UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

IMPLEMENTACIÓN DE CORREO ELECTRÓNICO PARA LA DIVISIÓN DE INGENIERÍAS CIVIL Y GEOMÁTICA DE LA FACULTAD DE INGENIERÍA

TESIS

PARA OBTENER EL TÍTULO DE

INGENIERO EN COMPUTACIÓN

PRESENTA:

ANGELES MARIELA JIMÉNEZ XOSPA
KARLA JESSICA GABRIELA DE LA LUZ ELEUTERIO

DIRECTOR

M. en I. TANYA ITZEL ARTEAGA RICCI

CIUDAD UNIVERSITARIA, MÉXICO, D.F. **2013**

Índice general

Índice de figuras

Índice de tablas

Introducción

A lo largo de la historia el hombre ha buscado formas, aunque sean primitivas, de comunicar sus pensamientos, ideas, mensajes e información. El intercambio de ésta se hacía a través de señas, y ha evolucionado hasta llegar a la comunicación a distancia mediante los dispositivos avanzados.

En los últimos años se fueron desarrollando distintas formas que permitieron acceder a diferentes tipos de comunicación: visual, verbal, escrita, entre otros. La principal de todas ellas fue la oral, hasta la aparición de la escritura, la cual fue impulsada en Roma.

En Roma se desarrolló el que fue el antecesor del periódico, se publicaban actas para comunicar diferentes acontecimientos de la ciudad y se colocaban en tablones de madera que se encontraban en los muros de las ciudadelas.

Es también gracias a la escritura que surgen las primeras cartas, propiciando así el sistema de Correo Postal, facilitando la información a distancia.

En el siglo XVI la comunicación escrita tomo fuerza al inventarse la imprenta, favoreciendo la rápida difusión de las noticias y facilitando el acceso a la información, llegando a un número mayor de personas.

En el siglo XIX aparecieron las máquinas de escribir, desplazando los textos manuscritos, reduciendo el tiempo en la realización de documentos y proporcionando un formato más oficial. La máquina de escribir formó uno de los instrumentos más útiles e indispensables en las oficinas del siglo XX hasta que fue desplazada por la computadora.

La computadora es una máquina electrónica utilizada para el procesamiento de datos, ofreciendo diferentes servicios: la realización rápida de documentos, descargar diferentes tipos de archivos (música, video, imágenes, entre otros), tener contacto con personas de todo el mundo a través de Internet, comunicarse con familiares o amigos mediante el correo electrónico por mencionar algunos.

Internet surgió de un proyecto desarrollado por el gobierno de los Estados Unidos para apoyar sus fuerzas militares. Tiempo después de su creación no sólo fue utilizado por el gobierno, sino también universidades y otros centros académicos, lo cual permitió la oportunidad de difundir la información de manera global, así como la interacción entre las personas, independientemente de su localización geográfica rompiendo de esta manera barreras y fronteras invisibles, dando paso al correo electrónico. En el siglo XX fue posible enviar mensajes de correo electrónico entre computadoras que se encontraran dentro de la misma red local. Con el paso del tiempo el correo electrónico es el servicio más utilizado en todo el mundo para la comunicación personal.

En los siguientes capítulos se hablará más ampliamente sobre las Tecnologías de la Información así como el uso, la función y la implementación del correo electrónico.

Objetivo General

Describir el funcionamiento e implementación que se llevará a cabo en la instalación y configuración del servidor de correo electrónico con el fin de que el personal académico y administrativo de la División de Ingenierías Civil y Geomática cuente con una cuenta de correo.

Objetivos Específicos

- Instalar y configurar un servidor de correo electrónico para el personal docente y administrativo de la División de Ingenierías Civil y Geomática.
- Lograr que el servidor de correos de la DICyG sea un distintivo institucional.

Capítulo 1

Marco Teórico

1.1. Antecedentes de las Tecnologías de la Información

Las Tecnologías de la Información o simplemente TI, hacen referencia al desarrollo e instalación de aplicaciones informáticas utilizando tecnologías de *hardware* y *software*, así como servicios relacionados con el almacenamiento, protección, procesamiento y transmisión digital de la información.

El primer término de Tecnología de la Información se definió por primera vez en los años 50 al surgir la primera computadora electrónica llamada ENIAC.

La ENIAC (*Electronic Numerical Integrator And Computer*, Computador e Integrador Numérico Electrónico) era utilizada por el Laboratorio de Investigación Balística del Ejército de los Estados Unidos y fue construida en la Universidad de Pensilvana por John Presper Eckert y John William Mauchly, ocupaba una superficie de $167m^2$, operaba con un total de 17, 468 tubos de vacío y era capaz de realizar 5000 sumas por segundo.

Fue en 1981 cuando IBM desarrollo la primera computadora personal (PC). Surgieron cuatro generaciones de computadoras entre la ENIAC y la PC. En cada generación se presentaba una disminución en el tamaño a la generación anterior. La primera generación utilizó, como ya se mencionó, tubos de vacío, la segunda y tercera utilizaron los transistores y circuitos integrados respectivamente y la cuarta generación utiliza microprocesadores que permitieron el uso de computadoras personales y el desarrollo de Internet.

Internet es un conjunto de redes descentralizadas comunicadas entre sí que operan a través de un protocolo en común. El proyecto que le dio origen a Internet fue creado en 1969 por el Departamento de Defensa de los Estados Unidos llamado ARPANET (por sus siglas en inglés *Advanced Research Project Network*) para apoyar a las fuerzas militares en la investigación y desarrollo de protocolos de comunicación ligando redes capaces de resistir usos rudos para que continuaran funcionando aunque una parte de la red se hubiera estropeado o perdido.

Para que las redes se comuniquen entre sí de manera global y garanticen su comunicación es necesario utilizar cierto "lenguaje en común" dando como resultado en 1972 el protocolo TCP/IP (*Transmission Control Protocol/Internet Protocol*) que es un sistema robusto y sólido encargado de la transmisión fiable de paquetes de datos a través de cualquier ruta disponible. Es bajo este protocolo que se integran todas las redes que conforman actualmente Internet.

Durante el desarrollo de este protocolo se incrementó el número de redes locales de agencias gubernamentales y de universidades que participaban en el proyecto, dando origen así a la conexión LAN.

Las personas que lo utilizaban al ver que la información que encontraban era útil, empezaron a aportar su propia información incrementando la ya existente, de esta manera empezó a crecer la información de manera global y poco a poco se fue convirtiendo en lo que es actualmente, pasando de ser una red gubernamental a una red pública tal y como se le conoce hoy en día.

Las redes actuales son mucho más rápidas, pueden transmitirse a distancias más largas y además ya se puede conectar a Internet de manera inalámbrica, permitiendo conectarse en lugares antes no pensados como por ejemplo en la playa, carretera, lugares públicos, entre otros.

Internet ha creado una revolución no solo en la informática sino en las comunicaciones de todo el mundo. El telégrafo, la radio y el teléfono fueron las bases para lo que después se convertiría en una de las herramientas más utilizadas por el ser humano.

Con su llegada viene la comunicación en tiempo real, facilitando la manera de investigar, hacer negocios, comprar, estudiar y comunicarnos con personas cercanas o externas a nosotros.

1.2. Beneficios de las comunicaciones electrónicas a la sociedad

Las nuevas tecnologías informáticas han generado una forma de comunicación de manera simultánea y no simultánea, fiable y rápida, con personas situadas en diferentes partes del mundo.

Existen grandes beneficios que las nuevas Tecnologías de la Información han ofrecido a la sociedad mundial en su conjunto, que van, desde la educación y formación, hasta la industria y la investigación. A continuación se mencionan algunos de estos beneficios:

- Tuvieron auge en los Gobiernos electrónicos (E-gobiernos), al introducir herramientas informáticas en las instituciones públicas, ya que propició una serie de cambios generalmente positivos, como la modernización de sus sistemas, la automatización de servicios, los procesos en línea y otros como: trámites fiscales; devoluciones y compensaciones, aumento o disminución de actividades, avisos al RFC, entre otros, que con los sistemas tradicionales se demoraban horas, ahora con las nuevas tecnologías tardan solo minutos.
- Hoy en día la mayoría de universidades, institutos y colegios cuentan con algún tipo de tecnología que ha mejorado esencialmente sus programas y servicios; la visita a versiones virtuales de los museos de mayor prestigio y reconocimiento mundial así como acceso a información electrónica, como: bolsa de trabajo, video conferencias, consulta de libros, tutoriales, entre otros.
- Acceder a diversos servicios localizados en diferentes países, por ejemplo; servicios jurídicos, asesorías, contabilidad, conferencias electrónicas, compras, e incluso servicios médicos.
- Se han logrado nuevas formas de producción y de generar riqueza basada en las ideas y especialmente en el conocimiento tecnológico, dando paso a una nueva economía.

1.3. Entornos de comunicación

Las herramientas del área de comunicación (foros de debate, listas de distribución, chats, SMS, mensajería instantánea, entre otros) tienen como finalidad resolver las diferentes necesidades de información y comunicación entre los individuos que participan en el proceso de aprendizaje para la incorporación de habilidades y saberes.

1.3.1. Grupos de noticias / *news*

Los *news* son foros de discusión electrónicos organizados por tema de interés en donde los usuarios pueden discutir e intercambiar información a través del correo electrónico. Cada grupo de noticias corresponde a un tema en específico. Dentro de los *news* los mensajes aparecen de manera pública permitiendo a los miembros del grupo leer y responder dichos mensajes (no es necesario haber realizado una suscripción previa para participar en el debate). Debido a que estos grupos generalmente no son moderados, la libertad del envío de mensajes es total, confiando en el criterio de los usuarios, lo que en algunas ocasiones provoca un ambiente conflictivo.

Los nombres de los grupos de noticias siguen una estructura jerárquica, la cual se separa por puntos y va de un tema general a uno en concreto, adaptando el tema para que los usuarios tengan mayor facilidad en identificar el área de interés. Ejemplo: *es.rec.juegos.ajedrez*.

Los *news* que se desarrollan en lengua española incluyen "es" o "esp". Las abreviaturas para algunos de los temas más utilizados son:

- *alt.* Temas alternativos
- *soc.* Sociedad
- *sci.* Ciencia
- *rec.* Entretenimiento
- *com.* Computación
- *gov.* Gobierno de los Estados Unidos

1.3.2. Listas de distribución

Las listas de distribución son discusiones que mantienen los usuarios inscritos dentro de una lista a través del correo electrónico, permitiendo así la distribución de la información a todos los miembros de la lista.

Cada vez que surge una pregunta, una respuesta o se quiere hacer una aportación al tema, un correo electrónico es enviado automáticamente a cada uno de los miembros de esa lista.

Todo este flujo de información es administrado por programas llamados administradores de listas de distribución MLM (por sus siglas en inglés *Mail List Manager*).

Los dos programas más utilizados son:

- *Majordomo*: Formado por diversos programas permitiendo administrar eficazmente las listas de correo electrónico en Internet, debido a que reduce al mínimo la intervención del administrador.
- *Listservs*: *Software* que gestiona todo tipo de listas de correo electrónico, tanto las que permiten solo enviar un tipo de información como la que permite la comunicación en dos sentidos.

En las listas de distribución intervienen cuatro agentes:

- Los suscriptores que participan en una lista, suelen pertenecer a una entidad profesional cuyo objetivo es llegar a una discusión sobre un tema concreto.
- La tecnología del correo electrónico.
- El programa de distribución de mensajes
- El servidor al que llegan y del que salen los mensajes enviados por los miembros de una lista. Para suscribirse a una lista de distribución se tiene que llenar un formulario (generalmente nombre de usuario o correo electrónico y contraseña) y mandárselo al administrador de la lista. El usuario sin ningún problema podrá suscribirse o borrarse de las listas ya existentes.

1.3.3. *Chat*

El *chat* es un programa que permite la comunicación simultánea en línea realizada en tiempo real entre dos o más personas a través de mensajes de texto, evolucionando hasta permitir la utilización de voz y video. El *chat* dio pie a los *chat rooms* (salas de charla) que son lugares virtuales organizados por tema donde la gente se une a la sala para conversar.

1.3.4. SMS (*Short Message Service*, Servicio de Mensaje Corto)

Servicio que permite enviar y recibir mensajes de texto cortos desde un celular a otro o enviarlos a través de Internet a otro celular, la capacidad máxima de los mensajes es de 160 caracteres (incluidos los espacios).

Los SMS también permiten recibir notificaciones de algún tema de interés: deportes, clima, cine, teatro, entre otros.

Los mensajes enviados son recibidos por un Centro de Servicio de Mensajes Cortos (*SMSC*) él cual le envía un mensaje al Registro de Localización Local[1] (*HLR*, *Home Location Register*) quien será el encargado de encontrar al cliente remitente. Si el cliente no está disponible el *HLR* conservará el mensaje durante algún periodo de tiempo e intentará volver a enviar el mensaje, si el cliente está disponible el *HLR* le enviará una notificación al *SMSC* el cual clasificara el mensaje como "enviado" y no intentará enviarlo de nuevo.

1.3.5. Mensajería instantánea (*IM*, *Instant Messaging*)

Es un servicio de comunicaciones a través de Internet utilizando una ventana privada entre dos o más personas basadas en texto plano o acompañados de iconos o *emoticons* con la finalidad de poder entablar una comunicación en tiempo real y para esto es necesario iniciar sesión, es decir, el usuario debe identificarse con su nombre de usuario o correo electrónico y su contraseña.

Entre los servicios que ofrece el *IM* es el "aviso de presencia", el cual indica; cuando una persona (dentro de la lista de contactos del usuario) se conecta, su estado de conexión y si quiere mantener una conversación con él.

Otro de los servicios que ofrece la mensajería instantánea es la capacidad de poder compartir archivos como son: imágenes, audio, y video, además de poder tener conversaciones de voz, *webcam*, videoconferencias e incluso juegos en línea entre usuarios.

Algunos mensajeros permiten dejar mensajes aunque la otra persona no esté conectada, lo cual posibilita ver el mensaje en el momento en que se inicie sesión. Entre los mensajeros más utilizados se encuentran:

- Google Talk: Programa gratuito de Google que permite llamar o enviar mensajes instantáneos gratuitos. Para poder utilizarlo se necesita una cuenta de correo Gmail.
- Yahoo Messenger: Programa gratuito de Yahoo que permite conversaciones de texto, voz y video, además llamadas internacionales gratuitas de PC a PC. Para poder utilizarlo se necesita una cuenta de Yahoo.
- Skype: Programa que permite mantener conversaciones no sólo a través de texto, sino también hablar con otros usuarios de Skype de forma gratuita, llamadas a teléfonos fijos y móviles de cualquier lugar del mundo por un precio reducido.

Al hablar de los entornos de comunicación se puede observar que un servicio que tienen en común la mayoría de ellos es el correo electrónico, pues gracias a él podrá recibir las preguntas, respuestas, novedades y notificaciones que hagan en dichos entornos y de esta forma mantenerse actualizado con sus temas de interés.

1.4. Antecedentes de las redes de computadoras

El primer intento de establecer una red de comunicaciones a nivel nacional surge a principios del siglo XIX al crearse el telégrafo óptico (parecidos a los molinos), el cual estaba conformado por unas torres con una serie de brazos que codificaban la información dependiendo su posición. Estas redes permanecieron hasta mediados del siglo, pues fueron sustituidas por el telégrafo. La red telegráfica y la red telefónica fueron los principales medios de transmisión de datos a nivel mundial.

En los años 60 se establece la conmutación de paquetes, el cual, es un método de fragmentar los mensajes en partes más pequeñas, encaminarlas hacia su destino y unirlas cuando lleguen a éste.

[1] HLR: Base de datos de todos los números de teléfono móvil en una red *GSM*.

Los primeros experimentos de la red de conmutación de paquetes surgieron en Reino Unido (*National Physics Laboratories*) y en Francia (*Societé Internationale de Telecommunications Aeronautiques*). Fue en el año de 1957 cuando esta tecnología llego a los Estados Unidos creando un organismo afiliado al Departamento de Defensa para impulsar el desarrollo tecnológico denominado ARPA (*Advaced Research Projects Agency*) quien busco crear un sistema de redes de comunicaciones que siguiera funcionando pese a que un punto de la red fuera destruido ya que la comunicación podía encaminarse a través de otra ruta naciendo así, el ARPANET.

Es en la década de 1970, cuando ARPANET realiza su primer conexión a través de todo el país instalada por AT&T entre la Universidad de California (UCLA) y la empresa Bolt Beranek and Newman, Inc. (BBN). El principal obstáculo con el que se encontró el desarrollo de la red fue la interconexión de las computadoras debido a que eran provenientes de diferentes creadores y, por lo tanto, cada una de ellas tenía diferentes sistemas de comunicación. Esto se resolvió con la estandarización de los protocolos de comunicación, surgiendo así, dos años después, el protocolo TCP/IP.

Poco a poco, ARPANET fue creciendo y más centros de investigación se fueron inscribiendo a la nueva red de comunicación. Así, en 1971 nació el primer programa de correo electrónico, mientras que en 1972 surgió la nomenclatura arroba (@). Aproximadamente en el año 1973, alrededor del 75 % del tráfico de ARPANET estaba basado en correos electrónicos.

En 1980 el Departamento de Defensa de los Estados Unidos adopta el protocolo TCP/IP para la conexión de redes.

En 1983, ARPA decide que todas las redes que busquen conectarse a ARPANET deben estar bajo el estándar TCP/IP y éste, al ser disponible y sin costo, permitió la conexión global de las redes sin tener inconvenientes al momento de comunicarse entre ellas.

En 1984 se crean los dominios *gov*, *mil*, *edu*, *com*, *org* y *net* así como los sufijos geográficos.

En 1989 la WWW (*World Wide Web*, Red Informática Mundial) conocida también como web, se originó en el CERN (Centro Europeo para la Investigación Nuclear) ubicado en Ginebra (Suiza), por Tim Berners-Lee.

Así, en 1990, ARPANET deja de existir ya que la red pasó de ser una red gubernamental a una red pública al contar con más de 100, 000 equipos conectados a Internet. Esto y la dispersión del protocolo TCP/IP sentó las bases del Internet actual. Se puede decir, por tanto, que Internet le debe a ARPANET su existencia.

