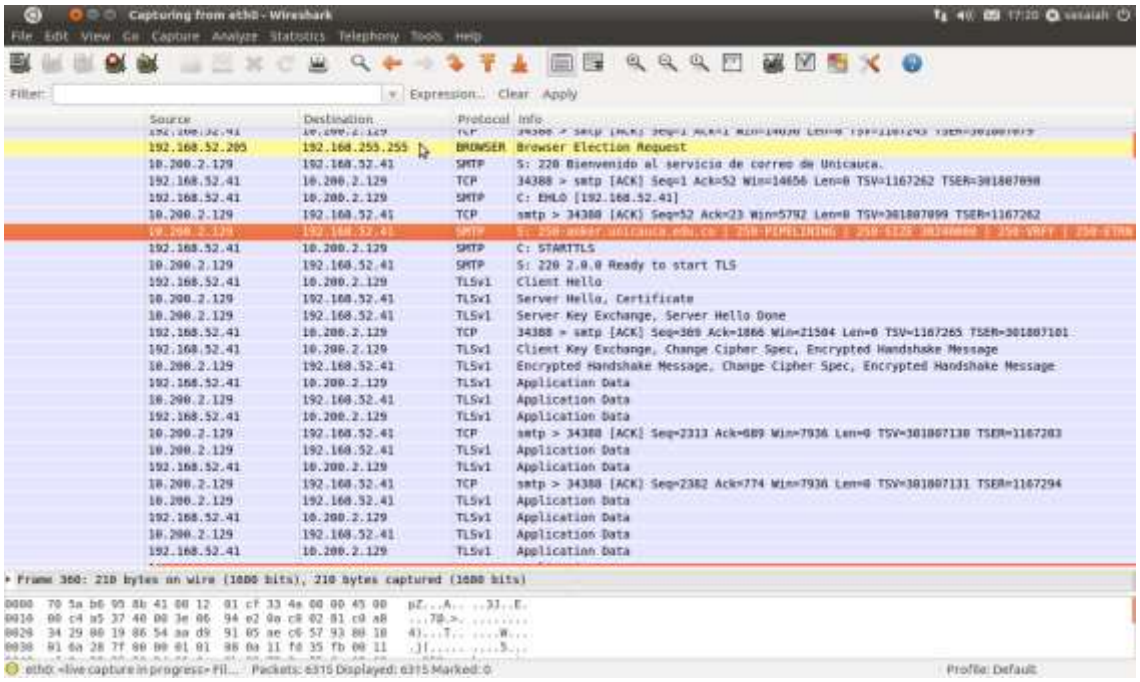


Figura 3.29 Captura de datos con Wireshark con TLS

Prueba de envío de mensaje con cliente Zimbra Desktop

La prueba de envío de correo se realizó con TLS activado en el servidor y no activado en el cliente de correo **Zimbra**. El envío de correo se observa en la Figura 3.30.

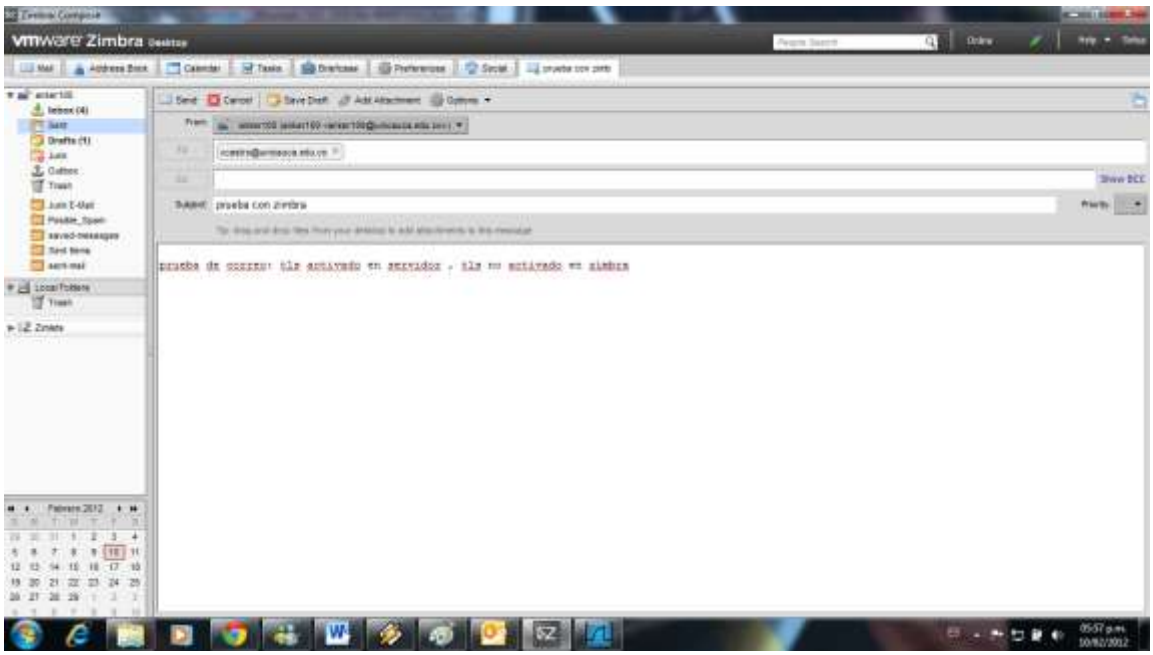


Figura 3.30 Envío de correo con Zimbra Desktop

La Figura 3.31 permite observar el tráfico SMTP, el camino se encuentra cifrado con TLS.

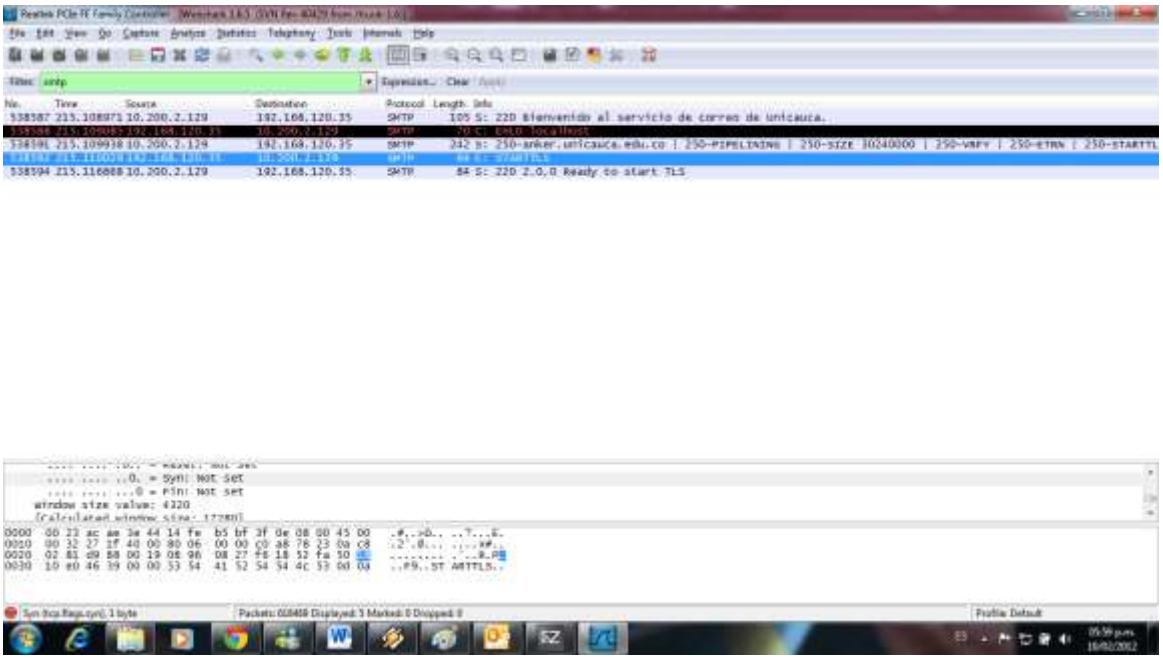


Figura 3.31 Comunicación SMTP - Zimbra

A continuación en la Figura 3.32 se puede ver la conexión TLS entre cliente y servidor:

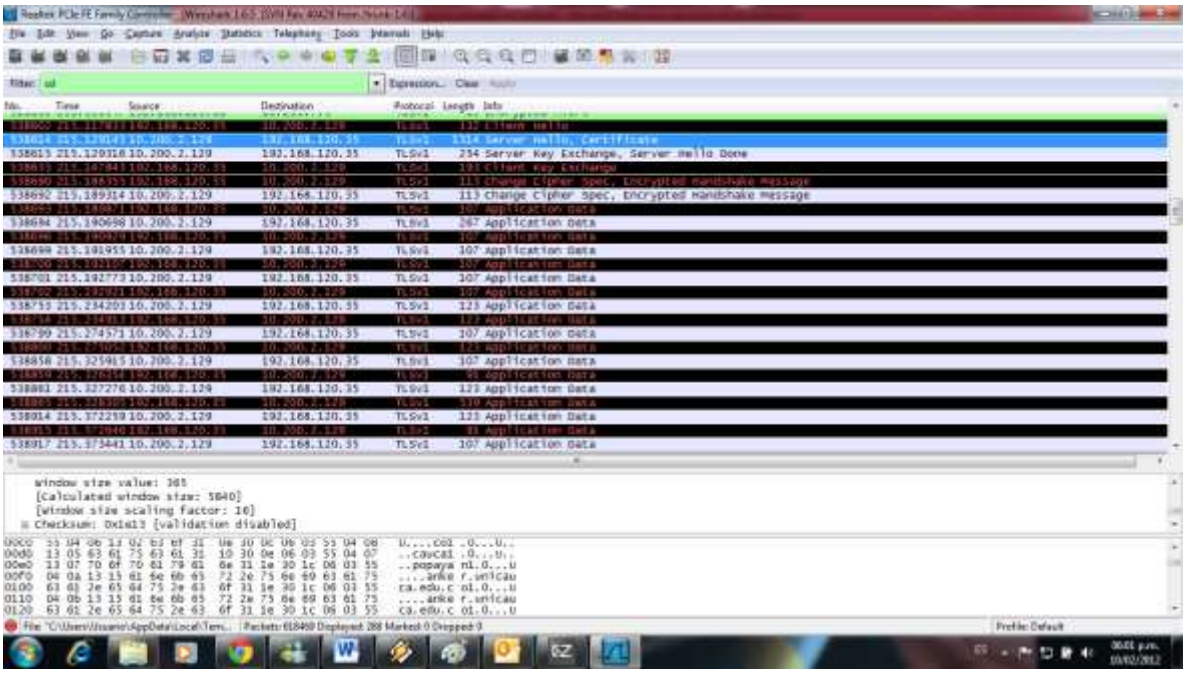


Figura 3.32 Conexión TLS - Zimbra

En la Figura 3.33 y Figura 3.34, se observa la verificación de la recepción del mensaje en la cuenta de usuario del destinatario:

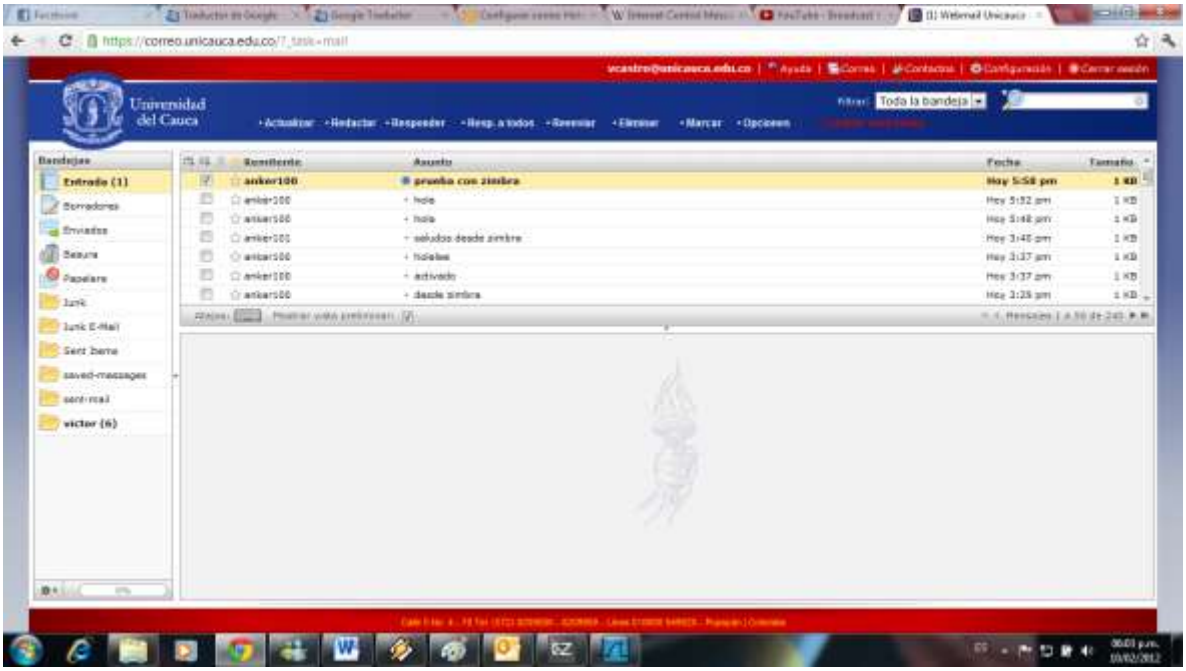


Figura 3.33 Mensajes de usuario - Zimbra

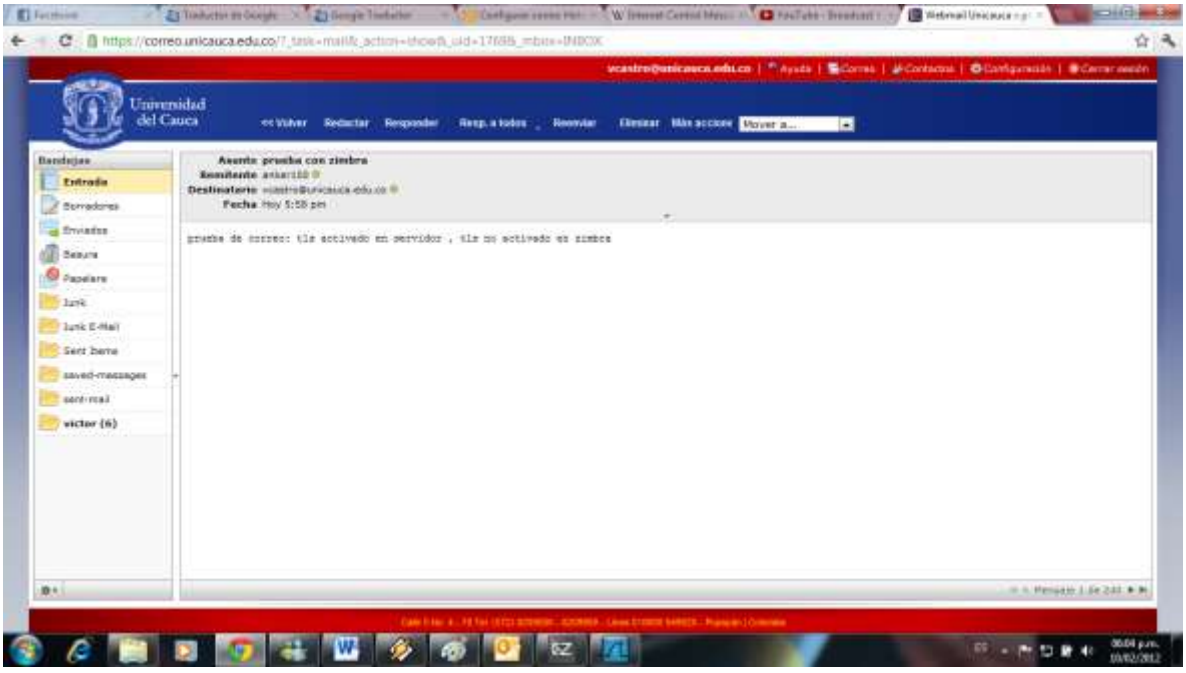


Figura 3.34 Mensaje recibido - Zimbra

Prueba de envío de mensaje con cliente Eudora

Para la prueba de autenticación con el cliente de correo **Eudora**, en la Figura 3.35 se muestra el correo que se va a enviar a una cuenta de Unicauca, este mensaje contiene la hora en que se envía y el nombre del cliente que lo envía (**Eudora**).

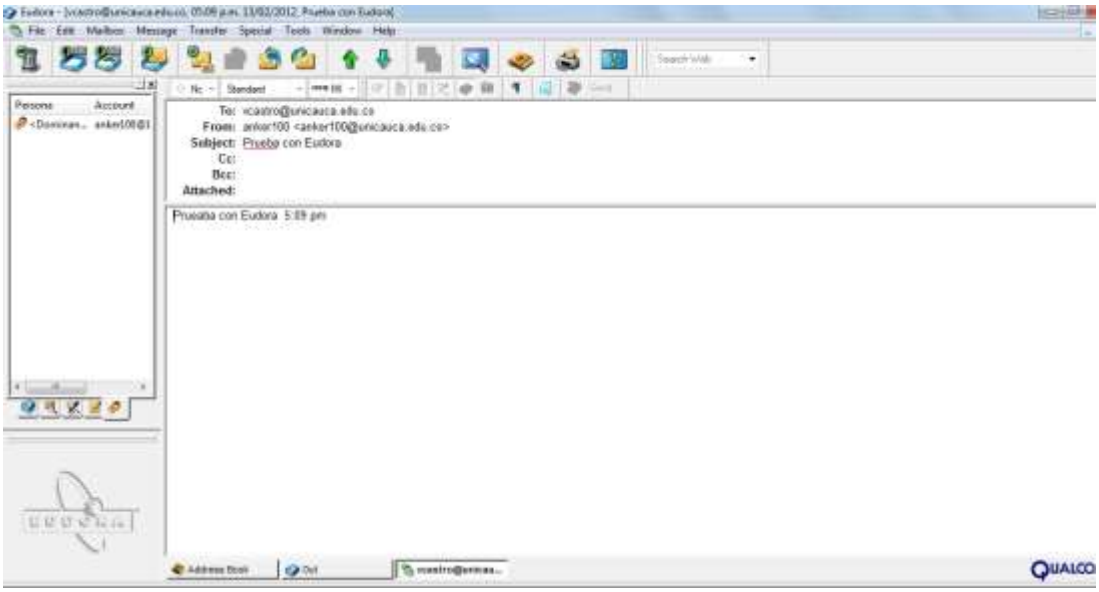


Figura 3.35 Mensaje desde Eudora

Al momento de realizar el envío de correo, la Figura 3.36 muestra que el sistema solicita que se introduzca la contraseña del usuario para poder hacerlo.

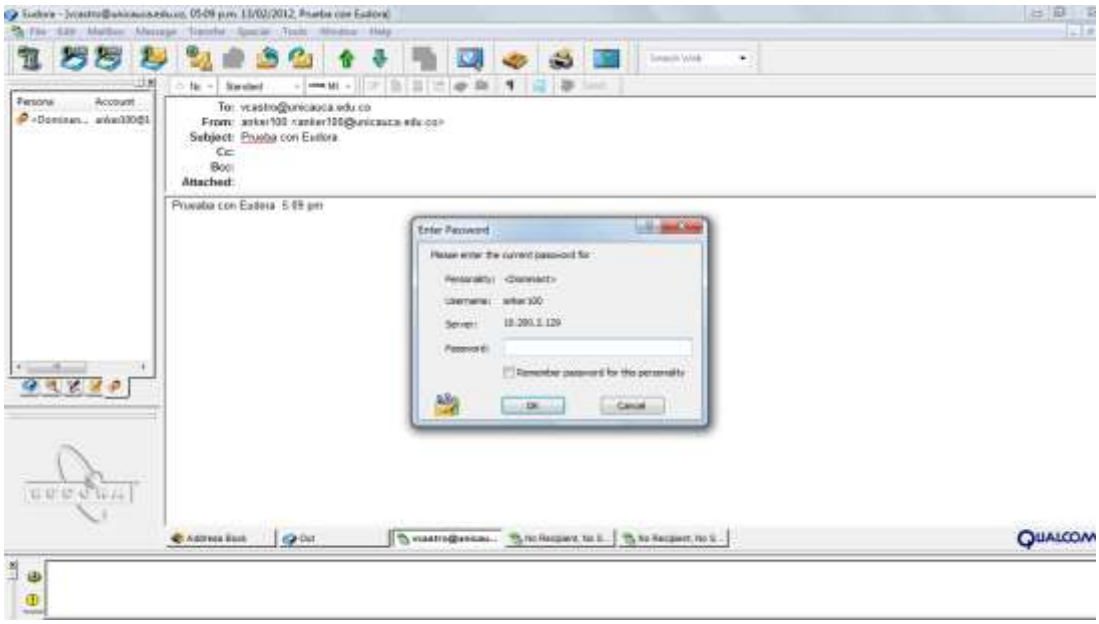


Figura 3.36 Autenticación con cliente Eudora

En la Figura 3.37 se puede observar que el correo ha llegado al usuario de Unicauca y la hora de llegada.

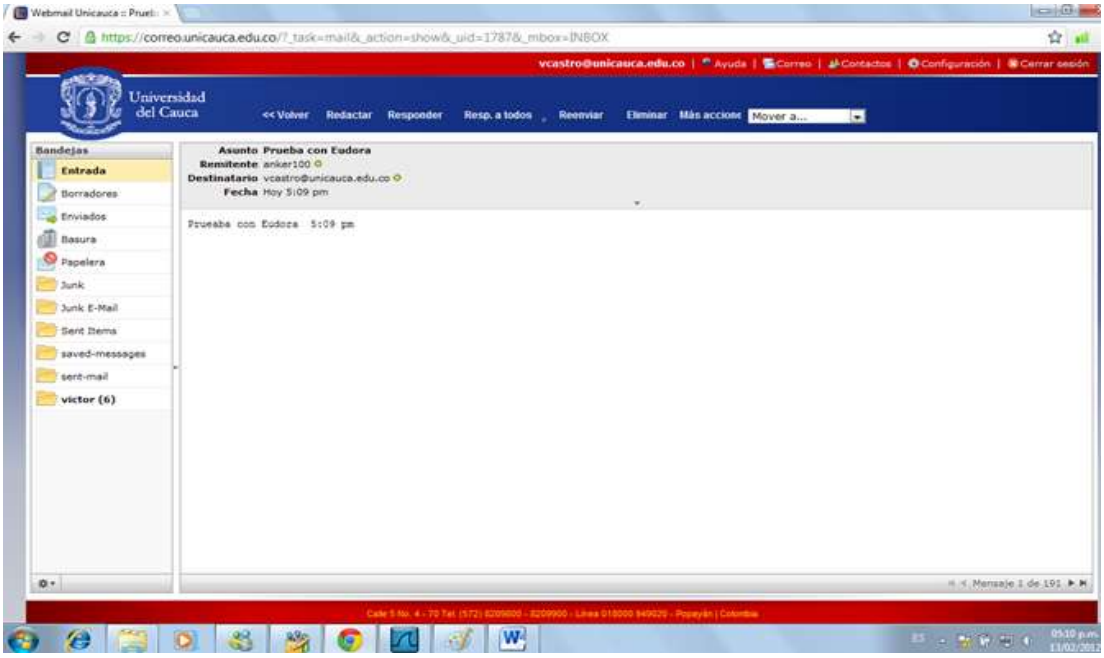


Figura 3.37 Recepción del mensaje Unicauca

En la Figura 3.38 y Figura 3.39 se observa que en el envío de correo se realizó una comunicación cifrada, se utilizó **Wireshark** para observar dicho comportamiento en la transmisión.