Fue en 1991 cuando la *web* hizo su debut al brindar instantáneamente orden y claridad al caos dentro del mundo informático al facilitar la búsqueda de información y permitiendo elegir el tipo de contenidos al que se quiere acceder como: texto, gráficos, vídeo, sonido entre otros. A partir de ese momento, Internet y la *web* crecieron de manera inesperada, al estimarse en el 2011 existen más de 2 mil millones de usuarios del Internet en el mundo y cerca de 35 millones en México.

El asombroso crecimiento que ha tenido Internet en los últimos años se ha debido, primordialmente, a la aparición de una herramienta que por facilidad de manejo y potencialidades, ha cautivado a un gran número de usuarios no necesariamente adentrados en el mundo computacional.

Es así como las redes de computadoras han cambiado la forma de comunicación de la sociedad actual, cuyo objetivo principal es el intercambio de datos. Las ventajas, beneficios y usos de éstas son muchas y dependerán en gran medida de las aplicaciones que se ejecuten sobre ellas.

1.5. Definición de red de computadoras

Una red está formada por dos o más computadoras conectadas entre sí formando una red con el propósito de compartir recursos, servicios e información, de manera segura, eficiente y confiable. Esto se puede lograr a través de un enlace físico o lógico.

Para que esta comunicación exista se necesita de dos componentes principalmente:

1. Conexión física (*hardware*) que se establecen mediante conectores y cables.
2. Conexión lógica (*software*) mediante programas utilizados para gestionar los equipos y el sistema operativo.

1.6. Componentes de una red

Como se mencionó anteriormente, una red de computadoras está conformada por varios componentes con funciones específicas tanto de *hardware* como de *software*. Dichos componentes se pueden agrupar en cuatro categorías principales:

1. Nodo: Dispositivos cuya función es la transferencia de datos, es decir, enviar y recibir mensajes a través de la red. Por ejemplo, computadoras personales e impresoras conectadas a la red.
2. Periféricos compartidos: Son dispositivos de almacenamiento ligados al servidor, como son: las unidades de discos ópticos, las impresoras, escáner, equipos de respaldo, impresoras y el resto de equipos que puedan ser utilizados por cualquiera en la red.
3. Dispositivos de red: Son aquellos que mueven y controlan el tráfico de la red. Por ejemplo, *hubs*, *routers*, *switches*, entre otros.
4. Medios de red como son los cables de cobre o la fibra óptica ya que proporcionan la conexión entre los *hosts* y los dispositivos de red.

1.7. Elementos fundamentales de las redes

Hay varios criterios por los que se pueden clasificar las redes de computadoras, según su tecnología, su tamaño, su topología, entre otros.

1.7.1. Tipos de redes

Según su tamaño, se pueden distinguir varios tipos de redes en función de su extensión:

- PAN (*Personal Area Networks*). Interconexión de dispositivos en el entorno usuario. Los dispositivos pueden o no pertenecer a la persona en cuestión. Llega a cubrir unos cuantos metros y puede estar conformada por no más de 8 equipos. Actualmente existen diversas tecnologías que permiten su desarrollo, entre ellas se encuentran la tecnología inalámbrica *Bluetooth* o las tecnologías de infrarrojos.
- LAN (*Local Area Network*). Conjunto de elementos físicos y lógicos conectados dentro de un mismo edificio.
- CAN (*Campus Area Network*). Colección de LANs que se encuentran en edificios diferentes dentro de un campus (universidad, oficinas de gobierno, maquilas o industrias).
- MAN (*Metropolitan Area Network*). Red de distribución de datos que se extienden sobre áreas geográficas de tipo urbano, como una ciudad.
- WAN (Wide Area Network). Red que intercomunica equipos en un área geográfica muy extensa, es decir, en edificios del mismo o diferente país.

1.7.2. Topología

Es el arreglo físico o lógico en el cual los dispositivos o nodos de una red (computadoras, impresoras, servidores, *hubs*, *switches*, *routers*, por mencionar algunos), se interconectan entre sí mediante un medio de comunicación.

Su objetivo es:

Buscar la forma más económica y eficaz de conectar los dispositivos para facilitar la funcionalidad del sistema.

- Evitar el tiempo de espera en la transmisión de datos.
- Permitir un mejor control y administración de la red.
- Permitir el aumento óptimo de equipos en la red.

Existen dos tipos de topologías: físicas y lógicas.

1.7.2.1. Topología Física

Se refiere al diseño en la que los dispositivos de la red están interconectados entre sí.

A continuación se describirán cada una de las topologías físicas.

- Topología tipo estrella: Red de comunicaciones en la cual, los cables de todas las computadoras son conectados a un dispositivo central (*hub* o *switch*). Los datos de una computadora son transmitidos por el dispositivo central al resto de las computadoras en red, dicho dispositivo controla el tráfico de datos por la red, reenviando los datos a su destino [14].

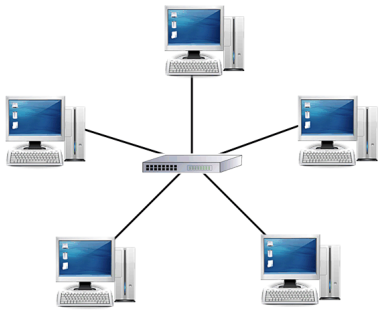


Figura 1.1: Topología tipo estrella

- Topología tipo bus: Todas las computadoras están conectadas directamente a un canal de comunicaciones común llamado *bus* o *backbone*.

  La información que se envía al bus llega a todos los nodos conectados, por tanto, cuando un nodo envía información al *bus* todos los demás nodos de la red pueden ver dicha información [14].

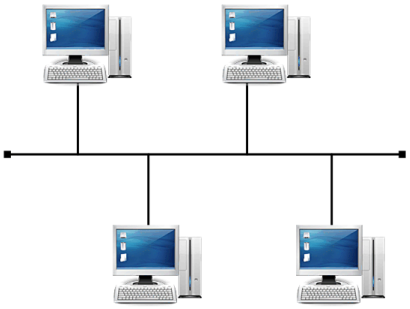


Figura 1.2: Topología tipo bus

- Topología tipo anillo: Conjunto de computadoras conectadas mediante enlaces punto a punto formando un círculo a través de un mismo cable por el cual viaja la información [14].

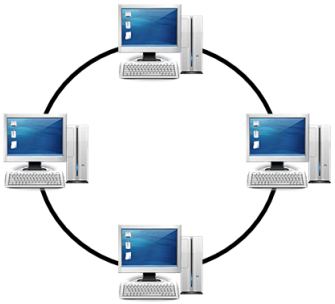


Figura 1.3: Topología tipo anillo

- Topología tipo árbol: Topología en la cual la mayoría de los nodos están conectados a concentradores secundarios que, a su vez, se conecta al concentrador central (*hub* o *switch*) [14].

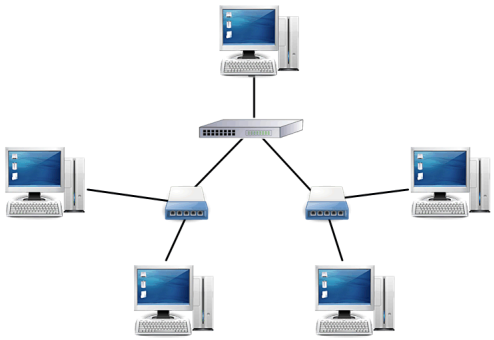


Figura 1.4: Topología tipo árbol

- Topología tipo malla: Topología en la cual cada nodo está conectado a todos los demás, mediante cables separados, de forma que los datos pueden viajar del nodo origen al destino siguiendo distintas rutas. La información es enviada exclusivamente a los dispositivos que se encuentran conectados eliminando así las colisiones e interferencias que pueden producirse cuando la información es compartida por varios dispositivos [14].

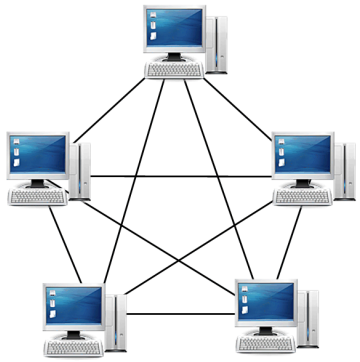


Figura 1.5: Topología tipo malla

Después de haber definido cada una de las topologías físicas, ahora se definirán las topologías lógicas, las cuales son las siguientes:

1.7.2.2. Topología Lógica

Forma en la que los datos acceden al medio de comunicación y la determina el protocolo de comunicación.

Topología *broadcast*. (Ethernet).Topología en la cual las estaciones de la red reciben todos los paquetes transmitidos, posteriormente, cada estación debe analizar si el paquete debe ser aceptado, rechazado o reenviado.

Transmisión de *Tokens*. Es aquella que controla el acceso a la red al transmitir un *token* electrónico de forma secuencial a cada *host*. Cuando éste recibe un *token*, puede enviar datos a través de la red. Si dicho *host* no tiene ningún dato para enviar, transmite el *token* al siguiente *host* y el proceso se vuelve a repetir.

1.8. Modelos de Referencia

Un modelo es aquel que establece una forma de construcción de protocolos con el fin de acoplar equipos de diferentes fabricantes [14]. Los más importantes en la actualidad son el modelo OSI y el TCP/IP. Éstos están

formados por capas o niveles ordenados de manera jerárquica creando así una pila de protocolos, la cual divide la información en subconjuntos más simples, reduciendo así la complejidad de la comunicación.

A continuación se hablará sobre cada uno de estos modelos.

1.8.1. Modelo de referencia OSI

Debido a la diversidad de las redes (creadas por diferentes fabricantes causando incompatibilidad entre ellas) la Organización Internacional para la Estandarización (*ISO*, *International Standard Organization*) empezó a desarrollar en 1977 un conjunto de normas que fueran comunes dentro de las redes, permitiendo así la comunicación entre equipos de diferentes fabricantes, naciendo así en 1983 el Modelo de Referencia de Interconexión de sistemas abiertos (*OSI* ,*Open System Interconection*) siendo estandarizado en 1984.

El Modelo OSI define una arquitectura formada por siete capas, las cuales se encargaran de descomponer el proceso de la comunicación en varios problemas más sencillos, de manera que cada capa resolverá un problema en específico.

Las siete capas del Modelo OSI son:

1. Física: define la transmisión de bits por un canal de comunicación para establecer y mantener la conexión física, sin importarle el significado o la estructura de los bits.
2. Enlace: controla la capa física activándola, manteniéndola y desactivándola, además de proveer los mecanismos necesarios para que la comunicación entre dos equipos sea confiable. Controla si se van a producir errores (datos dañados, perdidos o duplicados) y los corrige.
3. Red: encamina los paquetes hacia su destino buscando para ello la mejor ruta, además de encargarse de los problemas concernientes al control de flujo y control de congestionamiento.
4. Transporte: provee un mecanismo confiable para el intercambio de datos entre procesos en diferentes equipos, además de encargarse de segmentar y reensamblar los bloques de información.
5. Sesión: Organiza las funciones que permiten que dos usuarios se comuniquen a través de la red. Además de establecer, administrar y finalizar las conexiones entre aplicaciones locales y remotas.
6. Presentación: proporciona la sintaxis de los datos intercambiados entre los procesos, además de sus dos principales formatos que son cifrado y comprensión.
7. Aplicación: proporciona la interfaz al usuario para la realización de diferentes tareas.

Las capas inferiores (Física, Enlace de datos, y Red), lidian con las señales eléctricas, trozos de datos binarios y encaminamiento de paquetes a través de las redes.

Las capas superiores (Transporte, Sesión Presentación y Aplicación), se encargan de la gestión de las soluciones de los clientes, respuestas de los servidores, representación de los datos y los protocolos de redes desde el punto de vista del usuario.

1.8.2. Modelo de referencia TCP/IP

El modelo TCP/IP hace referencia a dos de los protocolos más importantes dentro de la familia de protocolos: el Protocolo de Control de Transmisión (TCP, *Transmission Control Protocol*) y el Protocolo de Internet (IP, *Internet Protocol*). Este modelo permite la comunicación entre diferentes computadoras con distinto sistema operativo sobre redes de área local (LAN) o redes de área extensa (WAN).

El TCP se encarga de fragmentar y unir los paquetes mientras que el IP hace llegar los fragmentos de información a su destino correcto.

El modelo TCP/IP se impuso sobre OSI al simplificar su esquema, basándose solo en cuatro capas.

Las cuatro capas son:

1. Interfaz de red: Controla los dispositivos de *hardware*. Encapsula los datos y específica la forma en cómo deben enrutarse hacía una red específica asignándole una dirección IP a las direcciones físicas.
2. Internet: Administra los *datagramas*, los desencapsula y selecciona la ruta más conveniente para su envío evitando así problemas de congestionamiento.
3. Transporte: Permite la comunicación entre un programa de aplicación a otro a través de los puertos, regula la información y provee un transporte confiable por donde viajan los paquetes de datos verificando así que éstos lleguen en la secuencia correcta y sin errores (retransmite datos perdidos y comprueba que los datos hayan llegado a su destino).
4. Aplicación: Ofrece la interfaz al usuario para que pueda utilizar las aplicaciones de Internet.

1.9. Principales protocolos

Un protocolo es un conjunto de reglas y procedimientos que deben seguir los equipos para poder enviar y recibir información a través de la red.

Los dos protocolos de red más importantes son:

- El protocolo TCP
- El protocolo IP

1.9.1. Protocolo TCP

El TCP (*Transmission Control Protocol*, Protocolo de Control de Transmisión) es un protocolo orientado a conexión, su objetivo principal es entregar los datagramas a su destino sin errores ni duplicados, entregando los datos en el mismo orden en que fueron enviados. En caso de que existan errores en la transmisión o se pierdan los datos el protocolo TCP reenvía la información.

Entre las características que tiene el protocolo TCP se encuentran:

- Orientado a conexión. Se debe de establecer la conexión antes de la transferencia de datos. Los equipos emisor/receptor se sincronizan para lograr el envío y la recepción de los datagramas.
- *Full Duplex*. Cada extremo de la conexión TCP consta de dos enlaces lógicos: uno de entrada y otro de salida. La cabecera TCP contiene el número de secuencia de los datos de salida así como de los datos de entrada.
- Fiable. Los datos se numeran en secuencia y se espera a que el receptor los reconozca, en caso de no reconocerlos, los datos se vuelven a transmitir. El receptor descarta los datos duplicados y los acomoda en el orden correcto independientemente de la secuencia en la que hayan llegado. Todos los segmentos transmitidos utilizan un código detector (*CRC* o suma de control) que verifica la integridad de la información.
- Flujo de bytes. Son los datos que se envían por los canales de entrada y salida. El número de secuencia y de reconocimiento de datos van definidos en las cabeceras TCP.
- Control de flujo en los extremos. El TCP implementa un control de flujo en el emisor para regular la cantidad de datos enviados, así como en el receptor para indicar cuanto espacio hay disponible en el *buffer*, evitando así transmisiones excesivas por parte del primero y la incapacidad de almacenamiento por parte del segundo.
- Segmentación de datos de aplicación. Los extremos negocian el tamaño máximo de los paquetes, segmentándolos y ajustándolos a un tamaño conveniente.

- Transmisión uno a uno. Se buscan enlaces libres y se establece un círculo virtual punto a punto, a esto se le conoce como *stream* o corriente de datos.

Para garantizar que no se pierdan los datos, el protocolo TCP consta de tres etapas:

- Establecimiento de la conexión: Las máquinas emisora y receptora establecen los parámetros necesarios para el intercambio de la información (el número de secuencia, tamaño del *buffer*, entre otros) [13].
- Transferencia de datos: La información viaja en ambos sentidos (bidireccional); se detectan y corrigen errores, se controla el flujo y la congestión de información [13].
- Cierre de conexión: Al terminar el envío y recepción de datos, la comunicación puede ser finalizada por cualquiera de las dos partes [13].

TCP utiliza los puertos para el acceso de diferente información, de esta forma la máquina cliente selecciona el puerto correspondiente a la aplicación deseada dentro de la máquina del servidor.

1.9.2. Protocolo IP

El IP (*Internet Protocol*, Protocolo Internet) es un protocolo no orientado a conexión. Su principal objetivo es transmitir los datagramas (también llamados paquetes) a través de las redes desde su origen a su destino, asignando a cada equipo un número único que le sirve como identificador dentro de la red.

Los datagramas atraviesan diferentes redes cuando viajan de un equipo a otro. El tamaño de los datagramas varía de una red a otra dependiendo del medio físico que se esté utilizando para la transmisión. A este tamaño se le conoce como MTU (*Maximum Transmission Unit*, Unidad Máxima de Transmisión), no puede transmitir un paquete con una longitud que exceda al MTU establecido en la red. En caso de que los datagramas superen el MTU establecido en la red, los paquetes serán fragmentados y posteriormente, cuando lleguen a su destino, se volverán a ensamblar.

Este protocolo no garantiza si un paquete llega o no a su destino, si llegan en el orden correcto, llegan dañados o si existen duplicados.

Los paquetes poseen una cabecera con la información de origen y destino (direcciones IP). Esta información es utilizada por los *routers* o *switches* para determinar el camino por el cual van a enviar los paquetes. Cada datagrama puede ser enviado por rutas diferentes, dependiendo de la congestión que exista en la red.

Las direcciones IP están estructuradas en cuatro octetos (32 bits) separados por un punto. Una dirección empieza con un número de red denominada *netID* (identificador de red) seguida de una dirección local denominada *host-ID* (identificador de host). Existen tres clases de direcciones Internet:

1. Clase A: El bit más significativo es el 0, los 7 bits siguientes son la red y los últimos 24 bits pertenecen a la dirección local.
2. Clase B: Los bits más significativos son uno-cero (10), los 14 bits siguientes son la red y los últimos 16 bits pertenecen a la dirección local.
3. Clase C: Los bits más significativos son uno-uno-cero (110), los 21 bits siguientes son la red y los últimos 8 bits pertenecen a la dirección local.

Existen otras dos clases que son poco utilizadas. La clase D y la clase E.