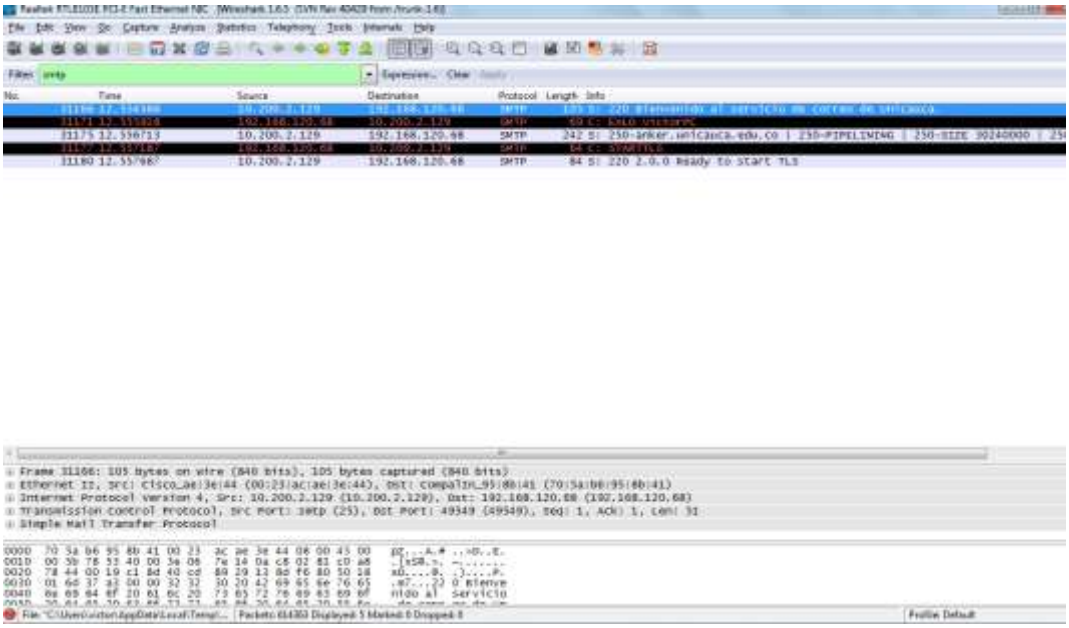


Figura 3.38 Comunicación SMTP con Wireshark

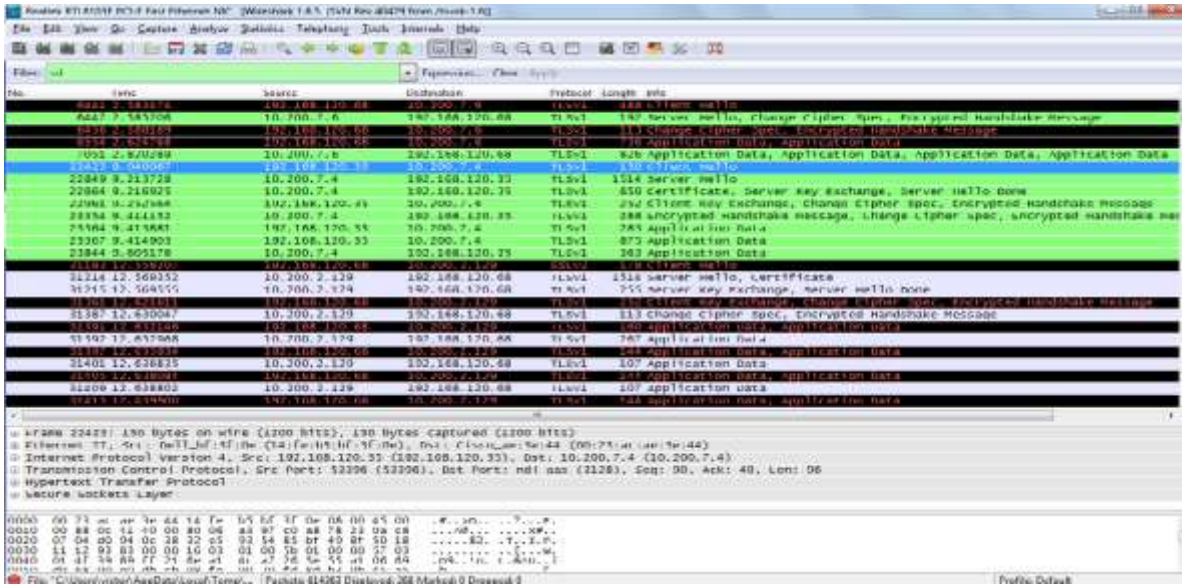


Figura 3.39 Captura de datos con Wireshark

En las pruebas realizadas con los clientes de correo, se puede observar el comportamiento del sistema que se configuró previamente, se puede encontrar el funcionamiento de la autenticación y el cifrado de acuerdo a las configuraciones hechas en el servidor y en los diferentes clientes de correo y de esta manera saber si el sistema que se quiere implementar funciona correctamente.

3.3.2 Pruebas y resultados en servidor de producción

Luego de haber realizado todas las configuraciones y pruebas necesarias en el servidor de prueba, se pasa a realizar estas mismas en el servidor de correo electrónico de la Universidad del Cauca (afrodita.unicauca.edu.co). Para verificar que este servidor está funcionando correctamente de acuerdo a las configuraciones de autenticación y cifrado efectuadas, se realizan algunas pruebas de envío de mensajes de correo para observar y analizar el comportamiento de este servidor. Las pruebas se llevaron a cabo desde consola y utilizando el cliente de correo **Outlook**.

3.3.2.1 Pruebas con telnet

Las primeras pruebas que se realizaron para observar como se encuentra funcionando el servidor Afrodita, se hicieron mediante una conexión por Telnet a este servidor. Se utilizaron las cuentas de usuario davidandrade@unicauca.edu.co y ferchodas@hotmail.com.

- **Prueba 1: intento de envío de correo sin autenticarse**

En esta prueba se realiza un intento de envío de correo desde una cuenta de Unicauca hacia una cuenta de Hotmail, en la Figura 3.40 se observa de forma clara este procedimiento.

Figura 3.40 Intento de envío de correo sin autenticarse

En la figura anterior se observa que el envío de correo se intenta realizar sin antes haber realizado el proceso de autenticación, por lo tanto no se puede enviar el mensaje, mostrando un anuncio de acceso denegado "`Relay access denied`".

- **Prueba 2: envío de correo con autenticación**

Esta prueba se realizó enviando un mensaje de correo desde una cuenta de Unicauca hacia un usuario de Hotmail. Para esta prueba se realiza el proceso de autenticación antes de enviar el mensaje por parte del usuario remitente, por lo tanto la entrega del mensaje se realiza de forma satisfactoria. En la Figura 3.41 se observa este procedimiento.

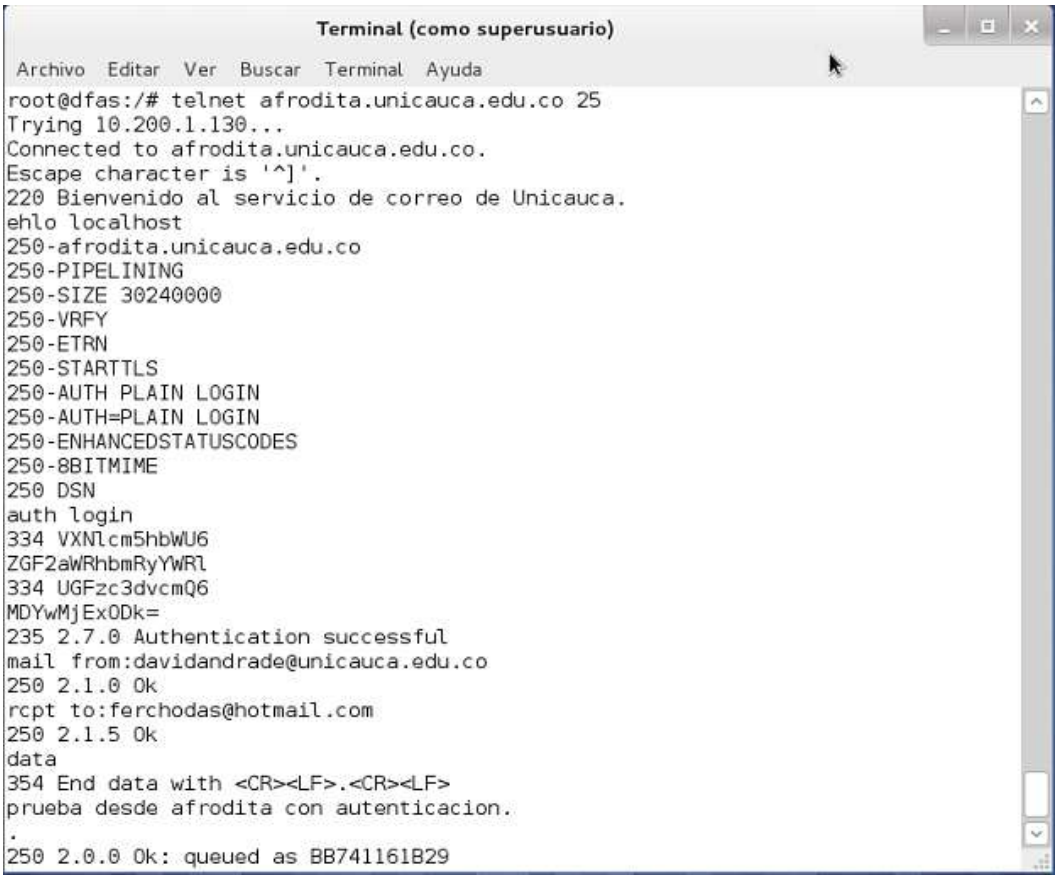


Figura 3.41 Envío de correo con autenticación

Antes de enviar el mensaje, se realiza el proceso de autenticación ingresando los datos de usuario de forma codificada (nombre de usuario y contraseña) a través del método de codificación base64, esto es para que la información de usuario no se haga visible.

La codificación del nombre de usuario y contraseña se realiza con el siguiente comando:

`perl –MMIME::Base64 –e 'print encode_base64("palabra a cifrar")'`

En la Figura 4.42 se puede observar este proceso de codificación.

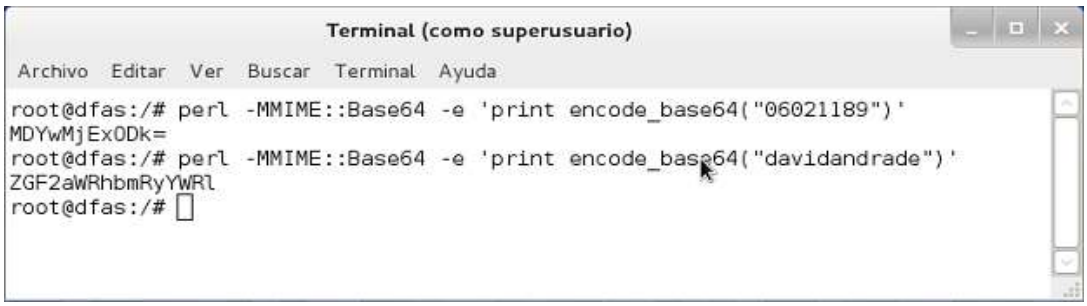


Figura 3.42 Codificación en Base64

3.3.2.2 Pruebas con cliente de correo

El cliente utilizado para las pruebas de envío de mensajes fue **Outlook**. Este se configuró para administrar la cuenta davidandrade@unicauca.edu.co para realizar envío de mensajes a la cuenta ferchodas@hotmail.com, a través del servidor afrodita.unicauca.edu.co.

- **Prueba 1: con solicitud de autenticación - sin cifrado**

Para esta prueba, **Outlook** se configuro de tal manera que solicite autenticación, pero sin conexión cifrada mediante TLS.

En la Figura 3.43 se observa la ventana de envío de mensajes del cliente **Outlook**.

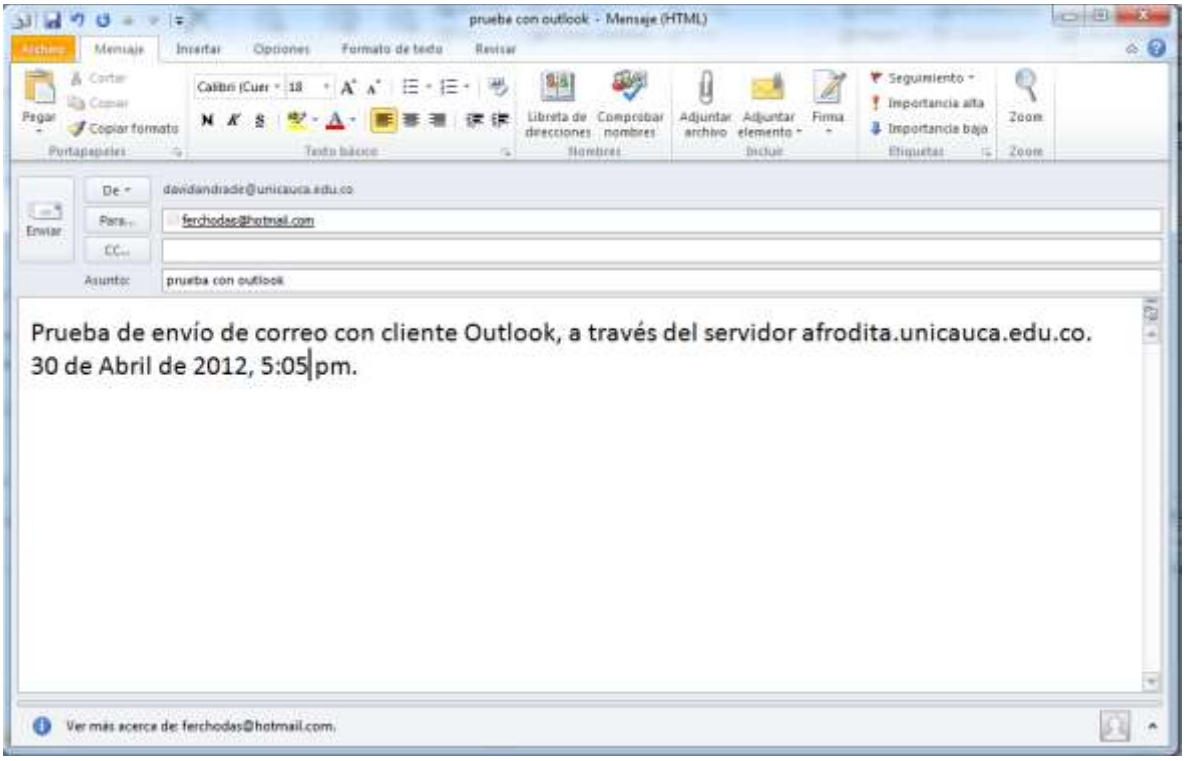


Figura 3.43 Envío de correo con solicitud de autenticación - sin cifrado

Al momento de enviar el mensaje, el sistema solicita el ingreso de la información de autenticación de usuario, mostrando la ventana de la Figura 3.44.