- Clase D: Utilizada para multicast. Los bits más significativos son uno-uno-uno-uno (1111), los 28 bits siguientes se utilizan para identificar al multicast al que va dirigido.
- Clase E: Utilizada únicamente para propósitos experimentales. Los bits más significativos son uno-uno-uno-uno (1111), los 28 bits siguientes se utilizan para identificar al multicast al que va dirigido.

En la tabla siguiente se puede observar más información sobre las clases de red [13, 14].

Clase	Rango del primer octeto	Número de Redes	Máscara de Red	Número de Host por red	Broadcast ID
A	1-126	126	255.0.0.0	16777216	x.255.255.255
B	128-191	16384	255.255.0.0	65534	x.x.255.255
C	192-223	2097152	255.255.255.0	254	x.x.x.255
D	224-239	-	-	-	-
E	240-255	-	-	-	-

Tabla 1.1: Información básica de las cinco clases de redes

Existen direcciones reservadas, entre las más importantes se encuentran:

- La dirección 0.0.0.0 se utiliza para identificación local (cuando el equipo no tiene asignada ninguna dirección IP)
- La dirección 127.x.x.x es la dirección de la propia máquina, se le llama dirección de bucle local o *loopback*.

1.10. Puertos lógicos

Un puerto es un número de 16 bits (de 0 a 65535) asignado a las conexiones tanto la de origen como la de destino, identificando así el proceso que se está llevando a cabo entre los equipos, de esta forma la máquina destino sabrá a qué aplicación entregará los datos recibidos.

La asignación de puertos permite a un equipo establecer diversas conexiones al mismo tiempo con máquinas distintas, pese a que todos los paquetes recibidos tienen la misma dirección, van dirigidos a puertos diferentes.

Los puertos no son asignados de manera aleatoria. La encargada de asignar los puertos a los protocolos, programas y aplicaciones además de las direcciones IP, es la entidad IANA (*Internet Assigned Numbers Authority*, Autoridad de Asignación de Números en Internet). La IANA clasifica los puertos en tres categorías:

1. Puertos bien conocidos (0 - 1023). Puertos reservados para los servicios de red conocidos (POP3, HTTP, SMTP, DNS, entre otros). Si se esta programando un *socket* y se le indica que se usara el puerto 0, el Sistema Operativo le asignara, automáticamente, un puerto libre.
2. Puertos registrados (1024 - 49151). Puertos que pueden ser utilizados por cualquier aplicación
3. Puertos dinámicos o privados (49152 - 65535). Puertos que se asignan de manera dinámica a las aplicaciones de los clientes al iniciar la conexión. Son poco usados.

El estado de un puerto puede ser:

- Abierto. El puerto acepta conexiones: Existe la posibilidad de acceder al puerto
- Cerrado. El puerto rechaza la conexión: No hay acceso al puerto.
- Bloqueado o Sigiloso. No hay respuesta: No se sabe si el equipo está conectado (estado ideal).

Entre los puertos bien conocidos más utilizados se encuentran [23]:

Puerto	Servicio
Puerto 21	FTP
Puerto 22	SSH
Puerto 23	Telnet
Puerto 25	SMTP
Puerto 53	DNS
Puerto 80	HTTP
Puerto 110	POP3
Puerto 143	IMAP
Puerto 443	SHTTP
Puerto 993	IMAP sobre SSL
Puerto 995	POP3 sobre SSL

Tabla 1.2: Puertos conocidos y el servicio que ofrecen

Hablando del modelo cliente/servidor, el servidor cuenta con los puertos bien conocidos (puertos fijos a los cuales se acceden para brindar el servicio) mientras que el cliente elige los puertos que estén disponibles (no incluye los puertos bien conocidos).

1.11. Medios de transmisión

Un medio de transmisión es un canal eléctrico u óptico por el cual es posible la transferencia de información a través de señales (ondas electromagnéticas) las cuales viajan desde el emisor al receptor. Este medio de comunicación puede ser un par de cables o inclusive el mismo aire. No importa el medio que se utilice, en la transmisión se puede encontrar factores importantes como: el ruido, la interferencia, entre otros, que impidan que la señal se propague correctamente.

Las características y parámetros más significativos que tienen los medios de transmisión son:

- Ancho de banda
- Longitud
- Seguridad
- Instalación sencilla
- Costo
- Fiabilidad en la transferencia de la comunicación

Los medios de transmisión se clasifican en guiados y no guiados. En ambos casos la transmisión se realiza mediante ondas electromagnéticas.

1.11.1. Medios de transmisión guiados

Son los medios que utilizan un cable para trasmitir la comunicación. El cable se encarga de conducir las señales desde un extremo a otro.

Entre los cables que se utilizan para conectar los equipos se encuentran:

- Par trenzado: Consiste en dos alambres de cobre cubiertos por plástico, trenzados entre sí y forrados en un revestimiento protector, formando así un cable. En cada par, un alambre sirve para enviar la señal de receptor mientras que el otro funciona como tierra. El trenzado permite bloquear el ruido y la interferencia del exterior [10].

- Cable coaxial: Consiste de un alambre de cobre duro, cuya parte central está forrado con material aislante y como segundo conductor, lleva una cubierta cilíndrica metálica en forma de malla o tejido trenzado, el cual está cubierto por otro forro aislante siendo así la funda del cable. La funda evita que las señales de otros cables o la radiación electromagnética afecte la información conducida a través del cable [10].

- Fibra óptica: Consiste en un núcleo que está formado por un conjunto de fibras o hilos muy finos de vidrio o plástico, a través de los cuales viaja la luz. El núcleo es rodeado de un revestimiento de cristal o plástico que será el que refleje la luz de vuelta al núcleo siguiendo una trayectoria en zigzag (funcionando como espejos), permitiendo así que la luz viaje por largas distancias. Este revestimiento se encuentra protegido por una cubierta externa de plástico resistente que cubre las fibras para protegerlas de la humedad y el entorno, haciéndola casi inmune al ruido y a la radiación electromagnética [10].

1.11.2. Medios de transmisión no guiados

Son los medios que no utilizan un conductor físico para comunicarse, ya que viajan a través del medio (aire o vacío). La transmisión y recepción de las señales se realiza por medio de antenas. Al momento de la transmisión, la antena irradia las señales en el medio, mientras que en la recepción la antena capta las señales del medio que la rodea.

Algunas de las formas de transmitir señales a través de medios no guiados son:

- Ondas de radio. Son ondas que se propagan en cualquier dirección (omnidireccionales), por lo tanto no requieren antenas parabólicas para la transmisión y recepción de las señales. Este tipo de ondas es menos sensible a la atenuación producida por la lluvia.

- Microondas. Ondas que viajan en línea recta (las antenas emisoras y receptoras deben estar cuidadosamente alineadas) con una frecuencia comprendida entre 1 y 40 GHz. A mayor frecuencia mayor es su ancho de banda, es decir, la velocidad que puede alcanzar la transmisión. La atenuación de este tipo de ondas aumenta con la lluvia y grandes cantidades de agua [10].

- Infrarrojos. Ondas que viajan en línea recta a corta distancia, este tipo de ondas no pueden atravesar superficies sólidas.

1.12. Arquitectura cliente/servidor

Arquitectura que implica la relación entre procesos que solicitan servicios (clientes) y procesos que los proporcionan (servidores). El servidor espera permanentemente a que el cliente le haga una petición, cuando el cliente genera la petición, el servidor la recibe, la procesa y le envía la información o la respuesta al cliente que lo solicitó.

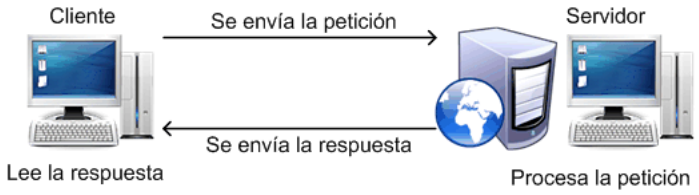


Figura 1.6: Modelo Cliente/Servidor

Por lo general, el término cliente/servidor se utiliza cuando los clientes se ubican en sitios diferentes al servidor, aunque esta definición también se puede utilizar cuando los clientes y el servidor estén dentro del mismo equipo.

1.12.1. Definición de cliente

El cliente es la estación de trabajo que solicita un servicio al servidor mediante su dirección IP y el puerto, el cual está reservado para un servicio en particular. Es a través de estos dos elementos que el servidor puede hacerle llegar la respuesta al cliente.

El proceso del cliente:

- Abre el canal de comunicación para acceder a la dirección de red atendida por el servidor.
- Le envía al servidor un mensaje de petición de servicio mediante su dirección IP y el puerto reservado para dicho servicio y espera hasta recibir respuesta.
- Si la obtiene hace uso del servicio, posteriormente proceder a cerrar el canal de comunicación y terminar la ejecución del proceso.

1.12.2. Definición de servidor

El servidor es el equipo encargado de atender las peticiones hechas por los clientes.

Los servidores pueden ser de varios tipos, entre ellos se encuentran los siguientes:

- Servidor de archivos. Mantiene los archivos en subdirectorios, los cuales son compartidos y almacenados para los usuarios de la red.
- Servidor de impresión. Tiene conectada una impresora a la red, la cual es compartida con los demás usuarios.
- Servidor de correo electrónico. Almacena, envía, recibe, y realiza otras operaciones para proporcionar servicios de Email para los clientes de la red.
- Servidor *web*. Proporciona un lugar para guardar y administrar documentos HTML (son documentos a modo de archivos con formato especial) que pueden ser accesibles por los usuarios de la red a través de navegadores.
- Servidor FTP. Utilizado para guardar archivos que puedan ser descargados por los usuarios dentro de la red.
- Servidor Proxy. Se utiliza para monitorear y controlar el acceso entre las redes, actuando como intermediario para que el servidor que recibe una petición no sepa verdaderamente quien es el que está detrás de ésta.

El proceso del servidor:

- Abre el canal de comunicación e informa a la red la dirección a la que responderá con disposición para aceptar peticiones a determinado servicio.
- Espera la petición del cliente a través del puerto y la IP otorgada a la red.
- Al recibir la petición atiende al cliente.
- Finalmente cierra la conexión.

Entre las principales características de la Arquitectura Cliente/Servidor, se encuentran las siguientes:

- El servidor muestra a todos sus clientes una interfaz única y bien definida.
- Las tareas del cliente y del servidor no utilizan los mismos recursos de cómputo, como velocidad del procesador, memoria, capacidad y velocidad del disco, entre otros.
- El cliente no depende de la localización física del servidor ni de su sistema operativo.

- Los cambios en el servidor involucran pocos o ningún cambio en el cliente.
- La relación que se establece, del servidor al cliente, puede ser de:
  - Uno a uno: El servidor atiende a los clientes uno detrás de otro (servidor iterativo).
  - Uno a muchos: El servidor atiende a varios clientes al mismo tiempo (servidor concurrente).

Los clientes corresponden a procesos activos (realizan peticiones de servicios a los servidores) y los servidores a procesos pasivos (esperan las peticiones de los clientes).

Capítulo 2

Correo Electrónico

2.1. Definición de correo electrónico

El correo electrónico o Email (*Electronic mail*) es un servicio a través de Internet mediante el protocolo SMTP (*Simple Mail Transfer Protocol*) que permite mandar y recibir mensajes a múltiples destinatarios o receptores que se encuentren en cualquier parte del mundo utilizando una computadora o un dispositivo afín. Estos mensajes pueden contener documentos adjuntos en diferentes formatos como: textos, gráficos, audio, entre otros.

El funcionamiento del Email es muy parecido al correo postal, ambos permiten el envió e intercambio de mensajes que llegan a su destino a través de una dirección con la diferencia de que el correo electrónico no necesita de una persona física para que entregue el mensaje, éste viaja a través de la red, de un servidor a otro. Los servidores que reciben el mensaje, comprueban la dirección y lo encaminan a la ruta correcta, repitiendo este proceso hasta que llegue al servidor destino, donde el mensaje será almacenado temporalmente en el buzón del destinatario hasta que éste lo revise.

El tiempo de espera para recibir un mensaje es relativo, puede tardar algunos segundos o incluso minutos, en raras ocasiones pueden llegar a tardar hasta un día, dependiendo del funcionamiento del servidor.

2.1.1. Estructura

La estructura de un Email se compone de dos partes fundamentales: encabezado y cuerpo del mensaje.

1. Encabezado (*mail header*): Esta parte contiene la dirección del remitente y del receptor (o receptores), la fecha y la hora de envío y el tema del mensaje.

   Los campos dentro del encabezado son los siguientes:

Figura 2.1: Encabezado del remitente bajo el cliente Hotmail

   - Para (*To*): En este campo se agrega la dirección de correo del quien recibirá el mensaje (receptor o receptores sea el caso).
   - Con Copia (*CC*): En este campo se agregan las direcciones de correo a quienes se les quiere hacer llegar una copia del mensaje, además del destinatario principal.

- Con Copia oculta (*CCo*): En este campo se pondrán las direcciones de correo a quienes se les quiere hacer llegar una copia del mensaje, además del destinatario principal, sin que los destinatarios anexos visualicen a quiénes más va dirigido el mensaje.
- Asunto (*Subject*): En este campo se agrega una breve explicación sobre el contenido o tema del mensaje.

Cuando se recibe un correo, el encabezado cambia, mostrando los siguientes campos:

Figura 2.2: Encabezado al recibir un mensaje bajo el cliente Hotmail

- Para (*From*): Este campo indica la dirección del remitente.
- Enviado el (*Sent*): Este campo indica el día, mes, año y hora en que fue enviado el mensaje.
- A (*To*): Este campo indica la dirección del destinatario.

2. Cuerpo (*mail body*): En este campo se escribe el contenido del mensaje y, dependiendo del cliente de correo que se utilice, se le puede dar formato al texto, cambiarle el color, agregar hipervínculos, imágenes, archivos adjuntos, entre otros.

Figura 2.3: Cuerpo del mensaje bajo el cliente Hotmail

2.1.2. Componentes de una dirección de correo electrónico

Para poder acceder al correo electrónico y contar con los servicios que éste ofrece es necesario que el usuario tenga una dirección de correo, la cual está formada por tres elementos principales:

1. Identificador del usuario: Indica el alias del usuario designado por el mismo. El alias sólo puede ser conformado por letras, números, puntos, guiones (alto y bajo). Si el nombre elegido ya existe, el servidor proporciona alternativas disponibles con cierta semejanza con el nombre original (no hay problema si el mismo nombre de usuario existe en otro servidor).

   *usuario@**hotmail**.com* y *usuario@**gmail**.com*

2. Signo @ (arroba): Se utiliza para separar el alias de la dirección del servidor. En 1971 el ingeniero Ray Tomlinson fue el primero en enviar un mensaje utilizando el símbolo @. Este símbolo estaba disponible en los teclados y no era usado en nombres propios, en cambio los signos como: corchetes, paréntesis, comas, entre otros, ya eran utilizados por el sistema para otros fines. En inglés el @ se pronuncia como at que significa "en" o "pertenece a".

3. Dominio o dirección del servidor: Hace referencia al servidor donde se encuentra la cuenta de correo. El servidor es administrado por el proveedor del servicio de correo electrónico.

   Todo lo que esté del lado derecho del símbolo arroba serán subdominios, que serán separados por puntos. Al último subdominio se le conoce como *dominio de más alto nivel*.

   El dominio está compuesto por tres grupos principales:

a) La organización (nombre del Servidor de la Organización).

b) El tipo (característica que define la funcionalidad del dominio).

c) País donde se encuentra el servidor (especifica el punto geográfico del dominio).

Dentro de los dominios más utilizados se encuentran:

- *.com* - Proviene de "compañía o empresa". Utilizado por organizaciones comerciales con ánimo de lucro.
- *.net* - Proviene de "Internet". Reservados para sitio web relacionado con Internet, tecnología y telecomunicaciones, es decir, organizaciones dedicadas a la red.
- *.org* - Proviene de "organización". Utilizado por organizaciones e instituciones, establecimientos educativos, organizaciones sin fines de lucro, entre otros.
- *.gov* – Reservado para las entidades gubernamentales de los Estados Unidos.
- *.biz* - Proviene de "*business*" (negocio). Utilizado en sitio web con actividad comercial o cualquier tipo de negocio.
- *.info* - Proviene de "*information*" (información). Utilizados para sitios web de carácter informativo.
- *.name* - Proviene de "*personal name*" (nombre personal). Sitio web con referencia a un nombre personal.
- *.edu* - Uso exclusivo de Universidades.
- *.tv* - Viene de "*televition*". Sitios relacionados al mundo televisivo.

Sin embargo hoy en día cualquier usuario puede hacer uso de esta terminación sin entrar en las características antes mencionadas.

Entre los dominios que indican el país se encuentran:

- *ar* – Argentina
- *es* – España
- *fr* - Francia
- *it* – Italia
- *mx* – México uk – Reino Unido
- *uy* – Uruguay

Estos tres elementos le permiten al usuario ser identificado dentro de la red. Las direcciones de correo son únicas, esto se hace con el fin de evitar problemas de direccionamiento al momento de mandar o recibir mensajes.

A continuación se ejemplifica una dirección de correo electrónico con cada uno de sus componentes.

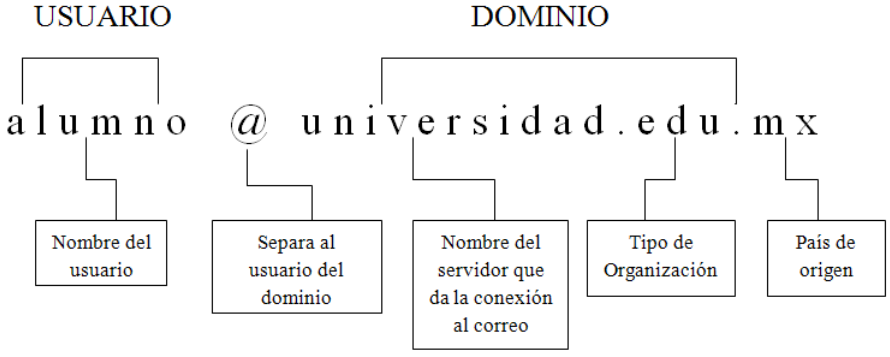


Figura 2.4: Componentes de una dirección de correo electrónico

2.1.3. Funciones

Las operaciones básicas son las acciones que se pueden hacer dentro de un correo electrónico. Las operaciones se muestran dependiendo de la situación del usuario, si va a redactar un nuevo mensaje o si lo recibió. A continuación se mostrarán las operaciones que aparecen en el correo electrónico cuando: se inicia sesión y se reenvía un mensaje.

- Las operaciones que aparecen cuando se inicia sesión son:
- Nuevo (*New*): Operación que permite crear un nuevo mensaje.
- Eliminar (*Delete*): Operación que permite borrar un mensaje visualizado o seleccionado.
- Correo no deseado (*Junk*): Operación que permite separar los mensajes "basura" o los que no se quieran recibir nuevamente, por ejemplo, la publicidad no solicitada (*spam*), sirviendo así, como filtro de mensajes.
- Limpiar: Operación que permite mover y/o eliminar todos los mensajes de una determinada cuenta, facilitando la administración de mensajes.
- Marcar como (*Mark as*): Operación que permite catalogar el mensaje como "leído", "no leído", "marcado", "sin marcar" y "phishing".
- Mover a (*Move to*): Operación que permite mover el mensaje a una carpeta en especial.
- Marca de seguimiento: Operación que indica que el usuario estará al pendiente de lo que pase con el mensaje.

Las operaciones que aparecen al recibir y modificar el mensaje son:

- Responder (*Reply*): Operación que permite enviar respuesta directa al remitente basado en el mensaje recibido. En el campo asunto automáticamente el servidor colocará "Re:" secundado del tema original.
- Responder a todos (*Reply to all*): Operación que permite enviar la respuesta a todos los usuarios que hayan sido incluidos dentro del mensaje recibido.
- Reenviar (*Forwarding*): Operación que permite enviar una copia del mensaje recibido a otros usuarios, señalando que el mensaje proviene del usuario actual. En el campo asunto automáticamente el servidor colocará "Rv" o "Fwd" secundado del tema original.
- Archivos adjuntos (*Attachments*): Operación que permite agregar archivos anexos al mensaje.

  Estos archivos pueden ser (por mencionar algunos):

  - Imágenes: JPG, GIF, PNG
  - Texto: DOC, TXT, PPT, PDF
  - Música: MP3, MP4, WAV
  - Video: DVD, AVI, FLV
  - Archivos .ZIP y .RAR
- Imprimir: Operación que permite imprimir el mensaje recibido.
- Archivar o Guardar (*Save draft*): Operación que permite almacenar el mensaje en el servidor sin que éste sea eliminado y acceder a él posteriormente.

2.1.4. Características

El correo electrónico posee varias características que lo hacen un medio eficaz, económico y accesible para los usuarios, resaltando así su superioridad sobre el correo tradicional.

Entre estas características se encuentran:

1. Velocidad. El tiempo que tarda en llegar un mensaje, desde que se envía hasta que se recibe, es casi instantáneo, independientemente de la localización geográfica de los usuarios, permitiendo una respuesta casi inmediata.

2. Económico. El servicio es gratuito, enviar un mensaje a un destinatario (independientemente de la distancia) no tiene costo alguno, sólo se paga el acceso a Internet.

3. Acceso. Contando con el equipo apropiado (computadora, teléfono, Internet, entre otros), se puede acceder al correo electrónico en cualquier parte del mundo y a cualquier hora del día.

4. Envío. El mensaje puede ser enviado al mismo tiempo a numerosos destinatarios.

5. Variedad de contenido. Como ya se ha mencionado en temas anteriores, el mensaje puede incluir texto, música, videos, imágenes, ejecutables, entre otros, además se puede cambiar el color, tamaño y la fuente de la letra, haciendo más vistoso el mensaje.

6. Capacidad. El correo electrónico puede transportar hasta 25Mb de información dentro de los archivos adjuntos, haciendo posible enviar una gran cantidad de archivos en un solo mensaje.

7. Clasificación de usuarios. El correo electrónico permite separar a los usuarios dentro de un grupo en específico, facilitando así el envío de mensajes con un tema de interés.

8. Gestión de mensajes. Los mensajes se pueden catalogar y almacenar dentro de una determinada carpeta, facilitando el acceso a ellos y reduciendo el tiempo de búsqueda.

9. Fácil manejo. El uso de una cuenta de correo no es difícil por lo que, con un poco de práctica, se puede aprender a utilizar este servicio.

10. Asíncrono. Para poder enviar o recibir un mensaje, los implicados no necesitan estar conectados simultáneamente, el correo será almacenado en el servidor donde el receptor podrá consultarlo cuando inicie sesión.

2.2. Tipos de agentes

Para el correcto funcionamiento de los sistemas de correo electrónico se necesitan de varias partes denominadas agentes. Estos agentes se dividen en tres clasificaciones, donde cada uno se responsabiliza de un determinado proceso de mover y administrar los mensajes del correo, de esta manera, se asegura que el mensaje llegue al destino correcto.

Estos agentes son:

MUA (Mail User Agent, Agente Usuario de Correo)

Este agente permite al usuario leer y redactar mensajes de correo (como mínimo), a través de una interfaz gráfica (Mozilla Mail, Ximina Evolution, Outlook, entre otros) o mediante una interfaz basada en texto (*Mutt Pine*, etc).

Algunos MUA son capaces de recuperar mensajes mediante los protocolos POP o IMAP configurando los buzones del correo para almacenar los mensajes entrantes y los mensajes salientes, enviándolos a un MTA.

MTA (Mail Transport Agent, Agente de Transporte de Correo)

Este agente se encarga de transferir los mensajes de correo electrónico entre las máquinas implicadas utilizando el protocolo SMTP. Los mensajes pueden pasar por diferentes MTA hasta llegar a su destino final. A este tipo de transferencia entre MTA se le denomina reenvío.

Ejemplos de MTA: Sendmai, Qmail, Postfix.

MDA (Mail Delivery Agent, Agente de Entrega de Correo)

Este agente es utilizado por el MTA y es el encargado de almacenar el correo electrónico en el buzón del usuario hasta que éste lo acepte. Este tipo de agente no transporta los mensajes entre sistemas ni le proporciona una interfaz al usuario.

Para enviar y recibir correos sólo son necesarios los agentes MTA y MUA, por lo que muchos usuarios no utilizan directamente los MDA.

Ejemplos de MDA: *bin/mail* y *Procmail*.

A continuación se muestra un ejemplo de cómo funcionan los agentes MUA, MTA y MDA al enviar un correo electrónico.

Figura 2.5: Funcionamiento de los agentes en el envío de un mensaje

2.3. Elementos

Para que un mensaje pueda enviarse y recibirse correctamente, el correo electrónico sigue reglas específicas para su adecuado funcionamiento. Estas reglas son conocidas como protocolos y son éstos los que se encargan de la transferencia (SMTP) y la entrega final de los mensajes (POP).

2.3.1. Transferencia de mensajes (SMTP, *Simple Mail Transfer Protocol*, Protocolo Simple de transferencia de correo electrónico)

Protocolo que se utiliza únicamente para el almacenamiento y la transferencia de correo electrónico entre servidores.

Cuando se manda un mensaje, el SMTP comprueba que exista un receptor con esa dirección, si es así, envía el mensaje al destinatario buscando la ruta más adecuada. Si el servidor del destinatario esta desconectado, el SMTP intentará establecer la conexión las veces que sea necesario hasta lograr el envío.

Este protocolo puede entregar mensajes a uno o más destinatarios.

2.3.1.1. Modelo SMTP

Para enviar un mensaje, el servidor SMTP (emisor) establece una conexión unidireccional (durante la conexión, el emisor puede enviar correos al receptor, pero el receptor no puede enviar correos al emisor) con el cliente SMTP (receptor).

El receptor debe de finalizar la conexión establecida y establecer otra en sentido contrario si quiere enviarle un correo al emisor, intercambiando así sus papeles.

Para lograr la conexión, el cliente genera comandos SMTP en formato ASCII y se los envía al servidor para que genere las respuestas a los dichos comandos.

Los pasos que sigue el modelo del SMTP son:

- El emisor SMTP establece la conexión con el receptor SMTP (siendo este el último destinatario o un intermediario) como respuesta a una solicitud de un usuario que envía un correo electrónico. El emisor manda al receptor el comando *HELO* y espera la respuesta.
- Al recibir la respuesta se establece el canal de transmisión. El emisor envía el comando *MAIL FROM* para identificarse, si el receptor puede aceptar el correo responderá con el comando *OK*.
- Se procede a identificar el destino del correo. El emisor envía el comando *RCPT TO*. Si el receptor acepta ese destino responde con el comando *OK*, en caso contrario rechaza el correo.
- Una vez acordado el destino, el emisor emite el comando *DATA* para informar al receptor que los datos que siguen a continuación son el mensaje, por lo que se envía el encabezado y el cuerpo del mensaje. Si el receptor ha procesado los datos de manera exitosa, responde con el comando *OK*.
- Si el emisor ha terminado de enviar todos los mensajes a su destino y quiere cambiar de conexión, emite el comando *TURN*. El receptor al recibir este comando responderá con el comando *OK* y tomará el control de la conexión, cambiando los roles emisor/receptor (el cliente pasa a ser el servidor y el servidor se convierte en cliente.
- Para terminar la sesión se emite el comando *QUIT*. Tanto el emisor como el receptor pueden terminar la sesión.

A continuación se mencionaran los comandos que utiliza el protocolo SMTP:

- *DATA*. Indica el comienzo del mensaje.
- *EXPN*. Verifica las listas de correo devolviendo el número de miembros dentro de ella.
- *HELO*. Identifica al cliente.
- *HELP*. Solicita información de ayuda al servidor sobre todos los comandos o sobre alguno en especial.
- *MAIL FROM*. Identifica al remitente del mensaje.
- *NOOP*. Hace que el servidor envíe una respuesta *OK*.
- *QUIT*. Finaliza la conexión.
- *RCPT TO*. Indica la dirección de correo destino.
- *RSET*. Abandona la transacción en curso, descartando los datos enviados y borrando todos los registros.
- *SAML*. Se envía el correo al buzón del usuario independientemente si llega o no a la terminal.
- *SEND*. Se envía el correo a una o más terminales.
- *SOML*. Se envía el correo a una o más terminales, si la terminal no puede recibir el mensaje, el buzón del usuario lo recibirá automáticamente. *TURN*. Intercambia los papeles del cliente y el servidor.
- *VRFY*. Solicita al servidor la verificación del destinatario.

A continuación se muestra el funcionamiento del SMTP:

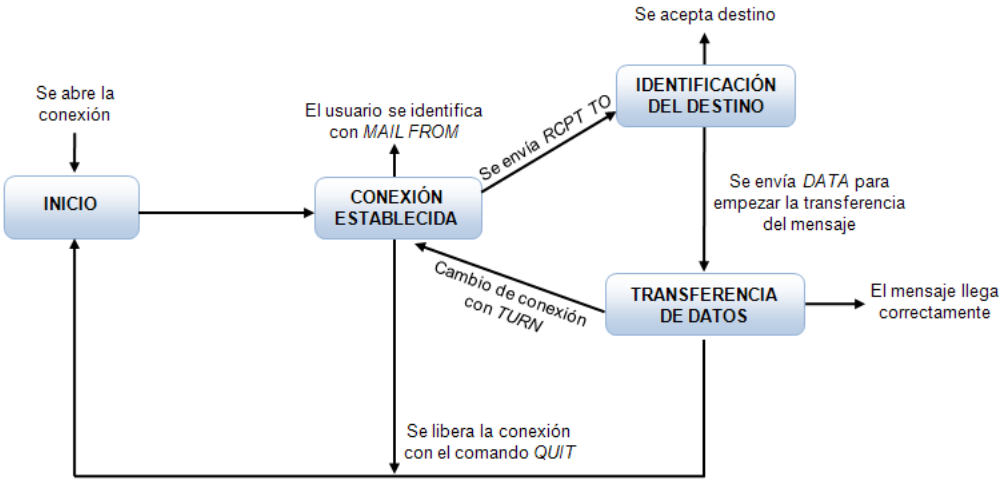


Figura 2.6: Funcionamiento del protocolo SMTP

2.3.2. Entrega final POP3 (Post Office Protocol, Protocolo de Oficina de Postal) e IMAP4 (Internet Message Access Protocol)

El protocolo POP3 (Post Office Protocol) se utiliza para la descarga de correo electrónico, basado en la arquitectura cliente/servidor. El cliente se conecta al servidor de correo y se descargan los mensajes a la máquina de éste, por tanto, los mensajes son eliminados del servidor.

2.3.2.1. Modelo del POP3

- Agente de usuario. Es el que utiliza el cliente POP3 para poder acceder al correo.
- Cliente POP3. Éste se comunica con el servidor para acceder al buzón de correo.
- Servidor POP3. Recibe peticiones de los clientes POP3 enviándolas a los buzones que correspondan cada una.

2.3.2.2. Estados del POP3

Toda sesión POP3 está definida por tres estados:

- Estado de autorización. Identificación del usuario.
- Estado de transacción. Administración del contenido del buzón del usuario. En caso de encontrar correos no deseados, éstos se marcarán y serán eliminados.
- Estado de actualización. Todas las modificaciones se realizan cuando el cliente finaliza el servicio.

Los principales comandos que utiliza POP3 de acuerdo a sus estados son:

1. Estado de autorización.
   - *USER* (nombre). Para identificar al usuario.
   - *PASS*. Especifica la contraseña del usuario.
2. Estado de transacción.

- *STAT*. Presenta el número de mensajes no leídos.
- *LIST*. Indica el tamaño del mensaje n o de todos.
- *RETR* (núm.). Indica el número del mensaje que se ha solicitado enviar.
- *DELE* (núm.). Borra el mensaje indicado con el número.
- *LAST*. Indica el número del último mensaje leído.
- *NOOP*. Permite establecer la conexión abierta en caso de inactividad.
- *RSET*. Recupera los mensajes borrados pero solo los de la conexión actual.
- *TOP* (núm. y líneas). Muestra la cabecera y el número de líneas del mensaje solicitado con el número.
- *QUIT*. Fin de la sesión POP3.

3. Estado de actualización.

   - Este estado no dispone de ningún comando asociado.

A continuación se muestra el funcionamiento del POP3:

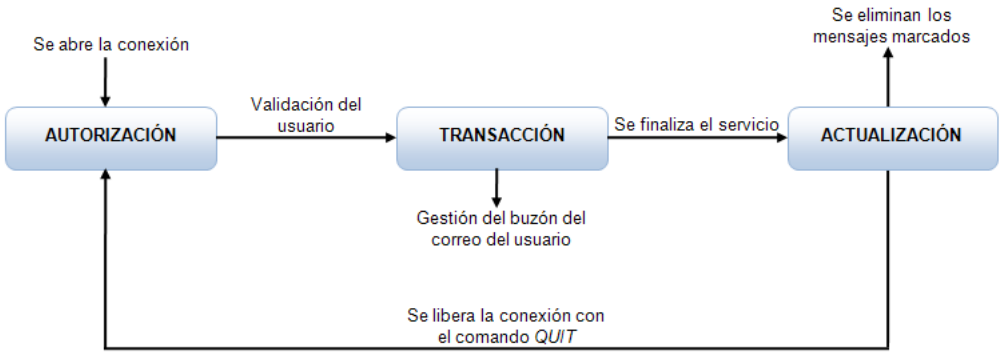


Figura 2.7: Estados del protocolo POP3

Cuando el cliente POP3 necesita acceder al buzón, se conecta con el servidor POP3, recupera la información que le interesa y cierra la conexión.

2.3.2.3. IMAP4

El protocolo IMAP (Internet Message Access Protocol) es el encargado de conservar los mensajes en el servidor, cuando el usuario consulta su buzón de correo únicamente lee las cabeceras del mensaje, éste, al ser abierto, es descargado a la máquina del cliente. Para esto es necesario mantener la conexión durante toda la sesión de usuario.

El protocolo IMAP usa un esquema cliente/servidor. El cliente se comunica con el servidor mediante comandos de texto, los cuales son respondidos por éste con un mensaje informativo, que puede ser:

- *OK*. Ejecución correcta.
- *NO*. Fallo de algún tipo en la ejecución.
- *BAD*. Error del protocolo (Comando incorrecto, error de sintaxis, entre otros).

Los mensajes de correo en IMAP se clasifican en carpetas, y tienen asociada la siguiente información:

- *UID*: Identificador único del mensaje, lo identifica explícitamente en el buzón.

- Número de secuencia: Número relativo al número de mensajes del buzón, desde 1 hasta el número total de mensajes.
- *Flags*: Indicadores de estado del mensaje. Puede ser:
  - Leído
  - Respondido
  - Borrado
  - Borrador
  - Nuevo: Ha llegado durante la última sesión

2.3.2.4. Estados del protocolo IMAP

Los estados del protocolo IMAP son:

- Estado no autentificado. Se acaba de establecer la conexión y el cliente aún no se ha identificado.
- Estado Autentificado. El cliente se ha identificado correctamente, pero aún no ha escogido el buzón activo.
- Seleccionado: El cliente ha seleccionado buzón, y ya puede ejecutar comandos de manejo de mensajes.
- Estado de salida del sistema (logout): La conexión se está cerrando, ya sea a petición del cliente o a criterio del servidor.

Los principales comandos que utiliza IMAP de acuerdo a sus estados son:

1. Estado no autentificado
   - *AUTHEENTICATE*. Indica al servidor el mecanismo de autenticación del cliente que se debe emplear y, si este se encuentra en las condiciones adecuadas para ello, se inicia.
   - *LOGIN*. Identifica al cliente frente al servidor y transporta su contraseña.
2. Estado Autentificado
   - *SELECT*. Selecciona un buzón.
   - *EXAMINE*. Selecciona un buzón pero en modo sólo lectura.
   - *CREATE*. Crear un buzón nuevo.
   - *DELETE*. Borra invariablemente el buzón especificado.
   - *RENAME*. Modifica el nombre de un buzón que ya existe.
   - *LIST*. Hace una búsqueda entre los diferentes nombres de buzón.
   - *LSUB*. Devuelve una lista de buzones que se encuentran subscritos.
   - *STATUS*. Permite obtener el estado del buzón especificado (número de mensajes que contiene, número de mensajes no leídos, recientes, entre otros).
   - *APPEND*. Añade un mensaje al buzón especificado.
3. Seleccionado.
   - *STORE*. Permite modificar los flags de un mensaje.
   - *FETCH*. Permite al cliente recuperar el mensaje o mensajes indicados o bien alguna de sus partes (la cabecera, el cuerpo, el tamaño del mensaje, entre otros).
   - *COPY*. Copia un mensaje desde el buzón actual a otro buzón especificado.
   - *EXPUNGE*. Elimina todos los mensajes del buzón actual marcados como borrados.