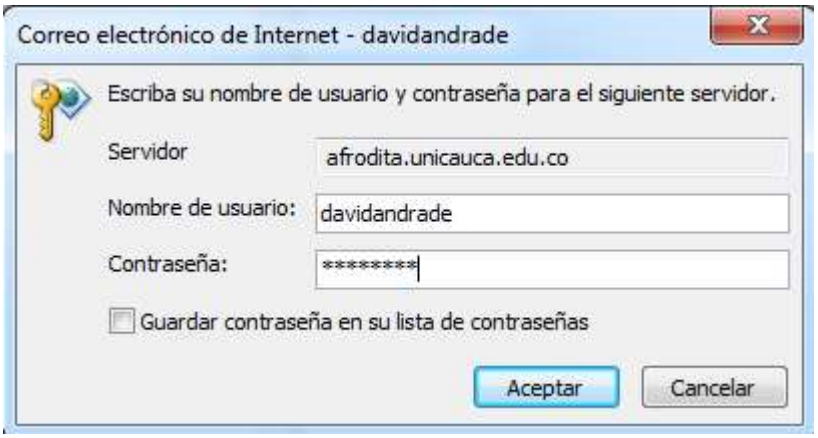


Figura 3.44 Solicitud de autenticación - sin cifrado

Para verificar que el mensaje fue enviado satisfactoriamente, la Figura 3.45 muestra que el mensaje quedo en la carpeta de elementos enviados por parte del usuario.

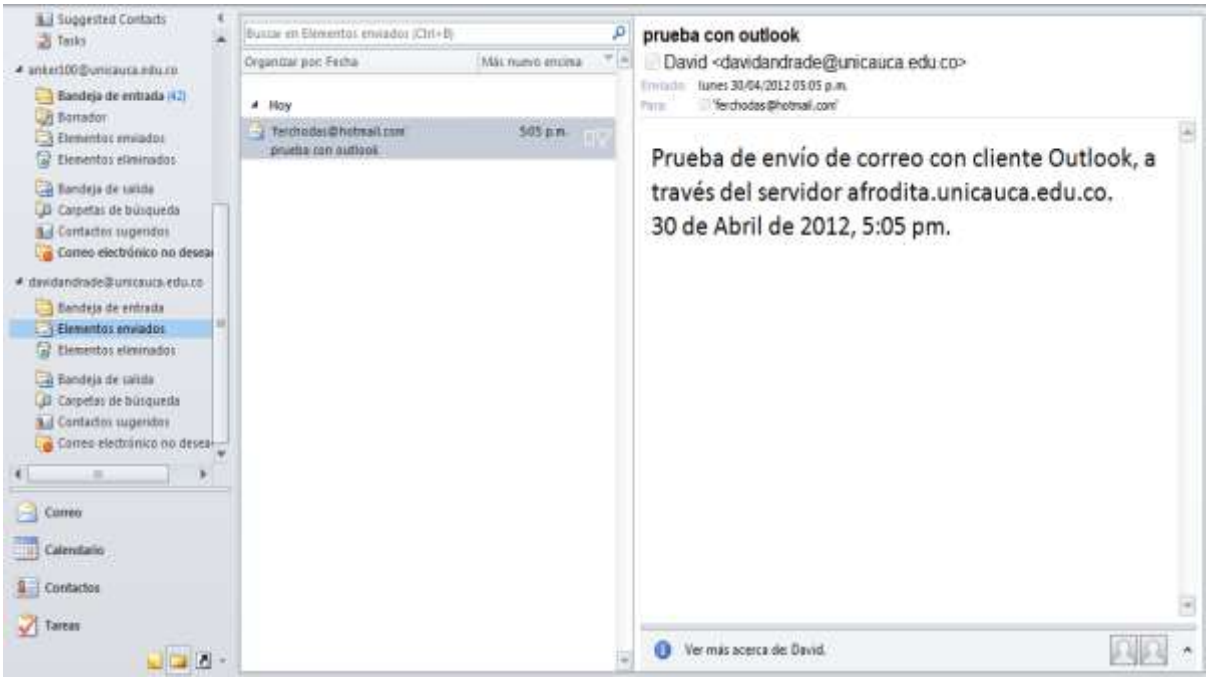


Figura 3.45 Mensaje enviado con solicitud de autenticación - sin cifrado

También se verifica en la bandeja de entrada del destinatario, como se observa en la Figura 3.46.

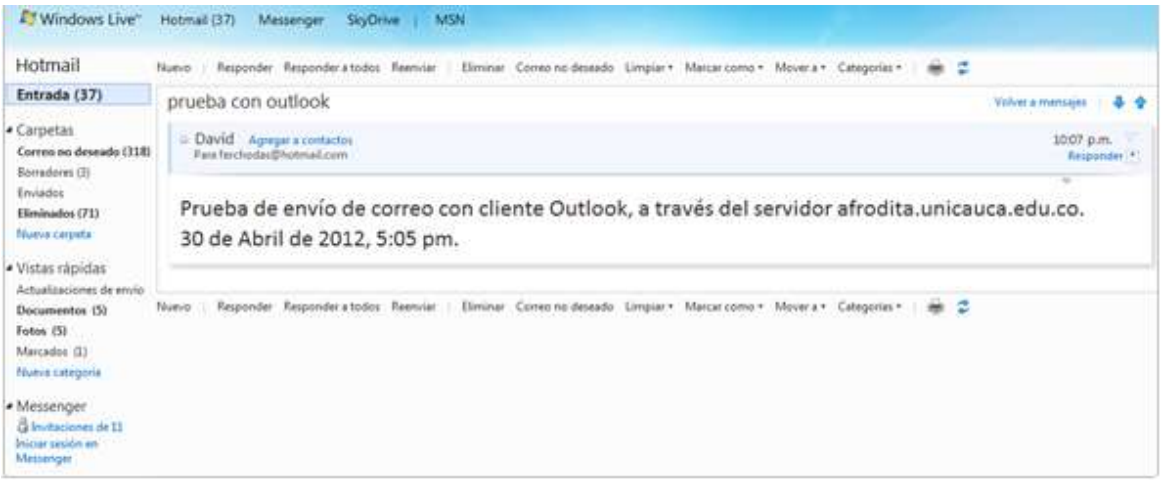


Figura 3.46 Mensaje recibido con solicitud de autenticación - sin cifrado

Se utilizó Wireshark para observar como se lleva a cabo todo este proceso, como se muestra en la Figura 3.47.

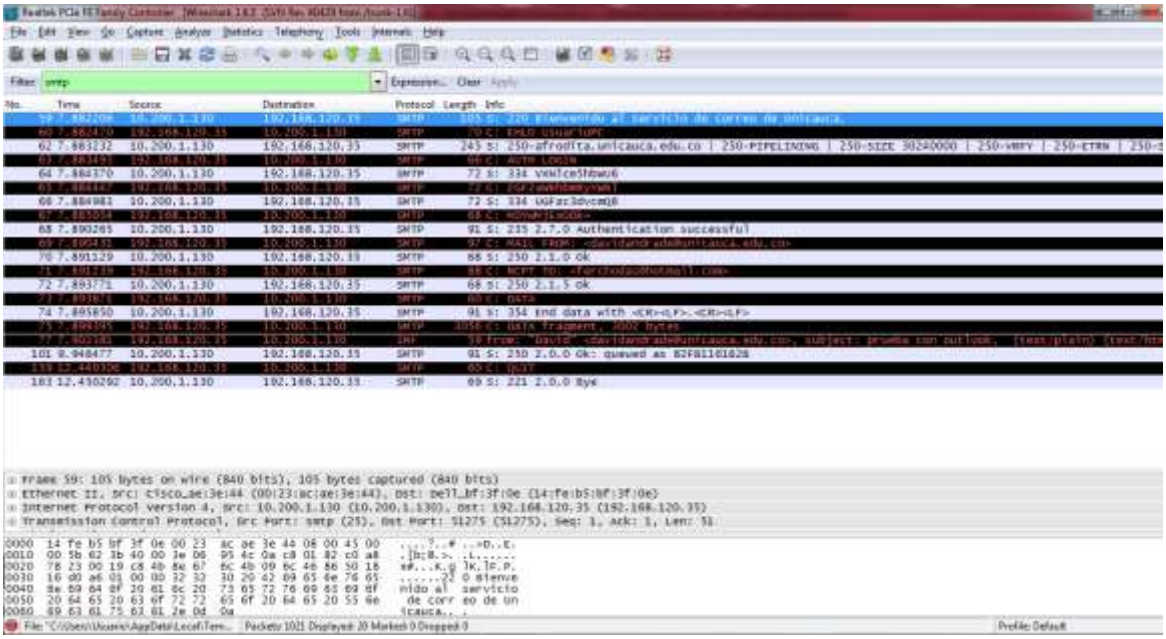


Figura 3.47 Análisis con Wireshark con solicitud de autenticación - sin cifrado

Como se configuró para que la comunicación no fuera cifrada, esta imagen permite observar el proceso de autenticación y del envío del mensaje. Se observa el usuario remitente y el destinatario, también se observa el asunto del mensaje enviado.

- **Prueba 2: cliente sin solicitud de autenticación**

Para esta prueba se configuró **Outlook** para que no solicite autenticación al momento de enviar el mensaje, como se ve en la Figura 3.48.

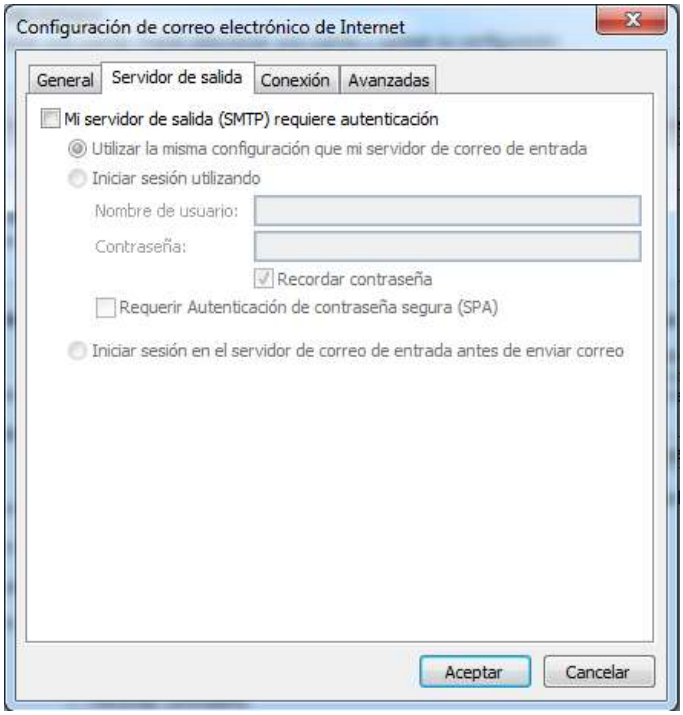


Figura 3.48 Cliente sin solicitud de autenticación

La Figura 3.49 muestra la ventana para realizar el envío del mensaje.

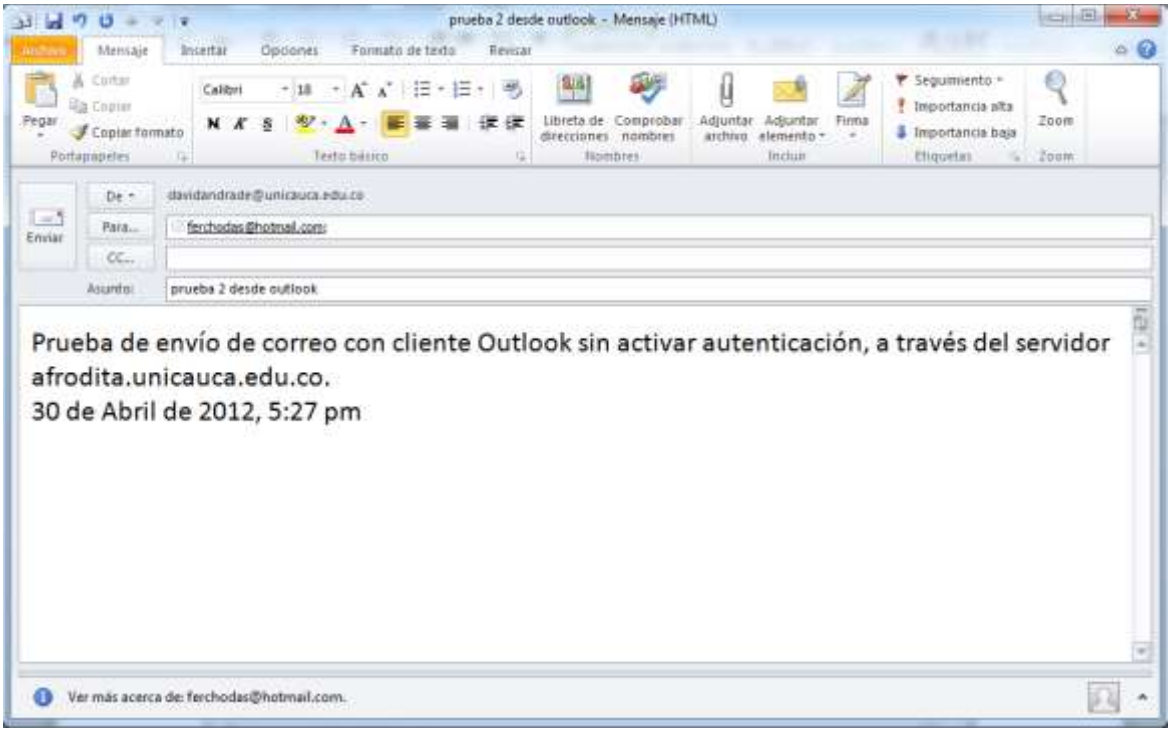


Figura 3.49 Envío de correo sin solicitud de autenticación

Como el servidor Afrodita ya esta configurado para solicitar los datos de autenticación, la Figura 3.50 muestra que no se puede enviar el mensaje ya que no se tiene activada la solicitud de autenticación en el cliente de correo. El sistema retorna un mensaje de acceso denegado para la entrega de este mensaje.