- *SEARCH*. Busca en el buzón seleccionado los mensajes que cumplan las condiciones especificadas.

4. Estado de salida del sistema (logout)
    - Este estado no dispone de ningún comando asociado.

Los comandos que puede emitir el cliente en cualquier estado son:

- *COMPABILITY*. Solicita un listado donde se especifique de las capacidades del servidor.
- *NOOP*. Se utiliza para el monitoreo constante del estado de los mensajes.
- *LOGOUT*. Informa al servidor de que el cliente desea terminar la conexión.

A continuación se muestra el funcionamiento del IMAP:

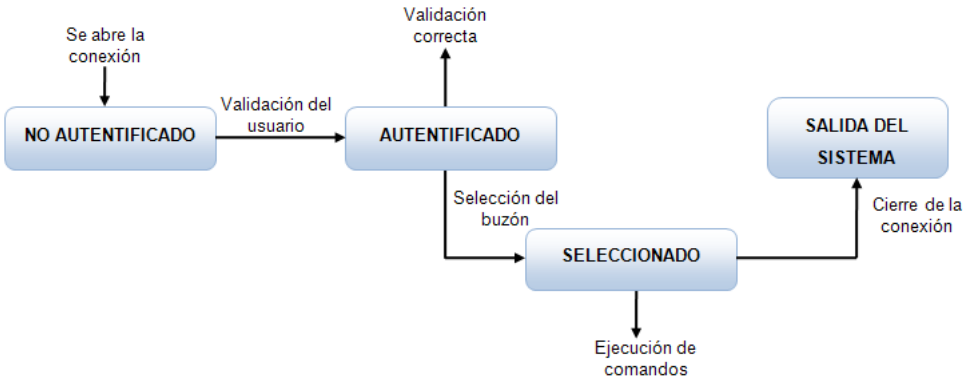


Figura 2.8: Estados del protocolo IMAP

Para poder enviar y recibir correos electrónicos es necesario contar con el protocolo SMTP y POP3 o IMAP, además de los agentes para la administración de los mensajes.

A continuación se ejemplifica el envío y recepción de un correo electrónico visualizando los tres protocolos anteriores así como los agentes que intervienen en el proceso.

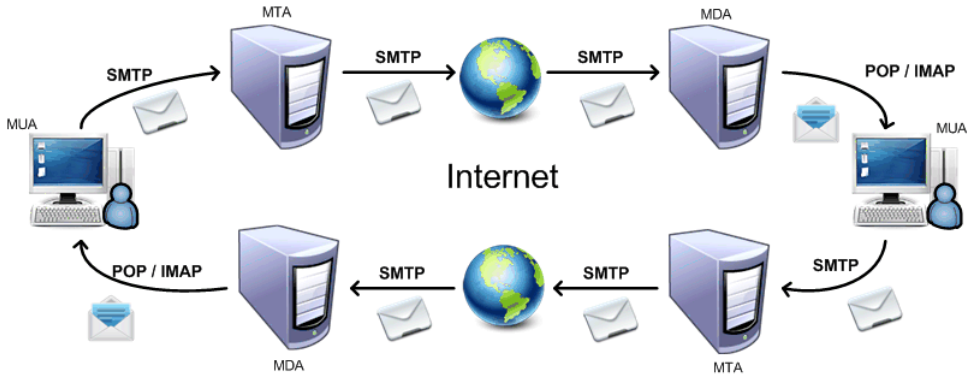


Figura 2.9: Protocos y agentes que intervienen en el envío y recepción de un correo electrónico

Los protocolos POP3 e IMAP (para la recepción), junto con SMTP (para el envío) constituyen el estándar de correo electrónico en Internet.

2.4. RFC (*Request for Comments*, Solicitud de Comentarios)

Los RFC son un conjunto de documentos iniciados en 1967 que describen los protocolos de Internet o propuestas para un nuevo protocolo.

La asociación encargada de regular las propuestas para crear un nuevo RFC es el IETF (*Internet Engineering Task Force*, Fuerza de Tareas de Ingeniería de Internet) ya que cualquier persona puede escribir y enviar un nuevo documento.

Cada RFC tiene asignado un título y un número único que sirve como identificador, éste número no puede repetirse, modificarse ni eliminarse aunque el documento quede obsoleto. Mientras mayor sea el número más actualizada será la versión.

Entre los RFC sobre los servicios más comunes se encuentran [27]:

Especificación	**RFC**
Correo electrónico (formato del mensaje)	RFC 2822
Protocolo SMTP	RFC 5321
Protocolo POP3	RFC 1939
Protocolo IMAP	RFC 2060
Protocolo TCP/IP	RFC 1180
Protocolo HTTP	RFC 2068
Números asignados	RFC 3232

Tabla 2.1: Ejemplos de protocolos y servicios que cuentan con RFC

No todos los RFC son normas, a cada uno se le asigna una denominación dependiendo del estado en que se encuentre.

Estos estados son:

- Informativo
- Experimental
- Mejor Práctica Actual
- Pistas Estándar
- Históricos

Si se desea consultar los RFC existentes, descargarlos o enviar una propuesta, a continuación se deja la página oficial de los RFC.

`http://www.rfc-editor.org/`

2.5. DNS (*Domain Name Server*, Sistema de Nombres de Dominio)

El DNS (*Domain Name Service*, Sistema de Nombres de Dominio) es un sistema de base de datos jerárquico distribuido que asocia las direcciones numéricas de la red (IP) con el nombre del equipo al que se desea acceder, además permite una interpretación sencilla entre los usuarios y los equipos dentro de Internet ya que resulta más fácil recordar el nombre de la página (por ejemplo *www.google.com*) que su IP.

El DNS guarda las direcciones que se van visitando dentro de una tabla, de esta forma se puede acceder más rápido a éstas y si la dirección no esta dentro de la tabla, se hace una petición al servidor DNS para que la almacene dentro de ella para visitas futuras.

Entre las características de los nombres de dominio se encuentran:

- Un nombre de dominio generalmente consiste en dos o más partes (o etiquetas) que van separadas por puntos.

- El nivel básico de los DNS es la zona *root* (raíz) la cual es representada por un punto a la derecha del dominio de primer nivel. La zona raíz es el punto de partida para realizar la resolución de nombres DNS.

- La etiqueta que se encuentra más a la derecha (parte final de la dirección) se le llama dominio de primer nivel (TLD, *Top Level Domain names*). Los TLD hacen referencia al origen geográfico del dominio y su tipo.

  Los dominios de primer nivel se clasifican en dos categorías:

  - Genéricos: Hacen referencia al tipo de actividad que tendrá el sitio *web*, formados por terminaciones de tres o más caracteres.

    A continuación se muestran algunos de los principales dominios genéricos así como su descripción [17]:

Dominio	**Significado**	**Definición**
.biz	*bizness* - negocio	Dominio que se utiliza para uso comercial
.com	comercial	Dominio utilizado por entidades u organizaciones comerciales
.edu	educación	Dominio restringido a instituciones educativas
.gov	gobierno	Dominio utilizado por un cuerpo, departamento o agencia gubernamental
.net	red	Dominio utilizado por la red u organizaciones de Internet
.org	organización	Dominio utilizado por organizaciones no lucrativas

Tabla 2.2: Ejemplos de TLD genéricos

  - Territoriales o Geográficos: Hace referencia al país del dominio, formado por dos letras del país.

    A continuación se mencionan los dominios de algunos países [17]:

Dominio	**País**
.ar	Argentina
.br	Brasil
.ca	Canadá
.es	España
.fr	Francia
.mx	México
.us	Estados Unidos

Tabla 2.3: Ejemplos de TLD territoriales

- Las etiquetas que se encuentran antes del TLD se les llama dominio de segundo nivel (SLD, *Second Level Domain names*). Generalmente describen la entidad o asociación al que pertenece el dominio.

- El tercer nivel, llamado también subdominio, se encuentra a la izquierda del segundo nivel.

- Debido a que los DNS tienen una jerarquía de árbol cada TLD contiene varios SLD y cada SLD contiene varios subdominios.

- La parte que se encuentra más a la izquierda de los subdominios es el nombre del equipo (*hostname*).

- Al conjunto que forma la raíz, el TLD, el SLD, los subdominios y el *host* separados por puntos se le llama *FQDN* (*Fully Qualified Domain Name*, Nombre de Dominio Completamente Calificado). Éste no puede exceder de los 255 caracteres (máximo 60 caracteres en cada nivel del dominio) y podrá tener una profundidad máxima de 127 niveles.

A continuación se muestra un ejemplo de la estructura de árbol DNS.

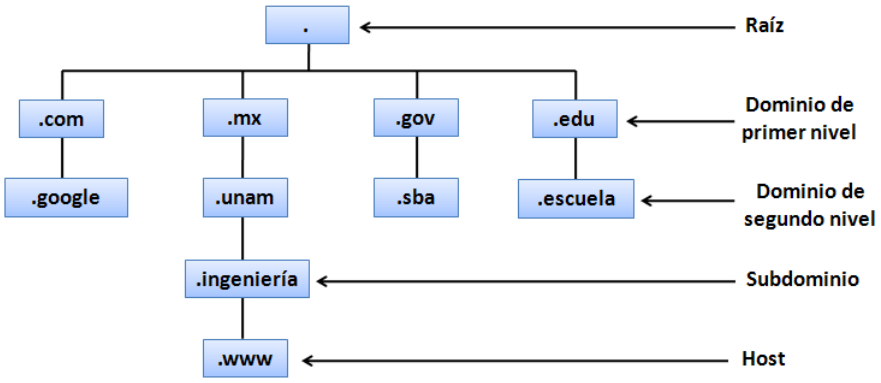


Figura 2.10: Jerarquía del DNS

El organismo responsable de la gestión y coordinación de los DNS a nivel mundial es el ICANN (*Internet Corporation for Assigned Names and Numbers*, Corporación para la Asignación de Nombres y Números de Internet). Garantiza que cada dirección sea única permitiendo a los usuarios de Internet encontrar todas las direcciones válidas además de garantizar que cada nombre de dominio este asociado a la dirección IP que le corresponda.

2.5.1. Herramientas

Principalmente encontramos tres herramientas para consultar registros DNS relacionados con un nombre de dominio por ejemplo: el servidor en el que se aloja la zona (registro *NS*), la redirección DNS para correo electrónico (registro *MX*), o cualquier otro registro como los de definición de servidor (registro *A*).

Estas herramientas son:

- *Nslookup*:Comando de Windows y Unix que permite consultar a un servidor DNS para obtener el nombre teniendo la dirección IP y viceversa.
- *Jwhois*: Comando que permite realizar consultas a través de servidores *WHOIS*.

  La sintaxis básica de *jwhois* es:

  $$jwhois < dominio >$$

- *Dig* (*Domain Information Groper*): Herramienta para hacer consultas a DNS y obtener información sobre direcciones *web*, name servers, entre otros, regresando las respuestas a través de los servidores consultados, además es de gran utilidad para detectar problemas en la configuración de los servidores de DNS debido a su flexibilidad, facilidad de uso y claridad en su salida.

  Esta herramienta se encuentra dentro del paquete de BIND (*Bind Name Berkeley Internet*) *software* de código abierto que implementa los DNS para protocolos de Internet.

  La sintaxis básica de *dig* es:

  $$dig < @servidor > < nombre > [tipo]$$

  Donde:

  - servidor: nombre o dirección IP del servidor a consultar.
  - nombre: nombre del registro del recurso que se está buscando.
  - tipo: tipo de consulta requerida (*ANY*, *A*, *NS*, *SOA*, *MX*, entre otros).

- Host: Comando útil para realizar búsquedas en el DNS, utilizado principalmente para convertir nombres en direcciones IP y viceversa.

  La sintaxis básica de *host* es:

  $$host\ [opciones]\ <dominio>\ [servidores]$$

  Algunas opciones son:

  - *-t* <tipo>: indica el tipo de record a devolver. Puede ser *A*, *ANY*, *PTR*, *NS*, entre otras.
  - *-R* <n>: permite modificar el número de intentos que se hacen para obtener la respuesta ya que por defecto es uno.
  - *-l*: lista toda la información del dominio.

2.5.2. Componentes

Por su funcionamiento, el DNS utiliza tres componentes principales:

- Clientes DNS (*DNS Resolvers* o *DNR*): Son peticiones de consulta para resolver nombres generados por los usuarios. Las consultas son generalmente para preguntar acerca de la dirección IP que corresponde a un determinado nombre de dominio.
- Servidores DNS (*DNS Name Servers*, Servidores de Nombre): Son servicios que contestan las peticiones realizadas por los clientes DNS consultando su base de datos. Si el servidor DNS no dispone de la dirección solicitada puede reenviar la petición a otro servidor.

  Existen dos tipos de servidores de nombre:

  - Servidor maestro/primario: Obtiene los datos del dominio a partir de un archivo alojado en el mismo servidor, de esta manera puede atender directamente las peticiones de los clientes además, el servidor maestro es responsable de mantener la información actualizada.
  - Servidor Esclavo/Secundario: Obtiene los datos del dominio a través de un servidor maestro realizando el proceso llamado transferencia de zona (Transferencia de Zona: es el mecanismo por que permite actualizar la información a los servidores secundarios a partir de los archivos de zona contenidos en el primario.). Cuando se inicializa el servidor secundario, éste carga una copia completa de los datos de zona del servidor primario (también los carga si los datos de una zona se modifican).
- Espacio de Nombres de Dominio (*Domain Namespace*): Es la base de datos que se encuentra de manera distribuida (varios equipos dentro de la red) y jerárquica (tiene forma de árbol), la cual se encarga de clasificar los dominios en niveles.

2.5.3. Zonas

Una zona es una parte gestionable de datos que contiene información sobre los nombres de dominio y direcciones IP de un dominio DNS o partes de éste. Cada zona es administrada por uno o más servidores DNS los cuales dan autorización para resolver o traducir direcciones IP a peticiones o consultas de un nombre de dominio.

Las zonas principales del DNS son:

- Zona de autoridad: Porción del espacio de nombres de dominio de la que es responsable el servidor DNS. Esta zona abarca un dominio y puede incluir subdominios.
- Zona principal: Es la zona con capacidad de lectura y escritura sobre la información.
- Zona secundaria: Es la zona que únicamente tiene capacidad de lectura sobre la información.

- Zona apéndice: Transfiere únicamente los registros del servidor de nombres de la propia zona.
- Zona de reenvío: Dirige todas las consultas de la zona a otros servidores.
- Zona de código auxiliar: Zona que únicamente contiene registros *SOA*, *NS* y *A*.
- Zona directa: Resuelve de nombre DNS a una dirección IP.
- Zona Inversa: Resuelve de dirección IP a nombre DNS.

2.5.4. Registros de Recursos (*RR*)

Dependiendo de la zona el servidor DNS almacena diferentes tipos de registros de recursos para resolver las direcciones IP a nombres de dominio. Estos registros constituyen la información de recursos asociada al dominio como lo son: el nombre, el tipo y la dirección del registro.

La estructura de los RR consta de cinco campos:

$$[nombre\_dominio]\ [TTL][class]\ type\ RDATA$$

donde:

- Nombre de *host* o nombre de dominio: Indica el nombre de dominio (*FQDN*) al que pertenece el recurso .
- *TTL* (*Time To Live*, Tiempo De Vida): Indica la duración en segundos que puede ser almacenada la información en la cache.
- Clase (*class*): Describe que tipo de dato se almacena en el registro.
- Tipo (*type*): Valor de 16 bits que define el tipo de registro.
- Dato Registro (*RDATA*): Son los datos relacionados con el registro. Aquí se encuentra la información que se espera según el tipo de registro.

A continuación se describen los principales Registros de Recursos [25, 26]:

Nombre del RR	**Tipo de Registro**	**Función**
Address	*A*	Traduce nombres de dominio a direcciones IP (IPv4)
Address	*AAA*	Traduce nombres de dominio a direcciones IP (IPv6)
Nombre Canónico (*Canonical Name*)	*CNAME*	CNAME Crea un alias para el nombre de dominio especificado
De intercambio de correo (*Mail Exchanger*)	*MX*	Identifica al servidor de correo responsable de un nombre de dominio
Servidores de Nombre (*Name Server*)	*NS*	Identifica el servidor de nombres para el dominio
Puntero (*Pointer*)	*PTR*	Asigna una dirección IP a un nombre de dominio
Inicio de Autoridad (*Start of Authority*)	*SOA*	Especifica la zona de la máquina de donde proviene la información principal
Servicio (*Service*)	*SRV*	Indica de forma genérica los servidores disponibles para un servicio, protocolo o dominio DNS
Texto (*Text*)	*TXT*	Permite asociar un texto con un dominio o subdominio

Tabla 2.4: Principales tipos de RR y su significado

2.5.5. Instalación y configuración del DNS

Para poder configurar el DNS en el equipo es necesario instalar el paquete BIND (acrónimo de *Berkeley Internet Name Domain*) sirviendo éste como complemento para atender las consultas además de proveer los componentes principales del DNS. Si el equipo se encuentra conectado a Internet de manera constante BIND mantendrá una tabla local con todos los nombres que va conociendo guardando las direcciones IP y los nombres de las máquinas, evitando así repetir las búsquedas.

Dado que el servidor funcionará bajo el Sistema Operativo Debian, únicamente se mencionará los archivos que van a modificarse bajo dicho SO.

El comando para la instalación del paquete BIND9 (última versión estable) es:

apt-get install bind9

Una vez instalado se deben modificar los archivos para configurar las zonas de autoridad que gestionará el servidor BIND.