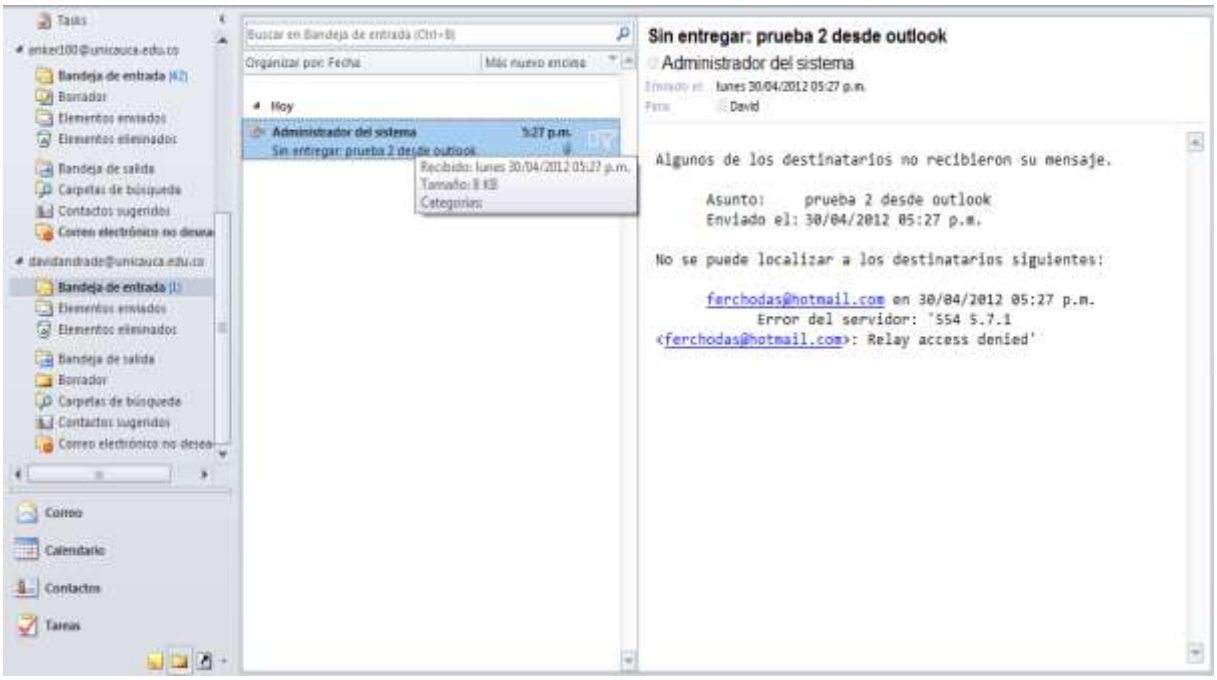


Figura 3.50 Mensaje sin entregar sin solicitud de autenticación

- **Prueba 3: con solicitud de autenticación y cifrado**

Esta prueba se realizó para observar como es el envío de los mensajes cuando se tiene activada la solicitud de autenticación y el cifrado con TLS en el cliente.

La Figura 3.51 muestra la ventana para enviar el mensaje de correo.

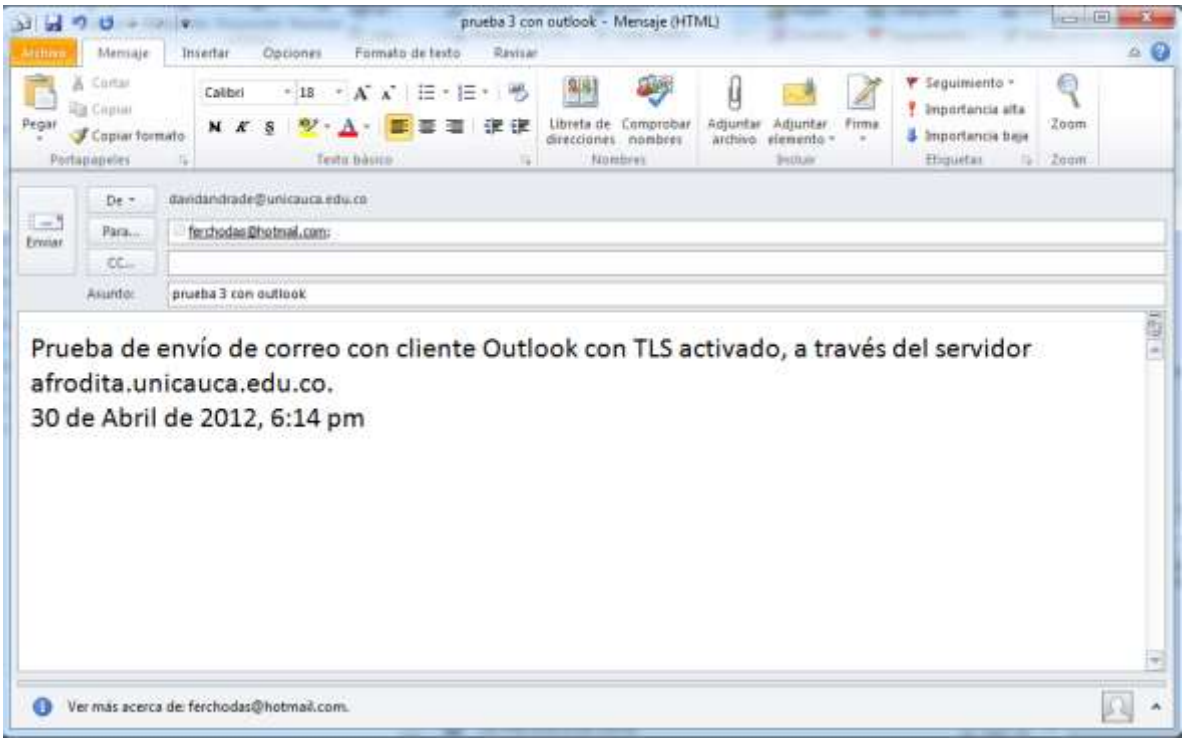


Figura 3.51 Envío de correo con solicitud de autenticación y cifrado

La Figura 3.52 muestra la ventana para ingresar la información de autenticación al momento de enviar el mensaje.

Figura 3.52 Solicitud de autenticación - con solicitud de autenticación y cifrado

Para verificar que el mensaje llego satisfactoriamente, se ingresa a la cuenta de usuario del destinatario como se ve en la Figura 3.53.

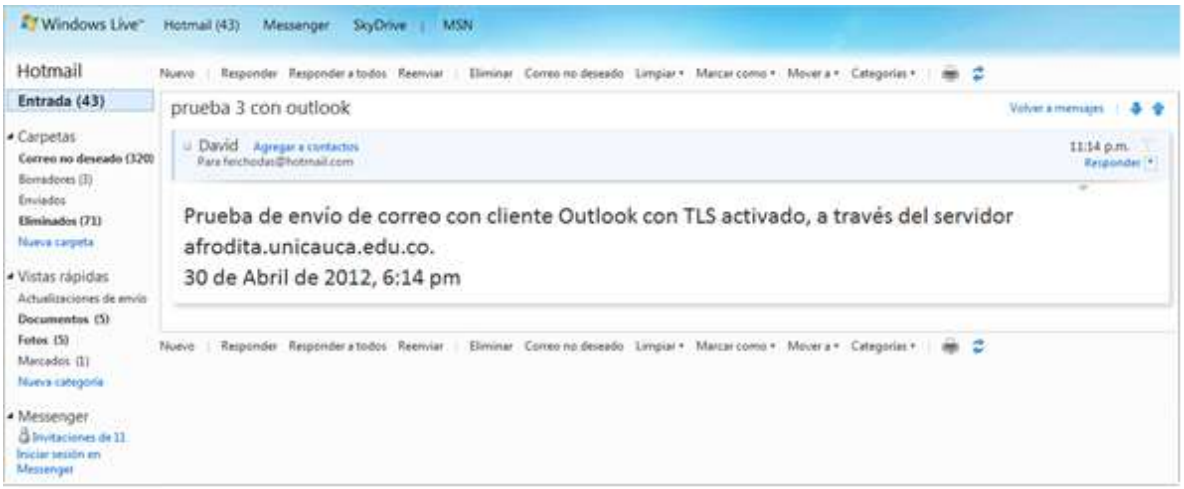


Figura 3.53 Mensaje recibido con solicitud de autenticación y cifrado

A través de **Wireshark**, en la Figura 3.54 se observa el comportamiento de la comunicación del envío del mensaje. No se evidencia los datos de autenticación de usuario ni los datos del mensaje ya que se encuentra activado el cifrado. Se evidencia el uso de TLS.

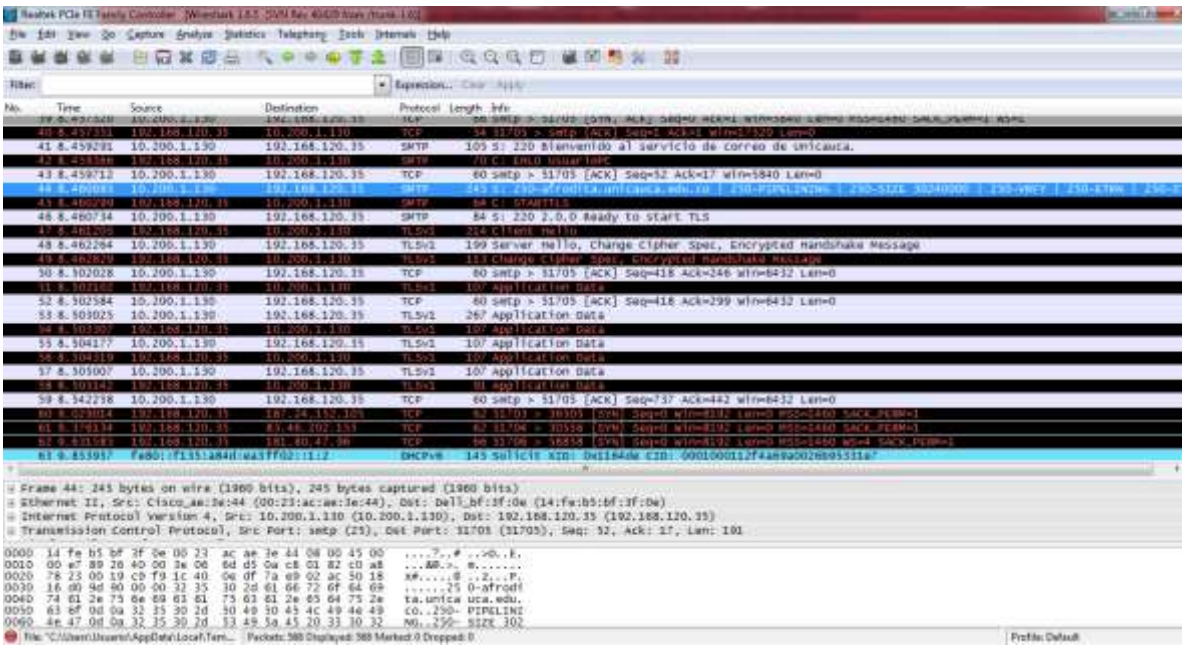


Figura 3.54 Análisis con Wireshark - con solicitud de autenticación y cifrado

Luego de realizar la configuración de autenticación para el servicio de correo de la Institución y verificar el funcionamiento por medio de pruebas a través de telnet y con clientes de correo, se realizaron pruebas de rechazo por fallo de autenticación en las que se muestra el intento de conexión de otros sistemas hacia el dominio de la Universidad del Cauca.

La Figura 3.55 muestra el archivo de registro del servidor de correo afrodita en donde se observa el rechazo por fallo de autenticación de un sistema que intentó conectarse con el dominio de la Institución.