Estos archivos son:

- */etc/bind/named.conf*: Almacena los archivos que cargará BIND cada vez que se reinicie.
- */etc/bind/named.conf.local*: Almacena las zonas con las que se va a trabajar (zona de resolución directa y zona de resolución inversa).
- */etc/bind/named.conf.options*: Permite redirigir las peticiones a otro servidor DNS cuando no se puedan resolver.
- */var/cache/bind/*: Almacena toda la información correspondiente a cada zona.

Para finalizar la configuración es necesario reiniciar el BIND para ellos se utiliza el comando:

/etc/init.d/bind9 restart

2.6. Servidores de Correo

Un servidor de correo es una aplicación en Internet cuya función es recibir, almacenar, gestionar y enviar los correos electrónicos a su destino final independientemente de la red que se este utilizando, permitiendo de esta manera la comunicación entre clientes de correo.

Entre los principales servidores de correo se encuentran:

- Mercury Mail Server: Compatible con Windows, Unix, GNU/Linux
- Microsoft Exchange Server: Compatible con Windows
- Sendmail: Compatible con Unix
- Qmail: Compatible con Unix
- Postfix: Compatible con Unix
- Zimbra: Compatible con Unix, Windows

2.6.1. Funcionamiento

Para el correcto funcionamiento del servidor son necesarios los protocolos SMTP, POP3, IMAP y los agentes MUA, MTA y MDA.

El funcionamiento del servidor de correo es el siguiente:

- El usuario (MUA) crea un correo electrónico (utilizando un cliente de correo) y lo envía al servidor de correo.
- El servidor envía una petición al DNS para que identifique y resuelva la dirección IP destino. Si el DNS reconoce la dirección envía en correo al MTA, sino reconoce la dirección el DNS le manda un aviso al servidor para que notifique al cliente de correo que no se pudo enviar el mensaje.
- Cuando el correo llega al MTA el mensaje será enviado a otros MTA (comunicándose entre sí a través del protocolo SMTP) que lo encaminarán al MTA destino (si el correo va dirigido a un servidor MTA local, el correo pasa directamente al MDA).
- Cuando el mensaje llega al MTA destino el correo se entrega al MDA, el cual es el encargado de almacenar el mensaje hasta que el usuario lo acepte.
- Por último, el usuario final (MUA) visualiza su correo usando, ya sea el protocolo POP3 o IMAP.

2.6.2. Características

Como se vio en el tema anterior existen diferentes servidores de correo, cada uno con sus ventajas y desventajas, sin embargo, comparten ciertas características en común.

Algunas de las características de los servidores son:

- Gestiona las cuentas de los clientes de correo.
- Cuenta con un servidor SMTP propio.
- Permite la configuración del espacio de las bandejas de los clientes (cuotas).
- Cuenta con un espacio donde se almacenarán los correos electrónicos (buzón de correo).
- Está protegido por un antivirus el cual se encargará de revisar todos los correos que lleguen, buscando troyanos, virus, gusanos, entre otros para identificarlos y eliminarlos.
- Cuenta con listas negras para identificar los correos basura o correos *spam*.
- Proporciona servicios de recuperación y transferencia de correo electrónico (colas de correo).
- Le permite al administrador de correo crear las cuentas que desee dentro del servidor siempre y cuando no repita los datos en el mismo orden.

2.7. Clientes de Correo

El cliente de correo es una aplicación que permite al usuario enviar y recibir correos electrónicos a través de una cuenta que se encuentra dentro del servidor de correos. Es el intermediario entre el servidor de correo y el usuario.

Existen diferentes proveedores de correo, se clasifican en tres tipos:

- *Web*: Este tipo de clientes se ejecutan a través de Internet, por ejemplo: Hotmail, Yahoo! Mail, Gmail, OpenWebmail, entre otros.
- Instalables: Este tipo de clientes se ejecutan directamente desde equipo del usuario, por ejemplo: Windows mail, Outlook, Mozilla Thunderbird, Pegasus, Evolution, entre otros.
- Texto: Este tipo de clientes se ejecutan a través de la línea de comandos, por ejemplo: Pine, Mutt, entre otros.

2.7.1. Funcionamiento

El proceso interno del envío y recepción del correo electrónico es invisible para el cliente de correo, únicamente notifica si el correo fue enviado, recibido o hubo algún problema en el envío.

Si el usuario quiere enviar y/o recibir un correo electrónico se necesitan los agentes MTA, MDA, MUA y los protocolos SMTP, POP3 o IMAP.

El funcionamiento de un cliente de correo es el siguiente:

- El usuario (MUA) se conecta a Internet y abre su cuenta de correo, accesando su usuario y contraseña.
- Envía el correo electrónico el cual viajara a través del protocolo SMTP y el agente MTA.
- Cuando el mensaje llega, se almacena en el buzón del cliente (MDA).
- El usuario receptor abre el correo electrónico utilizando el protocolo POP3 o el protocolo IMAP.
  - Si usa el protocolo POP3
    - Los mensajes se guardarán en el equipo del usuario.
    - Podrá leer los correos recibidos dentro de su equipo sin la necesidad de estar conectado a Internet.
    - Se libera espacio en el buzón del servidor de correos.
  - Si utiliza IMAP
    - Si el equipo es robado o se daña, los mensajes estarán a salvo dentro del servidor puesto que no son descargados al equipo del usuario.
    - El correo permanecerá en el buzón del servidor hasta que el usuario lo elimine.
    - Puede consultar su correo desde equipos diferentes, siempre y cuando tenga acceso a Internet.

2.7.2. Características

Como se vio en el tema anterior, existen diferentes clientes de correo, el usuario podrá elegir el tipo que más se acomode a sus necesidades, sin embargo, los clientes de correo comparten ciertas características en común.

Algunas características de los clientes de correo son:

- Proporciona herramientas que le faciliten la gestión al usuario (etiquetas, carpetas, limpieza, calendario, entre otros).
- El usuario puede gestionar sus correos, así como sus carpetas.
- Facilita la búsqueda de correos electrónicos o contactos que tenga el usuario.
- Permite la administración de las listas de usuarios que tenga el dueño de la cuenta.
- Algunos clientes cuentan con mensajería instantánea, mejorando la comunicación entre los usuarios.
- Fácil de usar.
- Permite exportar e importar listas de direcciones a otros clientes de correo siempre y cuando el otro cliente lo permita.

Capítulo 3

Diseño, Instalación e Implementación

3.1. Funcionamiento Actual de Correos no Institucionales

Como se mencionó en el capítulo anterior, uno de los servicios de mayor demanda es el correo electrónico, ya que permite la comunicación entre usuarios desde cualquier parte del mundo, a través del envío y recepción de mensajes.

Dado que en algunos establecimientos, instituciones o negocios no tienen los recursos para instalar y administrar un servidor de correos propio, existen varias compañías que proveen este servicio, diferenciándose entre sí por la calidad de éste y las herramientas que ofrece, por lo que los usuarios pueden elegir el que más les convenga de acuerdo a sus necesidades.

Para crear una cuenta, basta con visitar a la respectiva página oficial del proveedor del servicio, llenar un pequeño formulario con algunos datos personales del usuario y seguir los pasos en línea que se indiquen en la página.

Una vez creada, se ingresa a la cuenta usando el nombre de usuario y contraseña elegidos

Los elementos necesarios para el funcionamiento actual de correos no institucionales son:

- Dirección de correo. Indica el alias de un usuario además del nombre del proveedor al cual se encuentra inscrito.
- Proveedores de correo. Son las compañías que ofrecen el servicio para el envío/recepción de mensajes.

Las compañías que ofrecen este tipo de cuentas de correo se pueden clasificar en: gratuitos y de pago.

Gratuitos: Son los más utilizados, aunque incluyen un poco de publicidad, ya sea en su interfaz o incrustada en los mensajes, asegurando de esta forma, la publicidad de la compañía. Este tipo de cuentas permiten ver el correo electrónico desde cualquier equipo con acceso a Internet (lo que ofrece una ventaja a los usuarios que viajan constantemente) y además no es necesario un cliente de correo en específico para poder utilizarlo. Ejemplo: Gmail, Hotmail, Yahoo.

Pago: Las cuentas de correo generalmente vienen incluidas cuando se contrata un proveedor de Internet. Este tipo de cuentas de correo normalmente es utilizado en las empresas y no tanto para usarlas de forma personal. Ofrecen más herramientas y ventajas que las cuentas gratuitas (mayor capacidad de almacenamiento, mayor tamaño en los archivos adjuntos, entre otros). Ejemplo: Telefónica[1] y Ono[2].

El correo electrónico no institucional cuenta con los siguientes recursos:

- Manejo de chat interno

[1] Telefónica: Compañía de telefonía (móvil, fija y ADSL), Internet y Televisión ("Imagenio") cuyos inicios comenzaron desde 1924 en España. Hoy en día cuentan con cobertura multinacional.

[2] Ono: Compañía de Telefonía (móvil, fija y ADSL), Internet y Televisión. Cuyos inicios comenzaron desde 1998 en España. Hoy en día cuentan con cobertura a nivel nacional.

- Manejo de antispyware, antispam y correo no deseado.
- Manejo de agenda y/o calendario y bloc de notas.
- Se permite firma e imagen al correo.
- Importar contactos de un correo a otro.

La capacidad de almacenamiento total de la bandeja de entrada de algunos proveedores de correo son:

- Hotmail: De 5GB
- Yahoo: Ilimitado
- Gmail de 10GB

Nota: Todos los datos fueron sacados de la página oficial de los respectivos proveedores de correo.

Los correos no institucionales poseen los siguientes inconvenientes:

- Este tipo de correos tienen una base de clientes mucho más amplia. Una dirección de correo puede estar ya dada de alta y, debido a que no pueden existir direcciones iguales dentro del mismo servidor, no se podrá registrar el nombre de usuario que se tenía en mente sino uno parecido o elegir un alias nuevo. Las direcciones con nombres personales tendrán más variaciones por lo que será difícil recordarlas.
- Los alias pueden llegar a ser poco profesionales, debido a la gama de combinaciones de números, letras y guiones que el servicio ofrece, por lo que cuentas como "*ositocariñosito025_uu@dominio.com*" son mal vistos por empresas y/o instituciones.
- Debido a que no se paga por el servicio, el usuario está propenso a la publicidad dentro de los mensajes o dentro de la interfaz que ofrece la compañía ya que es a través de los anuncios que los proveedores obtienen sus ganancias. En ocasiones, únicamente permiten al usuario ver su correo dentro de un sitio *web* propio para asegurar que los usuarios reciban la publicidad.
- La cuenta puede ser bloqueada o incluso eliminada sin previo aviso si el usuario sobrepasa el tamaño del buzón especificado por la compañía.
- Las cuentas de correo no institucionales no son para siempre, las de paga dependen del servicio que se contrato y las gratuitas desaparecerán si el portal cierra o hay poca actividad en la cuenta, causando la baja de ésta por falta de uso. En cualquier caso, algunas compañías no suelen ofrecer servicios como la redirección de los correos o migrar a otra cuenta, perdiéndose así los mensajes en la red.
- Dado que las cuentas de correo no institucionales pueden crearse con datos falsos, los receptores no tendrán ninguna garantía de que el remitente sea la persona quien dice ser. La cuenta falsa puede hacerse pasar por bancos, empresas o incluso la misma compañía pidiéndole al usuario datos personales, depósitos, hacerle creer que ganó un premio y debe contestar una encuesta o mandar correos a sus contactos para validarlo o lo amenazan con cancelar su cuenta sino manda una determinada cantidad de correos, incrementando de esta forma la recepción de virus, troyanos y gusanos. A este tipo de mensajes se les llama correo basura o *spam*.

3.2. Estructura general de la DICyG

La División de Ingenierías Civil y Geomática está conformada por ocho departamentos: Construcción, Topografía, Geotecnia, Sanitaria y Ambiental, Hidráulica, Sistemas y Planeación, Estructuras y Geodesia, además la DICyG cuenta con:

- Secretaría académica
- Titulación

- Servicio social
- Especialización
- Posgrado
  - Maestría
  - Doctorado
- Coordinación de Ingeniería Civil
- Coordinación de Ingeniería Geomática
- Practicas escolares
- Coordinación de proyectos
- Sistemas de altas, bajas y cambios extraordinarios
- Inscripciones a los diferentes laboratorios.

La DICyG cuenta con un total aproximado de 90 personas: 15 administradores, 20 funcionarios, al rededor de 40 profesores de carrera y un número variado de alumnos de servicio social y becarios además del personal que se encuentra fuera del edificio principal.

3.2.1. Necesidades de la DICyG

La División de Ingenierías Civil y Geomática no cuenta con un servidor de correo propio, por lo que utilizan un correo comercial para realizar las actividades académicas y administrativas de cada una de las diferentes áreas con las que cuenta la División.

Entre las principales desventajas que esto ocasiona se encuentran:

1. No saber a qué dependencia corresponde.
2. Se puede hacer mal uso del correo electrónico al poder suplantar el nombre de usuario.
3. No existe una administración que gestione las cuentas de correo. Un profesor que ya no trabaja en la DICyG puede seguir recibiendo correos de la misma.
4. No se tiene la certeza de que se está contactando al personal de la DICyG.
5. No existe formalismo en sus cuentas de correo.
6. Dado que la cuenta que se usa es personal y se recibe todo tipo de correos, los mensajes provenientes de la DICyG pueden no llegarse a ver.
7. No existe la garantía de que las cuentas de correo que usan el personal docente y administrativo de la DICyG lo utilicen únicamente para asuntos de la misma.

Es por ello que la DICyG requiere de un servidor de correo institucional propio y funcional para poder comunicarse dentro y fuera de la misma, dándole un mayor profesionalismo al momento de enviar un correo electrónico. Las personas que reciban un correo perteneciente a la DICyG no sólo sabrán de que dependencia procede sino que estarán seguros de que proviene de un remitente confiable ya que las cuentas serán creadas con el nombre y apellido del personal administrativo y docente, evitando así alias informales. Además cualquier información relevante para la DICyG llegará a un único dominio.

3.2.2. Importancia de las TI para la DICyG

Como se menciono anteriormente las TI son las herramientas innovadoras que permiten el procesamiento, almacenamiento y la distribución de la información a través de medios digitales.

Las TI tienen como objetivo mejorar y facilitar la vida de las personas, ahorrándoles tiempo, ampliando su comunicación, fomentando su aprendizaje y mejorando el intercambio de información, siendo Internet el principal y más grande proveedor de ello además de la herramienta del correo electrónico.

Antes de la existencia de las TI, se tenían varias limitantes académicas y administrativas:

- Si los alumnos tenían duda sobre la clase o la tarea, la única forma de contactar al profesor era buscarlo en su cubículo (si lo tenía), en otra clase (si la daba) o buscarlo por la universidad, además de tener que ir a un horario determinado sin tener la certeza de que el profesor contara con tiempo disponible para atenderlos.
- Si se tenía dudas para algún trámite o hacer correcciones, era forzoso ir a ventanillas a preguntar en un horario específico afectando principalmente a los alumnos ya que cabía la posibilidad de que el horario de atención coincidiera con sus clases o que vivieran retirados de la universidad y no les fuera tan accesible regresar a la universidad.
- Si se tenía dudas para algún trámite, era forzoso ir a ventanillas a preguntar en un horario específico. Ésto afectaba principalmente a los alumnos ya que muchas veces los horarios no coincidían con el horario de clases, por lo que, tenían que esperar el horario establecido por ventanillas.
- El profesor no tenía forma de avisar si había cambios en las actividades acordadas para la clase o si iba a faltar a ésta por algún imprevisto.
- No existían los sitios para descargar las guías, tareas, apuntes o material de interés.
- Se tenía menos formalismo para la entrega de trabajos.
- Se tenía una difusión limitada para conferencias, talleres, asesorías y otras actividades culturales como conciertos y ferias.
- Si se tenía un aviso para los profesores o personal administrativo, no había forma de darle el mensaje si la persona ya no se encontraba en la universidad.
- Era imposible dar y obtener información en horario nocturno.
- Si se dejaban recados para el personal administrativo o docente no había garantía de que lo recibieran.

Gracias a las TI, la DICyG ha optimizado el manejo de la información y el desarrollo de la comunicación, ya que:

- Los alumnos pueden mandar sus dudas, tareas o comentarios al correo, blog, foro o página *web* del profesor.
- La forma de realizar los trámites pueden consultarse y realizarse a través de la página *web* de la división.
- Los profesores pueden subir las tareas, apuntes, instrucciones, prácticas, calificaciones o noticias a una página en especial para que los alumnos descarguen la información.
- Se puede tener comunicación con el personal docente y administrativo de la DICyG a través del correo electrónico.
- El personal docente y administrativo recibe correo electrónico sin interrumpir sus actividades actuales.
- La información que se necesite puede consultarse en el horario que se desee.
- La mayoría de los trámites se realizan en línea. Es en la entrega de documentación cuando se deberá ir a ventanilla.

- El calendario escolar, cursos, talleres e información de la DICyG puede consultarse en la página de la misma.
- Se reduce tiempo en comunicar avisos al personal docente y administrativo ya que puede hacerse mediante correo electrónico, redes sociales, teléfono o celular.
- Si el profesor lo desea, puede subir su horario y la ubicación de su cubículo para que alumnos y personal docente puedan encontrarlo más rápidamente.
- El personal docente y administrativo de la división puede dar atención individualizada al estudiante, profesor o personal de la universidad mediante el correo electrónico.

A través de su sitio *web* la DICyG actualiza la información de cada uno de los departamentos por los que está conformada, además de los planes y programas de estudio de los alumnos, sin olvidar formas de titulación, eventos, noticias, laboratorios, posgrados, conferencias, formatos y avisos entre otros sitios de interés no sólo para el alumno sino también para el personal de la misma.

3.2.3. Principales Servidores de Correo

Entre los principales servidores de correo se encuentran los siguientes:

- Sendmail

  Sendmail es un agente de transporte de correo (MTA), compatible con sistemas Unix. Como todos los MTA, su tarea principal consiste en encaminar los mensajes de correos de forma que estos lleguen a su destino. Además acepta conexiones de red procedentes de otros MTA y puede depositar el correo recibido en carpetas locales o entregarlo a otros programas. Esto lo realiza manteniéndose a la escucha del *socket* 25, comunicándose con los *daemons* de otros sistemas para recibir el correo entrante y enviar el correo saliente. Utiliza el protocolo SMTP, el cual se caracteriza por su eficiencia, sencillez y facilidad de depuración, gracias a los mensajes que acompañan a sus comandos.