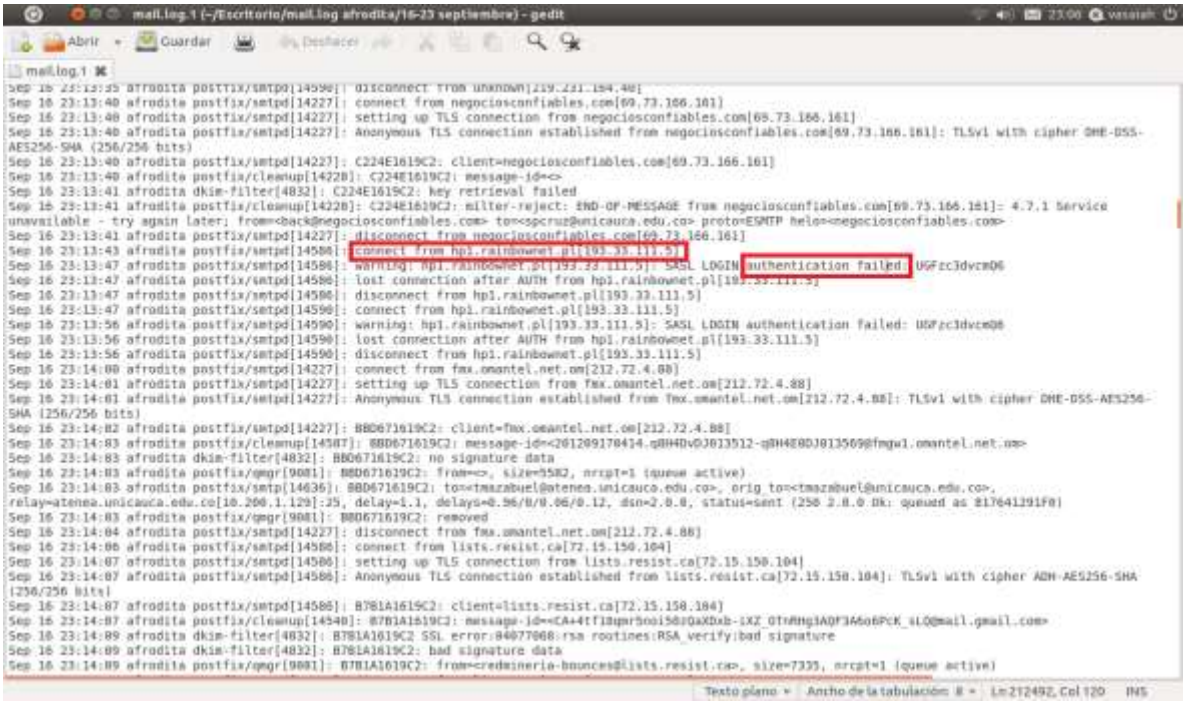


Figura 3.55 Archivo de registro de servidor Afrodita

En este archivo se observa el trabajo que el servidor realiza al rechazar una conexión por fallo de la autenticación, como se muestra en la Figura 3.56 el sistema rechaza la conexión del sistema que se ha identificado como hp1.rainbownet.pl, ya que este ha fallado al momento de autenticarse.

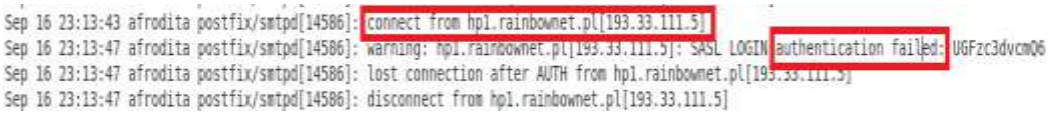


Figura 3.56 Rechazo de conexión por fallo de autenticación

Para verificar que el sistema está solicitando el proceso de autenticación y observar los rechazos por fallo de la misma, se tomó el registro del servidor durante un periodo de quince (15) días y se realizó una grafica con el número de conexiones rechazadas por día durante este periodo de tiempo. La Figura 3.57 muestra la cantidad de rechazos ejecutados por el servidor afrodita por fallo en la autenticación, realizadas entre las fechas del 16 y 30 de Septiembre. Se puede observar que el método de autenticación ha sido efectivo en el rechazo de conexiones no autorizadas.

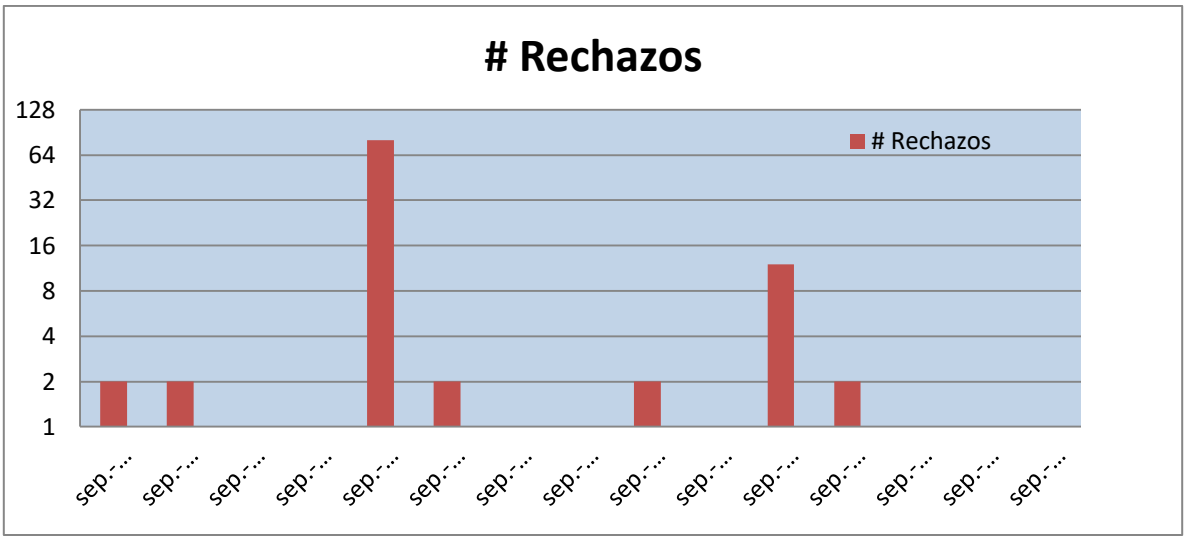


Figura 3.57 Rechazos en periodo de tiempo de 15 días

La implementación de la autenticación en el servicio de correo incrementa los niveles de seguridad, de tal forma que no se permiten accesos no autorizados al servidor de correo de la Universidad del Cauca, de esta manera se reducirán el número de mensajes *spam* que pueden ser transmitidos a través del dominio de la Institución hacia otros dominios.

Con la puesta en funcionamiento de la autenticación de usuario en el sistema de correo en el marco de este trabajo de grado, la División de Gestión de Tecnologías de Información y Comunicaciones (TIC), emitió un documento público dirigido a la comunidad universitaria, informando la realización de algunos cambios en el servicio de correo de la Institución y refiriéndose a que los usuarios que utilizan clientes de correo deben habilitar la autenticación para el servidor de salida. La Figura 3.58 muestra el comunicado que fue ubicado en el portal web de la Universidad del Cauca.

Figura 3.58 Comunicado para configuración de clientes de correo

3.4 PRUEBAS Y RESULTADOS DE ROBUSTEZ DE CONTRASEÑAS

Debido a la ausencia de un sistema que permita verificar la robustez de las contraseñas de los usuarios, se presenta en esta sección los esquemas de validación de acuerdo a la configuración de un módulo que permite realizar estas funciones.

Se especifica la configuración de un método de verificación de robustez de contraseñas y otro para generar contraseñas aleatorias automáticamente. A continuación se presenta la descripción de cada uno de estos sistemas.

3.4.1 Verificación de la robustez de contraseñas

Es de gran importancia dar a conocer a los usuarios el nivel de seguridad de la contraseña que se está estableciendo, para este caso se ha puesto en funcionamiento un código en **Javascript**, el cual permite que el usuario conozca el nivel de seguridad de la contraseña que esta originando.

A medida que el sistema va encontrando el nivel de seguridad de la contraseña, esta va cambiando de color, el menor nivel de seguridad es el color rojo y el nivel más seguro es el verde oscuro. A continuación se muestran algunas imágenes del sistema, mientras se introduce una contraseña.

En las Figura 3.59 se muestra una contraseña con un nivel de seguridad bajo.

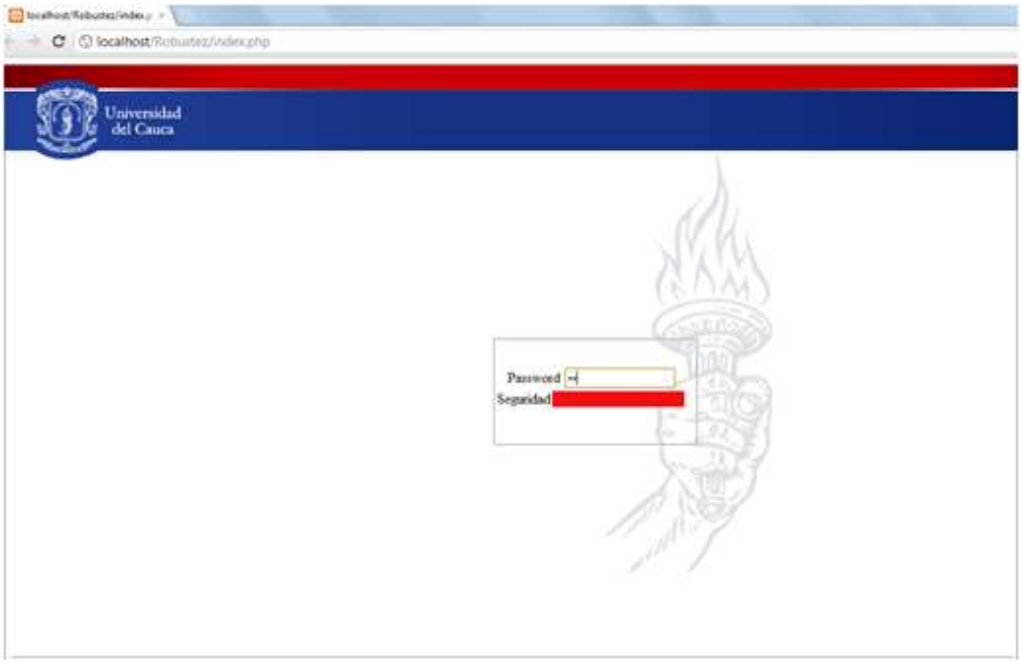


Figura 3.59 Contraseña nivel bajo

La Figura 3.60 muestra que se crea una contraseña de un nivel de seguridad medio-bajo.

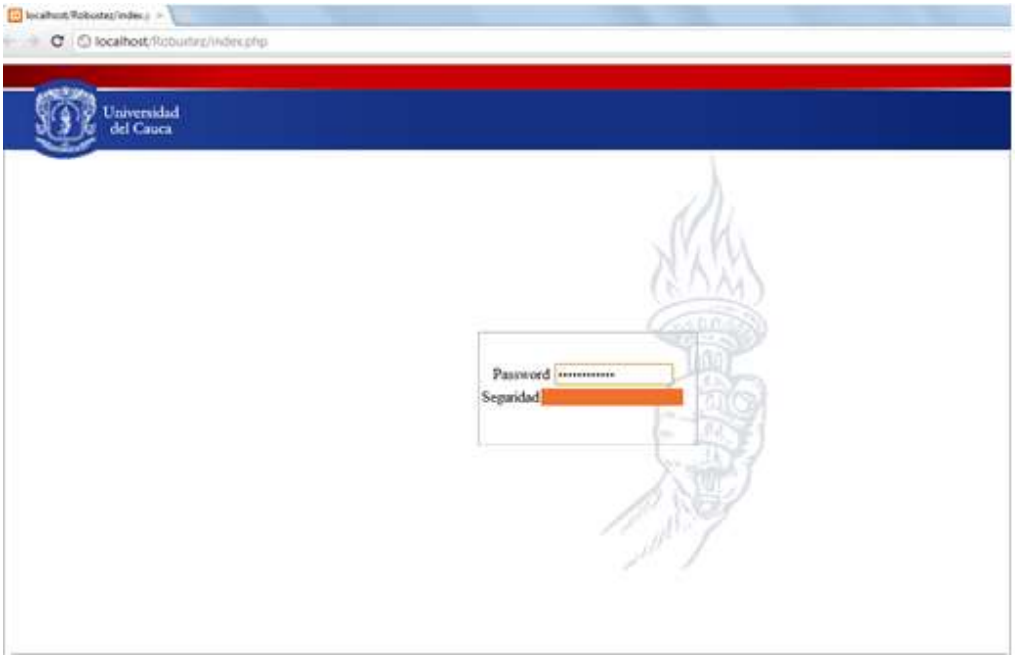


Figura 3.60 Contraseña nivel medio-bajo

En la Figura 3.61 se observa la creación de una contraseña de nivel medio-alto.

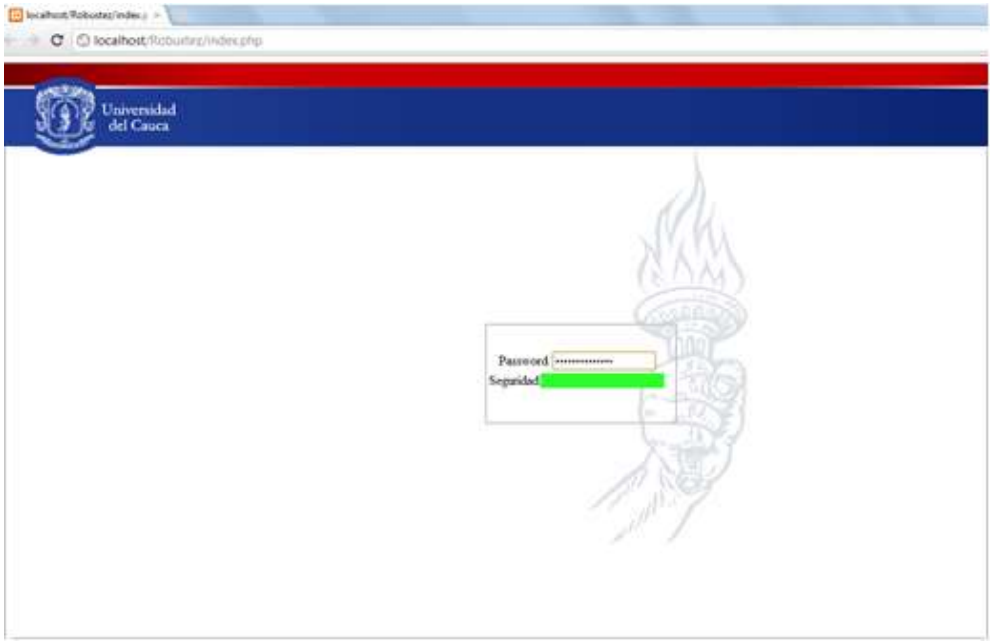


Figura 3.61 Contraseña nivel medio-alto

La Figura 3.62 muestra una contraseña con un nivel de seguridad alto.