- SquirrelMail

  SquirrelMail es un *software* libre de correo electrónico escrito en PHP4 que permite al usuario acceder a su correo a través de cualquier navegador siempre y cuando el servidor *web* soporte PHP y se tenga acceso a los servidores IMAP y SMTP.

  Es compatible con la mayoría de servidores web gracias a que sigue el estándar HTML 4.0 lo que le permite mostrar las páginas sin la necesidad de JavaScript. Además de contar con diferentes plugins que permite agregar nuevas características a la interfaz de SquirrelMail.

- Zimbra

  Es un programa colaborativo de mensajería basado en lenguaje Ajax[3] (JavaScript con *XML*) el cual permite compartir, almacenar y organizar mensajes de correo electrónico, citas, contactos, tareas, documentos entre otros servicios. Entre las versiones disponibles se encuentran: la de código abierto y la de soporte comercial con varios componentes extra de código cerrado. Disponible para Sistemas Operativos, Windows, Linux y Mac OS.

  Zimbra extiende sus capacidades gracias a plugins integrando de esta manera softwares externos a través del uso de *SOAP*[4] y *web* Services, además de contar con un servidor SMTP, POP e IMAP propio y antivirus integrado.

  Su interfaz puede personalizarse (cambiar el tema de la bandeja de entrada) y ofrece la versión de HTML para los equipos antiguos o entornos que no puedan utilizar JavaScript.

[3] Ajax (*Asynchronous JavaScript And XML*): Técnica de desarrollo *web* para crear aplicaciones interactivas (*RIA*, *Rich Internet Applications*).

[4] *SOAP* (*Simple Object Access Protocol*): Protocolo basado en *XML* para el intercambio de mensajes sobre redes de computadoras, usando generalmente HTTP.

A continuación se muestran otras características de estos servidores de correo:

Servidor	Protocolos	Distribuciones	Mayor compatibilidad con navegadores	Rendimiento	Seguridad
SendMail	IMAP y SMTP	Red Hat Enterprise Linux , FreeBSD, Fedora, Ubuntu, Debian Squeeze, CentOS, Mac OS X, Mandriva	iExplorer, Safari, Chrome, Firefox	Alto	Baja
SquirrelMail	SMTP, POP, IMAP y DNS	Linux tipo Red Hat, Ubuntu, Fedora, Oracle Linux, CentOS, Unix	iExplorer, Safari, Chrome, Firefox	Alto	Baja
Zimbra	SMTP, IMAP, SOAP, LMTP, POP	Red Hat Enterprise Linux, Fedora, Ubuntu, Opera, Debian, Mandriva y SUSE Linux, Mac OS X, Gentoo y VMware	iExplorer, Firefox, Safari, Chrome	Alto	Alta

Tabla 3.1: Comparación de los servidores de correo

3.2.4. Selección de *software* de base a emplearse

El Sistema Operativo (Operativa System, SO) es el conjunto de programas (*software* del sistema de base) que permite la administración de los recursos del equipo gestionando el *hardware* y brindando una interfaz para poder interactuar con el usuario. El encargado de inicializar el SO cuando es encendido el equipo es el boot (secuencia de arranque).

Las principales funciones de un SO son:

- Gestionar eficientemente el *hardware* y el *software*.
- Suministrar una interfaz para el usuario.
- Controlar y administrar la ejecución de programas, recursos y archivos.
- Gestión y recuperación de errores.
- Intérprete de comandos.

El usuario interactúa y le da órdenes al equipo a través de una interfaz. Existen varios tipos de interfaces, de las cuales cabe diferenciar entre el modo gráfico y el modo texto.

- Interfaz de Línea de Comandos (*Command Line Interface*, *CLI*)

  Esta interfaz permite manipular el SO a través de instrucciones textuales. Cada una de estas instrucciones es escrita en una línea de texto y se ejecutan al presionar ENTER, además permite programas *scripts* para la ejecución automática de varias líneas de comando. Estos comandos son reconocidos por el equipo y dependiendo de la secuencia, se realizará una operación específica. Ejemplo de Sistema Operativo con este tipo de interfaz: CP/M, VMS, MS-DOS y, en sus orígenes, UNIX.

- Interfaz Gráfica de Usuario (*Graphical User Interface*, *GUI*)

  Esta interfaz ofrece un conjunto de imágenes y programas gráficos que permite manipular el SO de forma directa a través de ventanas, menús, iconos, botones, por mencionar algunos. Este tipo de interfaz es más amigable para el usuario ya que no es necesario saber programar ni conocer comandos para darle instrucciones al equipo, visualiza donde están las aplicaciones y programas lo que le permite acceder más rápidamente a ellos y manipularlos, además puede trabajar en varios programas a la vez sin tener la necesidad de reiniciarlos. Utiliza principalmente el cursor y el teclado. Ejemplo de Sistema Operativo con este tipo de interfaz: Windows, Linux, Mac OS, aunque siempre es posible en estos sistemas operativos utilizar una interfaz en modo texto si fuera preciso (por ejemplo en la programación o dar instrucciones mediante la terminal).

Los SO más utilizados son:

- En teléfonos móviles: Android, Windows Phone, Windows Mobile, Linux, Symbian OS, BlackBerry OS, iOS.
- En Servidores: Unix, Windows Server o Linux, BSD, FreeBSB.
- En PCs y otras computadoras personales: Windows (XP, Vista, Windows 7, Windows 8), Linux (Ubuntu, Debian, Open Suse, entre otros) y Macintosh (Mac OS 8, Mac OS 9, Mac OS X de las cuales se derivan: 10.0 [Cheetah], 10.2 [Jaguar], 10.4 [Tiger], 10.7 [Lion], 10.8 [Mountain Lion], entre otros).

3.2.4.1. Windows

Microsoft Windows es una familia de Sistemas Operativos introducidos en 1985, desarrollados y comercializados por la empresa Microsoft la cual fue fundada en 1975 por Bill Gates y Paul Allen. Windows está disponible en versiones de 32 y 64 bits, asimismo ofrece una interfaz gráfica a través de ventanas (de ahí su nombre) permitiéndole al usuario trabajar en una o varias de éstas al mismo tiempo, realizando así diferentes tareas, además de ofrecerle distintas herramientas para simplificar el uso del equipo.

Los Sistemas Operativos iniciales de Microsoft manejaban el MS-DOS (Microsoft Disk Operativa System, Sistema Operativo de Disco de Microsoft), trabajaba con una interfaz en modo texto y una versión de 32 bits. Fue sustituido como SO principal por Sistemas Operativos que brindaban una interfaz gráfica las cuales contenían: menús desplegables, barras desplazables, iconos y cuadros de diálogo para facilitar el uso de los programas y del equipo. En la actualidad MS-DOS viene integrado como una aplicación de Windows, para acceder a él se debe ir a Símbolo del sistema o ejecutar el comando cms y en general se utiliza para realizar el mantenimiento del equipo, instalaciones, formateos, particiones, revisar las características de la red o acceder a una carpeta con un comando específico si no se conoce la ruta de ésta.

Es en la versión de Windows 95 cuando el Sistema Operativo tiene compatibilidad con Internet, conexión de red por acceso telefónico y nuevas funciones que facilitan la instalación de *hardware* y *software*, ofreciendo también funciones multimedia mejoradas, mejores gráficos apareciendo por primera vez en la interfaz el menú de inicio, la barra de tareas y los botones para minimizar, maximizar y cerrar ventanas.

Con Windows 2000 se mejora la confiabilidad, la facilidad de uso, la compatibilidad con Internet y con los equipos móviles, además se incluyen dispositivos inalámbricos avanzados, dispositivos USB e infrarrojos.

En el 2001 surge Windows XP con un diseño mejorado más fácil de utilizar, rápido, estable, incluyendo además un centro de servicios de ayuda, soporte técnico y actualizaciones de seguridad online, ésto debido a que se tenía mayor conciencia hacia los virus y piratas informáticos.

En el 2006 aparece Windows Vista introduciendo mejoras en la seguridad al poseer un firewall avanzado que evita el *spyware*, en las herramientas multimedia e interfaz gráfica, la barra de tareas, y los bordes de las ventanas adquieren una nueva apariencia al utilizar *XAML*[5] (*eXtensible Application Markup Language*, Lenguaje Extensible de Formato para Aplicaciones) y *DirectX*[6]. La búsqueda de archivos se realiza más rápidamente al contar con un explorador mejorado, además de tener la característica de "Ícono activo" que le permite al usuario ver lo que contiene el archivo sin la necesidad de abrirlo.

Debido a las fallas y poca eficiencia en esta versión (principalmente al consumir los requisitos del sistema) Microsoft tuvo que sacar la versión de Windows 7 mucho antes de la fecha prevista (comienzos del 2010). Esta versión apareció en el 2009 e incluye nuevas formar para trabajar con las ventanas mejorando la funcionalidad de la interfaz, haciéndola más amigable para el usuario, además de permitir el manejo táctil.

Finalmente, aparece Windows 8 introduciendo una interfaz totalmente nueva mejorando el manejo táctil, una nueva barra de tareas y una fácil administración de archivos, mejoras en la rapidez al cambiar de ventanas, el rendimiento del equipo y el uso de la batería.

Las versiones más recientes buscan corregir los errores de sus antecesoras, mejorando la seguridad, el rendimiento, la rapidez, el manejo del equipo, el diseño y la administración de carpetas y archivos.

Hoy en día la mayoría de los usuarios de bajo nivel están familiarizados con el Sistema Operativo modo gráfico, sin embargo, la línea de comandos sigue siendo utilizado por muchos usuarios de alto nivel (programadores).

[5] *XAML* : Lenguaje declarativo basado en *XML*, optimizado para mostrar interfaces gráficas a los usuarios.

[6] *DirectX:* Conjunto de *APIs* desarrolladas para facilitar tareas relacionadas con multimedia (juegos y vídeo especialmente), en plataforma Windows.

3.2.4.2. Linux

Linux es una familia de Sistemas Operativos libre basado en Unix. Fue creado por Linus Torvalds junto con un grupo de colaboradores en 1991 y actualmente es implementado por miles de usuarios en el mundo a través Internet gracias a que es código abierto, por lo tanto, cualquier usuario puede estudiar el código, escribir documentación, mejorar, ayudar en la depuración y renovar su diseño.

Dado que Linux se distribuye bajo la licencia de *GNU General Public License*, el código fuente siempre debe estar disponible para su modificación.

Su composición se basa de un núcleo central (*kernel*) quien es el encargado de administrar el *hardware* y el *software* responsable de tener al equipo listo para utilizarse, además de los programas que harán posible que el sistema funcione correctamente. Cada una de las distribuciones cuenta con su propia interfaz gráfica, bibliotecas y herramientas así como un sistema de administración de paquetes los cuales serán responsables de la instalación automática de *software*, asimismo estas distribuciones pueden adecuarse para necesidades específicas (por ejemplo: educativas, científicas, entre otras) o grupos específicos (por ejemplo: hogares, empresas, escuelas) además cada uno utiliza diferentes comandos para darle órdenes al equipo si se utiliza el modo texto.

Entre las distribuciones más conocidas se encuentran:

- Red Hat. Distribución Linux basado en paquetes, su nombre oficial es Red Hat Enterprise Linux (*RHEL*), desarrollado y gestionado por la compañía Red Hat. Fue la primera distribución que usó RPM para instalar y eliminar paquetes de forma individual. Cuenta con la herramienta *yum* que facilita la descarga de paquetes y actualización del *software*.

  Red Hat cuenta con una distribución dirigida a empresas (Red Hat Entreprise Linux AS) y otra orientada para los usuarios comerciales (Red Hat Enterprise Network). Ambas permiten actualizaciones al sistema, la diferencia entre ambas se encuentra en la gestión del sistema: al adquirir la primera el usuario tiene derecho a soporte mientras que con la segunda debes pagar por ello.

- Fedora. Distribución Linux basado en *RPM* creada en 2003 y gestionada por una comunidad internacional de desarrolladores y colaboradores además de contar con el apoyo y respaldo de Red Hat.

  Una de las diferencias entre está distribución y las demás de Linux es que los desarrolladores realizan los cambios en las fuentes originales en vez de utilizar los conocidos "*parches*", de este modo las actualizaciones podrán estar disponibles para cualquier variante GNU/Linux. La actualización entre versiones se realiza cada seis meses ofreciendo sólo un mes de apoyo a la versión anterior. También se pueden distribuir variantes personalizadas de Fedora (llamadas Fedora *spins*) para usuarios con necesidades específicas.

  Cuenta con la herramienta yum o su alternativa *apt-rpm* para la actualización y la descarga de paquetes.

- Debian. Distribución Linux basado en paquetes, los cuales contienen ejecutables, *scripts*, documentación e información de configuración gestionados por un sistema de seguimiento de fallos que será el encargado de mantener dichos paquetes actualizados e informar a los usuarios y desarrolladores si se presenta algún error y, de esta forma, arreglarlo lo más pronto posible. Los servidores de Debian comprueban que los paquetes provienen de un lugar auténtico, de esta forma disminuyen la presencia de programas dañinos para le sistema, además de sacar *parches* lo más pronto posible para arreglar los problemas de seguridad de los paquetes ya existentes así, cuando Debian se actualice a través de Internet, se puede descargar e instalar dichos *parches* de seguridad.

  Entre las ventajas que ofrece está distribución es la facilidad para instalar y desinstalarlo además de ser el primero en permitir actualizaciones sin la necesidad de reinstalación.

- Ubuntu. Distribución Linux compuesto por paquetes y basado totalmente en los principios de *software* libre. Está enfocado a la facilidad de uso e instalación, dirigido para usuarios de mediano nivel (de ahí su lema "Ubuntu: Linux para seres humanos"), por lo tanto, está diseñado para computadoras personales (de escritorio y laptops). Es patrocinada por la compañía británica Canonical Ltd. creada y financiada por el sudafricano Mark Shuttleworth además de contar con apoyo de usuarios internacionales y soporte profesional para su mantenimiento y gestión. Las versiones estables son liberadas cada 6 meses y se mantienen actualizadas hasta 18 meses después de su lanzamiento (hablando de seguridad).

> Esta distribución se basa en la libertad, descarga, copia, distribución, estudio, gestión y mejora de su *software* para cualquier propósito sin la necesidad de pago además del usuario debe poder utilizarlo en su idioma natal y a pesar de cualquier discapacidad. De esta forma no sólo se garantiza la disponibilidad de Ubuntu de forma gratuita si no también el usuario tiene el derecho a su modificación para que el sistema trabaje de acuerdo a sus necesidades.

Existen muchas más distribuciones de Linux, pero no se va a profundizar en ellos dado que el presente trabajo no se basa en Sistemas Operativos, sin embargo, la distribución Debian es relevante para la implementación del servidor, por lo tanto en el siguiente tema se profundizará un poco más sobre él.

3.2.4.3. Debian

En 1993 Ian Murdock da lugar al proyecto Debian, cuyo objetivo principal es distribuir un conjunto de *software* capaz de satisfacer la mayoría de las necesidades de los usuarios de una computadora de manera abierta en la línea de Linux y GNU, dando lugar al sistema operativo que han denominado Debian GNU/Linux.

Actualmente Debian cuenta con 18, 733 paquetes disponibles, manteniendo sus distribuciones en tres estados:

- *Stable* (estable). Contiene los paquetes oficiales; esta distribución garantiza que todo funcionará correctamente, por tal motivo está lista para usarse.
- *Testing* (de prueba). Contiene paquetes que aún no han sido aceptados en la distribución estable, pero que en cierto tiempo lo estarán.
- *Unstable* (inestable). Contiene paquetes en desarrollo; probablemente habrá paquetes que no funcionarán del todo bien, sin embargo tiene los paquetes más nuevos.

Con el paso del tiempo, los paquetes pueden pasar de una distribución inestable a una de prueba y finalmente llegan a estable después de una revisión minuciosa. Debian es considerado la distribución más robusta de Linux, debido a la gran cantidad de paquetes que tiene disponibles en sus repositorios, todas las arquitecturas que soporta y la garantía de que en su versión estable todo está probado.

Entre las ventajas que posee Debian se encuentra:

- Instalación sencilla, debido a que se puede realizar directamente desde un CD, una memoria portable (capacidad mínima de 2 Gigas dependiendo la versión) o inclusive desde Internet.
- Sistema de empaquetamiento de *software*, ya que, cuenta con *dpkg* cuyo sistema de empaquetamiento se encarga de los conflictos que pueda presentar el *software*.
- Paquetes bien integrados, en el cual, Debian empaqueta los grupos en un lugar determinado, se localizan todos los paquetes en un mismo sitio, además de que elimina todos los problemas de dependencias complejas. Esto lo hace más robusto.
- Actualizaciones fáciles, la actualización a una nueva versión de Debian es sencilla gracias a su sistema de empaquetamiento.
- Rápido y ligero en memoria, dado que Debian está basado en GNU/Linux ocupa pocos recursos y el código fuente está siempre accesible para su uso, lo que hace que el sistema funcione de manera más efectiva.
- *Software* de seguridad. Debian cuenta con software *GPG*[7] y *PGP*[8] que permite enviar correo entre los usuarios manteniendo su privacidad, además de que permite la creación de conexiones seguras a otras máquinas siempre que se tenga SSH instalado.

Además de contar con una comunidad de sistema de seguimiento de errores, el cual es público y por tal motivo se aconseja a los usuarios que envíen sus informes de errores y, de esta manera, se les pueda notificar a los usuarios la causa del error, como y cuando ha sido solucionado.

[7] *GPG* (*GNU Privacy Guard*). Herramienta de cifrado y firmas digitales, de *software* libre licenciado bajo GPL.
[8] *PGP* (*Pretty Good Privacy*). Sistema usado para la encriptación y desencriptación protegiendo así la información, además de facilitar la autenticación de documentos gracias a firmas digitales.

3.2.5. Comparativo de Sistemas Operativos

Como se observó en el tema anterior Windows y Linux tienen ciertas similitudes así como diferencias lo que le permite al usuario elegir con cual de los dos trabajar ya sea por los recursos que utiliza, las versiones, la facilidad de uso, entre otros.