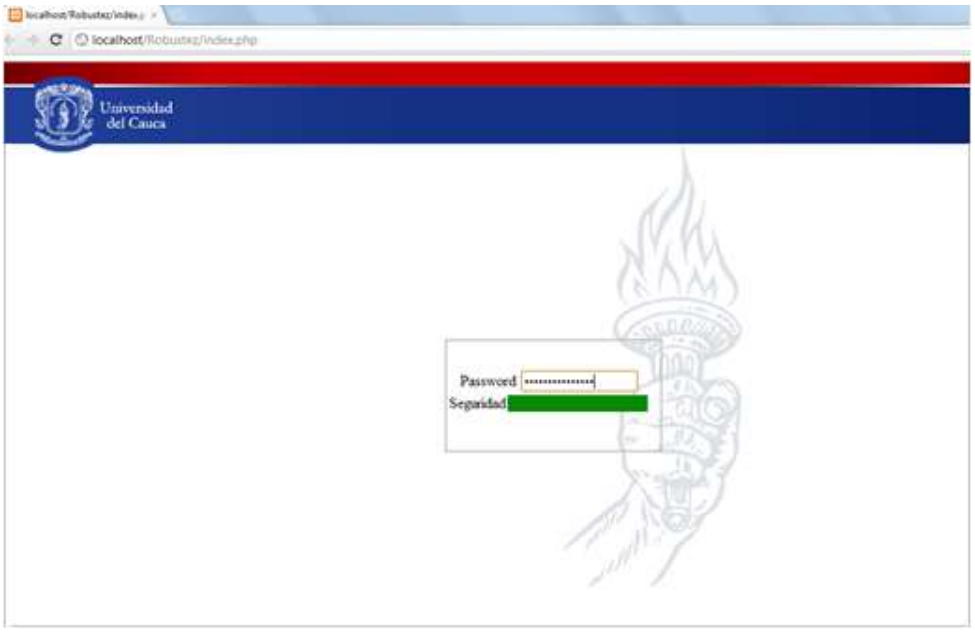


Figura 3.62 Contraseña nivel alto

En la Figura 3.63 se muestra el módulo para la verificación de robustez de contraseñas tal como se encuentra ahora aplicado al sistema de correo electrónico de la Institución.

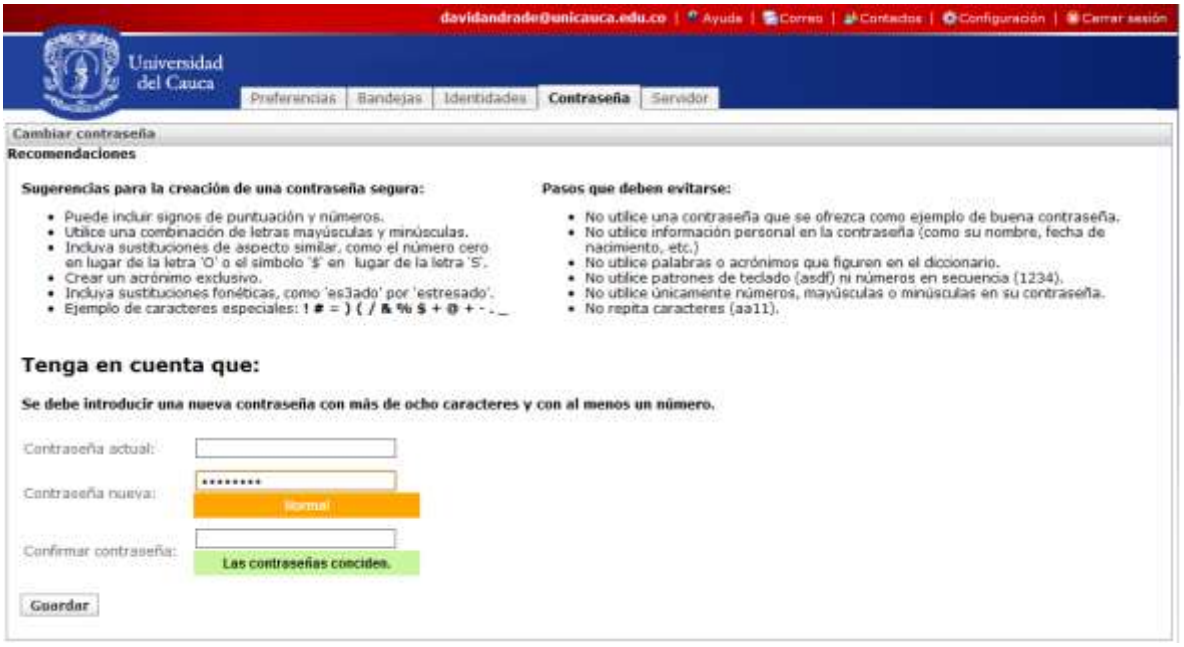


Figura 3.63 Verificación de robustez de contraseñas en Unicauca

En cuanto a la verificación de robustez de contraseñas, ahora se cuenta con un módulo que permite a los usuarios darle un nivel de seguridad a sus contraseñas para brindar mayor protección a sus cuentas. El nivel de seguridad se va mostrando a medida que el usuario va ingresando la contraseña y esta va aumentando su robustez. Cada uno de los

niveles que se tienen configurados en este módulo se representa por medio de un color, estos son:

- **Inseguro**: representado con color rojo, indica que la robustez de la contraseña es baja.
- **Normal**: representado con color naranja, indica que la robustez de la contraseña es media, esto quiere decir que la contraseña tiene un nivel aceptable de seguridad pero no se considera suficientemente robusta.
- **Optimo**: representado con color verde, indica que la robustez de la contraseña es alta.

3.4.2 Generador automático de contraseñas

Inicialmente se pensó en incluir en el portal web de la Universidad un módulo que permitiera la creación automática de contraseñas puesto que la mayoría de las veces no se hace fácil para los usuarios crear una contraseña segura, pero este método fue descartado ya que generaba contraseñas demasiado complejas y difíciles de recordar.

En las siguientes figuras se muestra el módulo en funcionamiento y se observa la complejidad contraseñas que éste genera, lo cual demuestra porque ésta opción fue descartada.

La Figura 3.64 muestra la creación de una contraseña de 8 caracteres.

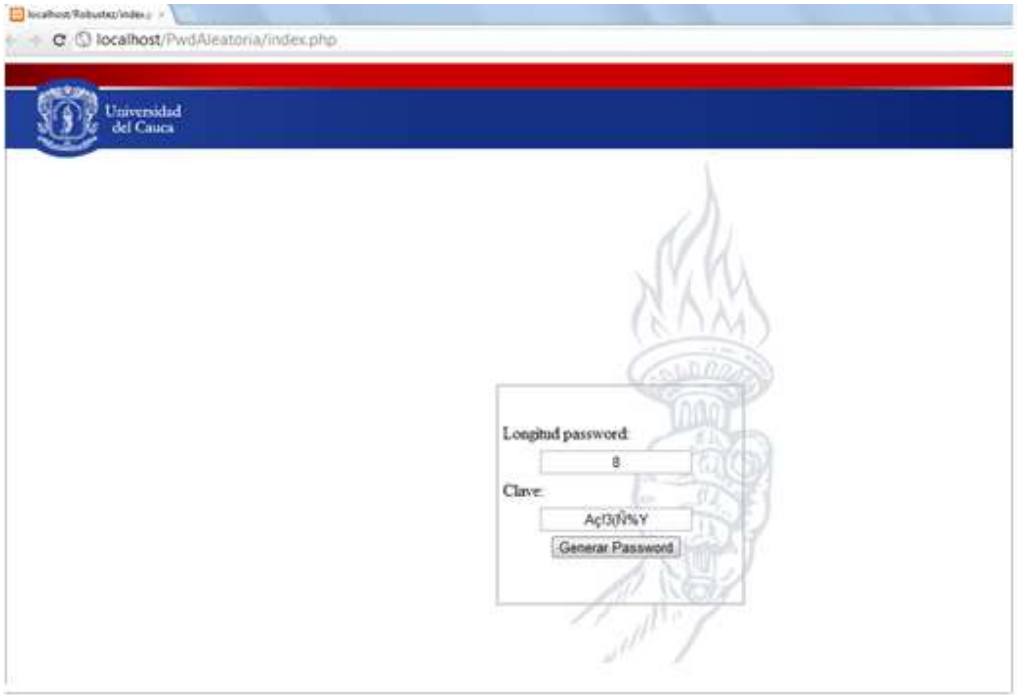


Figura 3.64 Contraseña de 8 caracteres

La Figura 3.65 muestra la creación de una contraseña de 14 caracteres.

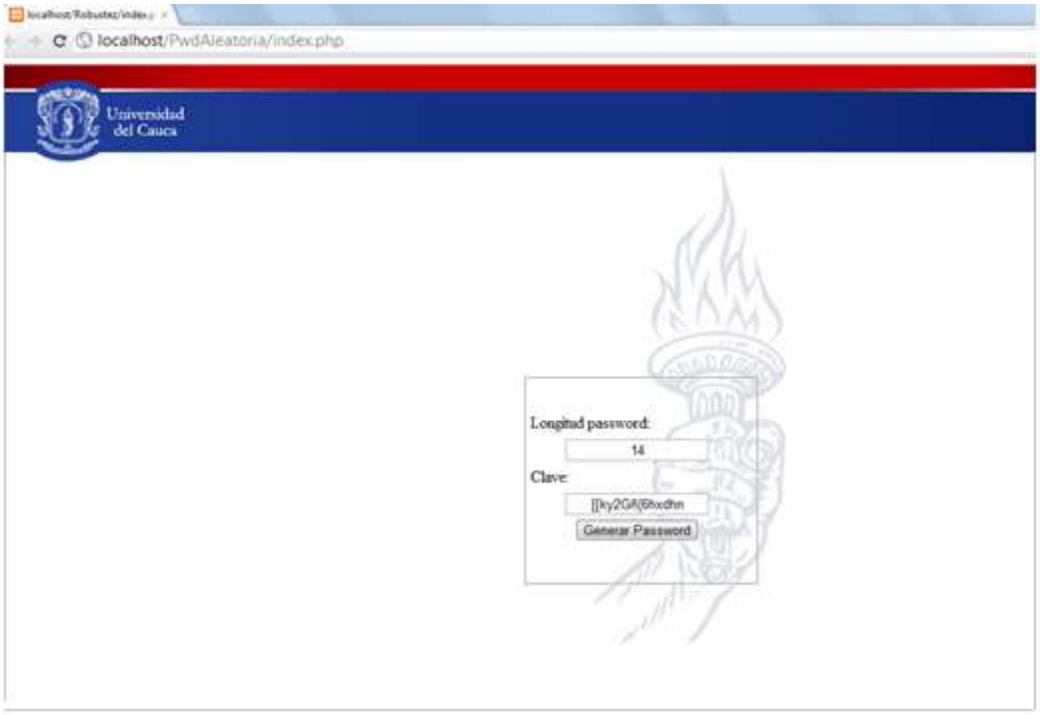


Figura 3.65 Contraseña de 14 caracteres

Al finalizar estas pruebas y generar la validación de los resultados, se puede decir que se atendieron a las necesidades del sistema de correo electrónico de la Universidad del Cauca en cuanto al control de *spam*, autenticación, cifrado y verificación de robustez de contraseñas dando cumplimiento a los objetivos propuestos para el desarrollo de este trabajo de grado aportando mayor seguridad y confiabilidad en lo que se refiere al uso autorizado del servicio de correo y también incrementando el control de los mensajes que circulan por los servidores de la Institución.

En el Anexo I se evidencia la aceptación por parte de la administración de servicios de internet de la Institución, debido al aporte de este trabajo de grado con la solución de las falencias presentadas en el servicio de correo.

Con la culminación de este trabajo de grado se obtuvo un mayor nivel de conocimiento en cuanto a servidores basados en Linux, especialmente acerca del servidor de correo electrónico y la importancia que este tiene dentro de una Institución. Se conocieron los problemas mas comunes que se pueden presentar en éste sistema y los métodos que se pueden utilizar para mitigarlos, se aprendió que para poner en marcha un servicio de correo electrónico, es necesario realizar diversas instalaciones y configuraciones y también tener en cuenta diferentes aspectos para obtener como resultado final un sistema en correcto funcionamiento.

CAPITULO 4

4 CONCLUSIONES Y RECOMENDACIONES

Los objetivos propuestos por este trabajo de grado se han cumplido y al mismo tiempo se han analizado comparativamente las herramientas necesarias para que el sistema de correo de la Universidad del Cauca pueda ofrecer un mejor servicio a sus usuarios.

En este trabajo de grado se deja en evidencia las herramientas con las cuales se obtuvieron mejores resultados para atender las necesidades del sistema de correo de la Institución.

4.1 CONCLUSIONES

- El mejoramiento del sistema de correo de la Institución ofrece a los usuarios un servicio más seguro y confiable en el cual se busca garantizar la entrega de correo al destinatario y la total integridad de los datos que se transmiten por los servidores de correo de la Universidad del Cauca.
- El servicio de correo electrónico, por ser uno de los más utilizados debido a que ayuda a simplificar y a realizar de forma efectiva las labores de los usuarios, se hace necesario mantener una constante supervisión y actualización de sus componentes para que se encuentre en óptimas condiciones de funcionamiento.
- Un sistema puede tener un nivel de funcionamiento óptimo pero no esta exento de recibir mejoras de cualquier tipo.
- Un sistema seguro y robusto puede ser implementado con la utilización de sistemas basados en software libre.
- La implementación de un módulo *antispam* genera una reducción en la carga de un servidor de correo y además evita las molestias de los usuarios al recibir en su bandeja de correo gran cantidad de mensajes que ellos no han solicitado.
- Aunque existan herramientas comerciales que ayudan a prevenir el *spam* como por ejemplo **Fortigate** y su modulo *antispam UTM***,** este se puede complementar con el uso de otros programas soportados bajo la licencia del software libre para controlar el correo saliente y el correo interno de la Institución.
- La integración de las herramientas antispam seleccionadas al servicio de correo permitió mejorar la capacidad del sistema de detectar mensajes *spam* que llegan al dominio y también de aquellos que se generan internamente.
- La integración del sistema de autenticación al servicio de correo aportó una solución efectiva que mejoró la seguridad del sistema, proporcionando un mecanismo en el cual los servidores de correo de la Universidad del Cauca solo sean utilizados para enviar mensajes por los usuarios de la Institución.

- La implementación de la autenticación en el servicio de correo ha reducido el envío de correo no deseado a través del servidor de correo de la Universidad del Cauca, ya que no se permiten conexiones de otros sistemas que quieran enviar correo masivo a través del servidor de la institución.

- Si un sistema de correo se encuentra configurado con autenticación, es importante realizar cifrado del canal de comunicación para proteger la información de usuario.
- La integración de las herramientas que manejan *quotas* de correo y el servicio de autenticación aumenta el nivel de eficiencia del sistema de correo, ya que limitando la cantidad de correo que un usuario puede enviar hacia otros dominios y además que el servidor solicite autenticación de usuario, se puede mitigar la caída del servidor de correo de la Universidad en una lista negra.

- El módulo para generar contraseñas con una alta entropía suele ser un componente necesario para un buen servicio de correo electrónico, ya que permite que los usuarios tengan cierto nivel de seguridad para que sus contraseñas no puedan ser descifradas, y así proteger sus cuentas de correo de accesos no autorizados.
- En el módulo de robustez de contraseñas, aunque es óptimo tener una entropía bastante alta, en el momento de llevarse a la practica es necesario hacer ajustes al nivel de seguridad que va a tener una contraseña para que esta pueda acomodarse a una situación real, es decir si se le exige al usuario la creación de una contraseña con una entropía muy alta puede ocurrir que a este se le sea muy difícil de recordar y al final termine por olvidarla.

4.2 RECOMENDACIONES

- Proporcionar capacitación a los usuarios del sistema de correo de la Universidad del Cauca, en la cual se evidencien métodos para la creación de contraseñas robustas.

- Generar conciencia en aquellas personas que utilizan el servicio de correo de la Universidad del Cauca para que no registren sus cuentas de correo en páginas de internet cuya procedencia no sea confiable, también en que se abstengan de responder las cadenas de mensajes que llegan a su cuenta puesto que estas son métodos de los *spammers* para obtener direcciones de correo y así enviar *spam* a dichas direcciones.

- Dar a conocer a los usuarios acerca de la utilización de los clientes de correo, para utilizar de manera efectiva la autenticación y el cifrado.

- Cuando se realicen trabajos de este tipo se recomienda buscar la documentación más reciente y proveniente de sitios confiables, en lo posible de sitios oficiales en

donde la información ofrecida es actualizada, ya que se encuentra gran cantidad de información que puede estar obsoleta y que puede no ser útil al momento de comprender y de realizar las instalaciones y configuraciones pertinentes.

- Mantener una investigación permanente sobre los avances de las tecnologías y aplicaciones desarrolladas para los sistemas de correo electrónico, ya que los *spammers* y *hackers* son bastantes innovadores y constantemente desarrollan técnicas para violar la seguridad de los servidores de correo y esto conlleva a que se generen nuevos métodos para contrarrestar este tipo de ataques.

4.3 TRABAJOS FUTUROS

- Definir un método de detección de *spam* por apreciación de usuario, esto es, desarrollar una herramienta que permita al usuario por medio de una opción en el portal web, definir si el correo que llega a su cuenta es o no *spam*.

REFERENCIAS BIBLIOGRÁFICAS

[1] «www.fortinet.com,» Fortinet, 2012. [En línea]. Available: http://www.fortinet.com/products/fortigate/.

[2] Fortinet, «www.fortinet.com,» [En línea]. Available: http://www.fortinet.com/sites/default/files/productdatasheets/FGT300Series_DS.pdf. [Último acceso: 2012].

[3] U. d. L. A. A. Holguin, «Autenticación Centralizada Con Tecnología Ldap,» 2002.

[4] «glosario de informatica e internet,» [En línea]. Available: http://www.internetglosario.com/560/Spam.html.

[5] «web.mit.edu,» 2008. [En línea]. Available: http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-sg-es-4/s1-wstation-pass.html.

[6] Á. R. Gallón, *El Lenguaje Unificado de Modelado,* 2000.

[7] «es.scribd.com,» [En línea]. Available: http://es.scribd.com/doc/50406603/CASOS-DE-USO-03.

[8] J.Myers, «SMTP Service Extension for Authentication,» [En línea]. Available: www.faqs.org/rfcs/rfc2554.html#b.

[9] Grupo de Nuevas Actividades Profesionales, «Correo Electronico y Spam,» [En línea]. Available: http://es.scribd.com/doc/19049881/20/Medidas-de-lucha-contra-el-Spam.

[10] P. R.Thomas, «Anti_spam Comparison Report,» [En línea]. Available: https://www.westcoastlabs.com/downloads/productTestReport_0061/Anti-spam_Comparative_Report.pdf.

[11] RedIRIS, «www.rediris.es,» 2008. [En línea]. Available: http://www.rediris.es/race/doc/RACE.v2.2.pdf.

[12] Bankoi, 2010. [En línea]. Available: http://www.helpdesk-software.ws/es/it/18082004.htm.

[13] «Filtros bayesianos,» [En línea]. Available: http://www.laflecha.net/articulos/blackhats/estadistica/.

[14] S. S. C. c. y. c. Spam, «J.Fernandez,» *Germinuz,* 2005.

[15] «Subdirección de Seguridad de la Información,» 2011. [En línea]. Available: http://www.seguridad.unam.mx/documento/?id=8.

[16] U. d. C. Grupo I+D Nuevas Tecnologias en Telecomunicaciones, «Análisis de Modelos de Evaluación de Calidad de Software Libre,» 2012.

[17] D. Hernandez, «Analisis de FLOSS con OpenBRR, QSOS y OMM,» 2012. [En línea]. Available: http://dherna.homeip.net/blog/?p=434.

[18] 2012. [En línea]. Available: http://en.wikipedia.org/wiki/Open_source_software_assessment_methodologies.

[19] «Open Maturity Model,» 2010. [En línea]. Available: http://www.qualipso.org/omm-champion.

[20] «Comparación de (OpenBRR y QSOS) Breve Análisis a estas Metodologías,» 2011. [En línea]. Available: http://www.isotel-tics.com/blog-mswl-sergioml/?p=375.

[21] [En línea]. Available: http://spamassassin.apache.org/.

[22] 2011. [En línea]. Available: http://dspam.sourceforge.net/.

[23] «Debian Package Tracking System,» [En línea]. Available: http://packages.qa.debian.org/s/spamassassin.html.

[24] [En línea]. Available: http://bugs.debian.org/cgi-bin/pkgreport.cgi?src=dspam.

[25] «sourceforge.net,» 2012. [En línea]. Available: http://sourceforge.net/tracker/?atid=1126467&group_id=250683&func=browse.

[26] «Apache Spamassassin Project,» [En línea]. Available: http://spamassassin.apache.org/tests_3_3_x.html.

[27] «packages.debian.org,» [En línea]. Available: http://packages.debian.org/source/testing/dspam.

[28] «wiki.apache.org,» [En línea]. Available: http://wiki.apache.org/spamassassin/MailingLists.

[29] «sourceforge.net,» [En línea]. Available: http://sourceforge.net/project/memberlist.php?group_id=250683.

[30] «sourceforge.net,» [En línea]. Available: http://sourceforge.net/mail/?group_id=250683.

[31] «sourceforge.net,» [En línea]. Available: http://sourceforge.net/project/memberlist.php?group_id=250683.

[32] «spamassassin.apache.org,» [En línea]. Available: http://spamassassin.apache.org/doc.html.

[33] «wiki.apache.org,» [En línea]. Available: http://wiki.apache.org/spamassassin/WeLoveVolunteers.

[34] «packages.qa.debian.org,» [En línea]. Available: http://packages.qa.debian.org/s/spamassassin.html.

[35] «dspam.nuclearelephant.com,» [En línea]. Available: http://dspam.nuclearelephant.com/.

[36] [En línea]. Available: http://rtc.umn.edu/dspam/I_am_DSPAM_Summer_2011_Newsletter.pdf.

[37] [En línea]. Available: http://wiki.apache.org/spamassassin/MailingLists.

[38] [En línea]. Available: http://gmane.org/plot-rate.php/plot.png?group=gmane.mail.spam.spamassassin.general&plot.png.

[39] [En línea]. Available: http://svn.apache.org/repos/asf/spamassassin/trunk/CREDITS.

[40] [En línea]. Available: http://egrojgomez.blogspot.com/2008_12_19_archive.html.

[41] [En línea]. Available: http://sourceforge.net/mailarchive/forum.php?forum_name=dspam-user.

[42] [En línea]. Available: http://sourceforge.net/projects/dspam/support.

[43] [En línea]. Available: http://lwn.net/Articles/87818/.

[44] J.Muñoz, «Metodologia para la incorporación de medidas de seguridad en sistemas de información de gran implantación».

[45] P.Perez, «La seguridad en el correo electronico,» 2007.

[46] «Documento descriptivo del servicio de correo electrónico de la universidad de la Rioja».

[47] P. P. B. Perez. [En línea]. Available: https://webmail.unizar.es/desarrollo/rediris_boletin5859.pdf.

[48] Grupo GNU/Linux de la Universidad del Cauca, «gluc.unicauca.edu.co,» 2008. [En línea]. Available: http://gluc.unicauca.edu.co/wiki/index.php/Documentaci%C3%B3n_MTAs_y_Tabla_comparativa .

[49] 2011. [En línea]. Available: http://translate.google.com.co/translate?hl=es&sl=en&tl=es&u=http%3A%2F%2Fen.wikipedia.org%2Fwiki%2FSendmail.

[50] P. Koetter, «www.linux-magazin.de,» 2007. [En línea]. Available: http://www.linux-magazin.de/Heft-Abo/Ausgaben/2007/06/Auf-der-Teststrecke.

[51] J. Suarez, «www.redes-linux.com,» 2007. [En línea]. Available: http://www.redes-linux.com/manuales/openldap/curso_openldap.pdf.

[52] P. Hoffman. [En línea]. Available: http://blog.pablohoffman.com/problemas-con-mails-de-adinet.

[53] 2012. [En línea]. Available: http://support.google.com/a/bin/answer.py?hl=es&hlrm=es&answer=33786.

[54] «lubrin.org,» 2006. [En línea]. Available: http://lubrin.org/spip.php?article63.

[55] [En línea]. Available: http://www.policyd.org/.

[56] [En línea]. Available: http://www.naguissa.com/universidad/wiki-td/SSL_TLS.html.

[57] M. Alvarez, «desarrollo web.com,» [En línea]. Available: http://www.desarrolloweb.com/articulos/script-informar-seguridad-clave-javascript.html.

[58] U. S. Bolivar, «El Plan de Pruebas,» [En línea]. Available: http://ldc.usb.ve/~teruel/ci4713/clases2001/planPruebas.html.

[59] M. Tabares, «Introduccion a las pruebas de software,» 2011. [En línea]. Available: http://es.slideshare.net/mstabare/introduccin-de-pruebas-de-software.

[60] M. M. D.Caballo, Estudio del Open/Free (GNU/Linux) como plataforma de servicios de red en entornos empresariales.