A continuación se muestran las principales diferencias entre el Sistema Operativo Windows y Linux [15, 31]:

Características	**Windows**	**Linux**
Filosofía	Perteneciente a Microsoft, sólo ella puede manipularlo y distribuirlo	Sistema de código abierto, cualquiera puede manipularlo y distribuirlo
Precio	Depende de la versión que se desee adquirir	Gratuito
Desarrollo	Depende únicamente del personal de Microsoft	Depende de los programadores voluntarios a nivel mundial que deseen ayudar con la gestión del SO
Código Fuente	Privado	Abierto para los usuarios
Estabilidad	Poca, generalmente pide reiniciar la máquina para que ciertas actualizaciones e instalaciones funcionen correctamente, además si un proceso deja de correr la pantalla se bloquea, evitando así el seguir trabajando	Alta, no pide reiniciar constantemente, si una aplicación se llegara a bloquear se puede terminar el proceso de una manera sencilla, por lo que se puede seguir trabajando
Seguridad	La mayoría de los ataques, así como los virus, son dirigidos a equipos que tienen Windows, incluso los ataques pueden venir desde las mismas actualizaciones	Los ataques hacia él son excasos y son pocos los virus que pueden afectarle, por lo que generalmente se dice que es libre de virus
Facilidad de uso	Para usuarios de bajo y mediano nivel	Para usuarios de bajo, medio y alto nivel
Controladores de *hardware*	Deben bajarse de Internet	Los básicos están incluidos en la instalación de este SO
Difusión	Es más utilizado en equipos domésticos y en empresas	Poco usado en equipos domésticos, se utiliza más para servidores y administradores
Disponibilidad de aplicaciones	Cuenta con aplicaciones desde básicas hasta especializadas, van dirigidas a las máquinas personales y pequeñas empresas	Cuenta con aplicaciones desde básicas hasta especializadas, van dirigidas a servidores y grandes empresas
Precio de los programas	La mayoría son de pago, es necesario pagar por las licencias	Generalmente libres y gratuitos, aunque también hay de pago
Compatibilidad con otros SO	Presenta incompatibilidad con otros SO (incluso con versiones anteriores del mismo)	Buena compatibilidad con otros SO de la misma familia y de otros tipos
Actualizaciones	Debido a los errores que pueden surgir en la versión, es necesario estar actualizando constatemente y en ocasiones es forzoso reiniciar el equipo para su correcto funcionamiento	Sencillas, sólo se bajan los repositorios necesarios para mejorar su funcionamiento, no es necesario reiniciar el equipo

Tabla 3.2: Tabla comparativa entre Windows y Linux

La implementación del servidor debe hacerse bajo los requerimientos y recursos ofrecidos por la DICyG, por lo tanto, el Sistema Operativo a utilizar será Debian ya que es el sistema base para la implementación de servidores por su facilidad de instalación y uso.

3.2.6. Implementación de diseño

Como parte de las necesidades de comunicación identificadas en el objetivo, se consideró fundamental que la División de Ingenierías Civil y Geomática contara con un servicio institucional de correo electrónico, el cual

le permitirá a cada usuario intercambiar mensajes con otras personas dentro y fuera de la DICyG, además hacer uso de esta cuenta les dará cierta presencia en Internet y los vinculará a la comunidad académica institucional, UNAM.

Para llevar a cabo dicho objetivo, se realizó una pequeña encuesta al personal de la DICyG (tanto personal académico como administrativo) y se obtuvieron los siguientes resultados:

El personal de la DICyG:

- Usan el correo electrónico diariamente debido a que se comunican con administrativos, profesores y/o alumnos para sus diferentes tareas dentro y fuera de la misma.
- Cada usuario manda un aproximado de 30 correos electrónicos diariamente, recibiendo alrededor de 100 correos electrónicos a la semana.
- El mayor número de correos recibidos por un único usuario es de mil.
- Prevalece Windows como SO e Internet Explorer como navegador principal.
- Consideran el correo electrónico uno de los medios más efectivos para comunicarse a distancia, ya que, éste no tiene un costo, además de poder enviar cualquier tipo de archivo necesario para cumplir con sus actividades dentro y fuera de la División.
- Utilizan diferentes clientes de correo electrónico ya sea por su facilidad de uso, su interfaz o que cubra sus necesidades con la mayor efectividad posible. El cliente más común fue Windows Mail Live.
- La mayoría utiliza un correo comercial como: Gmail, Hotmail y Yahoo, pero también hay quienes utilizan tanto correo comercial como correo institucional siendo éste "unam.mx".
- Consideran que es importante un correo institucional para tener mayor respaldo al momento de comunicarse por correo electrónico.
- Los exploradores más utilizados por el personal de la División son:
  - Mozilla Firefox
  - Chrome
  - Internet Explorer

Para llevar a cabo la implementación del servidor de correo electrónico para la DICyG y realizar diversas pruebas, se trabajó con un equipo que contaba con las siguientes características:

- Software del servidor de prueba:
  - Debian Squeeze i386 netinst
- Hardware del servidor de prueba:
  - Intel Pentium 4 de 2.0 GHz
  - 256 MB de Memoria RAM
  - 80 GB de disco duro

El servidor de correo debe contar con las siguientes características:

- Disponible para plataformas Linux
- Ser código abierto
- Flexibilidad para poder adaptarlo de acuerdo a las necesidades de la división
- Ser una herramienta gratuita

- Ofrecer ventajas de seguridad
- Gran capacidad de almacenamiento
- Rendimiento óptimo
- Interfaz agradable para los usuarios
- Fácil instalación y gestión
- Ofrezca las tareas básicas para los usuarios (calendario, recordatorios, maletín)
- Compatible con los servidores *web* que se utilizan en la División

Al comparar los servidores de correo más utilizados, se concluyó que el servidor que ofrecía todas las características buscadas era Zimbra, por lo tanto, es el servidor que se implementará en la División.

3.2.6.1. Servidor de Correo Zimbra

La Suite de Colaboración Zimbra (*Zimbra Collaboration Suite* o ZCS) es un servidor de correo electrónico, mensajería y colaboración innovadora, basado en código abierto. Está disponible para diversas plataformas y distribuciones Linux y MacOS X. En poco tiempo, Zimbra se ha convertido en la solución líder a nivel mundial para las empresas, instituciones académicas y gubernamentales.

Zimbra ofrece tanto el servidor de correo como su respectivo cliente. Cuenta con dos tipos de versiones y cada una posee diferentes distribuciones: la versión de código abierto (software que tiene disponible su código fuente para cualquier usuario) y código cerrado (software que no tiene disponible su código fuente para cualquier usuario).

Las nuevas versiones y actualizaciones, facilitan día a día nuevas funcionalidades que mejoran la experiencia con el usuario, además de la seguridad y la robustez. Dispone del código fuente completo, documentación, herramientas de migración (para *Exchange*, por ejemplo) además de incluir protección anti-spam y antivirus.

Los elementos sobre los que está basado Zimbra son:

- Flexibilidad. Se puede personalizar fácilmente según las necesidades de la organización.
- Libertad. El cliente puede utilizar diversas plataformas *web* para su visualización y uso.
- Durabilidad. La capacidad de almacenamiento del servidor puede ampliarse así como el calendario haciendo fiable la fecha de recepción y envió de los mensajes.
- Bajo mantenimiento. Servicio completamente sencillo, puedes gestionarse tanto a través de la interfaz gráfica que ofrece el servidor como desde modo consola.

Algunas de las características especiales de Zimbra son las siguientes:

- Servidor ZCS: Utiliza componentes de código abierto como: Postfix, MySQL, OpenLDAP y Lucene, su interfaz de programación esta basado de SOAP (*Simple Object Access Protocol*), además actúa como servidor IMAP y POP3.
- Cliente ZCS: Contiene correo electrónico, contactos, calendarios compartidos, VoIP, entre otras herramientas. Todo esto incluido en el navegador *web* basado en AJAX.
- Compatibilidad con aplicaciones de escritorio: ZCS puede sincronizarse con: Microsoft Outlook, Entourage, Apple Mail, Libreta de direcciones e iCal, entre otros; además de contar con un soporte completo de aplicaciones IMAP/POP.
- Zimbra para móviles: ZCS puede sincronizarse con dispositivos que usen Windows Mobile, Symbian y Palm, sin la necesidad de un servidor adicional.

- Servidores ZCS Linux y Mac OS X: Cuenta con el agente MTA, antispam, antivirus, directorio, base de datos, herramientas de migración y consola de administración *web* basada en AJAX.

Zimbra no sólo permite personalizar el entorno si no también incluye soporte para sus temas (y si se desea hacer uno propio) y una versión sólo HTML para PCs que sean antiguas o entornos que no puedan hacer uso de JavaScript, además, permite la personalización de logos, textos y mensajes. Está diseñado sobre una arquitectura estable, usando tecnologías de código abierto. El servidor se integra con otros sistemas como el MTA, la base de datos y los paquetes de seguridad.

Zimbra empaqueta todos los componentes principales en un simple instalador y utiliza, entre otras:

- Tecnologías como:
  - Linux, Sistema Operativo de código libre. Jetty, como servidor de aplicaciones *web*.
  - Postfix, a través del cual, Zimbra incorpora varios filtros de seguridad, como antivirus y antispam.
  - MySQL, *software* de base de datos, el cual guarda los detalles de los mensajes.
  - OpenLDAP, proporciona la autenticación de usuario.
  - Lucene, motor de búsqueda que permite a los usuarios y administradores examinar mensajes a través de diversas carpetas de correo, ya sea metadatos o contenidos en el cuerpo del mensaje.
  - Verity, fuente de terceros capaz de convertir ciertos tipos de archivos adjuntos a HTML.
- Protocolos tales como:
  - SMTP: Se utiliza para que dos servidores de correo intercambien mensajes.
  - LMTP: Utilizado cuando se desea implementar un sistema donde el receptor del correo no maneje colas.
  - SOAP: Permite intercambiar información estructurada en un ambiente disperso y distribuido.
  - XML (*Extensible Markup Language*): Para el intercambio organizado y seguro de información.
  - IMAP: Permite el acceso al correo electrónico almacenados en un servidor.
  - POP: Se utiliza para obtener los mensajes guardados en el servidor y pasárselos al usuario. Zimbra reúne varios filtros de seguridad, como antivirus y antispam. Asimismo soporta por defecto los protocolos principales de cifrado de canal, los cuales proporcionan comunicaciones seguras por la red como lo son: SSL y TLS.

Entre los servicios que ofrece Zimbra se encuentran:

- Correo electrónico
- Libreta de direcciones
- Agendas
- Tareas
- Bloc de notas
- Calendario y gestión del mismo
- Filtros de correo
- Elección de tema
- Maletín de documentos
- Búsquedas avanzadas (en todos sus componentes y módulos)
- Guardar búsquedas
- Herramientas de importación de datos
- Permite ampliar sus herramientas con *zimlets* (extensiones o plugins para dar mayor funcionalidad a Zimbra)

3.2.6.2. Ventajas/Desventajas

A continuación se presentarán las principales ventajas como desventajas al utilizar Zimbra.

Ventajas de Zimbra, cuenta con:

- *SpamAssassom* y *ClamAV* incluidos (antispam y antivirus respectivamente).
- Interfaz *web* amigable, la cual brindará todo lo necesario tanto para el administrador, como para los usuarios.
- Protocolos SMTP, IMAP y POP incluidos.
- Sesión segura utilizando SSL para el administrador.

Para el cliente, puede:

- Personalizar su interfaz con el tema que más sea de su agrado.
- Facilidad para clasificar y organizar sus correos por medio de carpetas, etiquetas distintivas y filtros.
- Ordenar sus mensajes por: remitente, mensaje, fecha o importancia.
- Asignarle un alias a sus contactos.
- Importar y exportar sus listas de contactos, agendas, tareas, entre otros.
- Crear filtros para dirigir los correos automáticamente a la carpeta deseada.
- Almacenar cualquier tipo de archivos en el maletín para acceder rápidamente a él.
- Crear y gestionar varias agendas y calendarios.
- Visor de archivos adjuntos.
- Corrector ortográfico.
- Herramienta de autocompletar.
- Acceder su cuenta desde cualquier explorador (que cumpla con las características ya mencionadas) sin importar el SO que se esté utilizando.

Además de contar con:

- Una interfaz intuitiva, clara y fácil de manejar.
- Antivirus, filtro de *spam*.
- Enlace directo al administrador del servidor.

Para el administrador:

- Puede dar o denegar permisos, así como ciertas herramientas y temas.
- Fácil creación y eliminación de cuentas.
- Cuenta con una dirección de correo por si los usuarios quieren ponerse en contacto con él.
- Avisos diarios del estado del servidor así como anomalías.
- Fácil asignación de contraseñas en caso de extravío por parte de los usuarios.

- Puede crear cuentas con roles de administración limitada.
- Utiliza el directorio interno de Zimbra o directorios externos (Active Directory o LDAP) para la autenticación de los usuarios.
- El servidor le avisa al administrador cuando la capacidad de la memoria empieza a llegar a su límite.
- Se puede acceder al panel de administración desde cualquier explorador (que cumpla con las características ya mencionadas) sin importar el SO que se esté utilizando.

Entre las desventajas que tiene se encuentran:

- Consume gran cantidad de memoria para el óptimo desempeño de ciertas herramientas.
- Para que los cambios hechos al servidor surtan efecto éste debe reiniciarse.
- Guarda información en la caché, lo que consume memoria en la RAM del servidor.
- La información almacenada en la caché no puede borrarse ya que Zimbra tendría un mal rendimiento.

3.2.6.3. Requerimientos mínimos

Los requerimientos de *Zimbra Collaboration Suite* (ZCS) son, en comparación con otros productos similares, bastante bajos.

Requisitos del sistema para:

Servidores

Evaluación y pruebas

- Procesador Intel / AMD de 32-bits o 64-bits CPU de 1,5 GHz o superior.
- Mínimo 1 GB de RAM.
- Mínimo 5 GB de espacio libre en disco para el software y los registros.
- Espacio en tmp para instalaciones y actualizaciones.
- Mínimo 7 GB en opt.
- Espacio en memoria de 120 GB para almacenamiento de correos (promedio de 60 a 80 usuarios).
- Espacio en disco adicional para el almacenamiento de correo y la base de datos (éste depende del número de cuentas y de la cuota de disco asignada a cada una).

Requisitos generales

- Configuración del *firewall* ajustado en "no *firewall*" y desactivar la seguridad mejorada de Linux (SELinux).
- Para instalaciones de más de 100 cuentas no usar RAID-5 para mejor rendimiento.

Sistemas Operativos

- Red Hat Enterprise Linux
  - AS/ES 6, (64 bits) versión 7.1.3 y posteriores
  - AS/ES 5, (32 bits o 64 bits)

  - AS/ES 4, (32 bits o 64 bits)
- SUSE Linux Enterprise
  - Server 11 SP1 (64 bits)
  - Server 10 (32 bits o 64 bits)
- Ubuntu
  - 10.04 LTS Server Edition (64 bits)
  - 8.04 LTS Server Edition (32 bits o 64bits)
- Fedora
  - 13 (64 bits)
  - 11 (32 bits o 64bits)
- Debian 5 (32 bits o 64bits)
- Mac OS X: 10.4, 10.5, 10.6 o superior.

Sistema de archivos

- ext3 para distribuciones Linux.

Dependencias

- Para Red Hat Enterprise, Fedora Core y SUSE se debe contar con las siguientes dependencias:
  - Acceso como super usuario (*sudo*).
  - *NPTL*: Manejo de hilos.
  - *Libidn*: Codifica y descodifica nombres de dominio internacionalizados (IDNA).
  - *GMP*: GNU para la librería de precisión múltiple.
- Para Ubuntu 8.04 LTS o Ubuntu 10.04 LTS, y Debian 5 se debe contar con las siguientes dependencias:
- Acceso como super usuario (*sudo*).
- *libidn11*: Codifica y descodifica nombres de dominio internacionalizados
- *libpcre3*: Permite soportar expresiones regulares cuya sintaxis y semántica sean parecidas al lenguaje de Perl5.
- *libexpat1*: Librería compartida del ejecutable expat y manejo de *XML* de C.
- *libgmp3c2*: Librería que proporciona los archivos de cabecera y los enlaces simbólicos para la compilación y enlace de los programas.
- SSH: Permite instalar tanto el servidor como el cliente *OpenSSH*.
- Bind9: Permite instalar y modificar el servidor DNS así como sus archivos.

Administrador: Sistemas Operativos y Navegadores

- Windows: Windows 2000, XP, Vista o Windows 7 con cualquiera de los navegadores siguientes:
  - Internet Explorer 7 u 8
  - Firefox 3.0, 3.5 ó 3.6

  - Safari 4 ó 5
  - Google Chrome 2.1, 2.2 ó 2.3
- Mac OS X: 10.4, 10.5 ó 10.6 con cualquiera de los navegadores siguientes:
  - Firefox 3.0, 3.5 ó 3.6
  - Safari 4 ó 5
  - Google Chrome 2.1, 2.2 ó 2.3
- Linux: Red Hat, Ubuntu, Debian, Fedora o SUSE con cualquiera de los navegadores siguientes:
  Firefox 3.0, 3.5 ó 3.6
  Google Chrome 2.1, 2.2 ó 2.3

Clientes

Equipo

- Mínimo
  - Intel / AMD / con poder del CPU de 750MHz
  - 256 MB de RAM
  - Resolución de pantalla de 1024 x 768
  - Velocidad de Internet: 128 kbps o superior
- Recomendado
  - Intel / AMD / con poder del CPU de 1.5GHz
  - 512 MB de RAM
  - Resolución de pantalla de 1024 x 768
  - Velocidad de Internet: 128 kbps o superior

Sistemas Operativos y Navegadores

- Windows: Windows 2000, XP SP 3, Vista SP2 o Windows 7 con cualquiera de los siguientes navegadores:
  - Internet Explorer 6, 7 u 8 (para un mejor rendimiento usar de la versión 7 en adelante)
  - Firefox 3.0. 3.5 ó 3.6
  - Safari 3, 4 ó 5
  - Google Chrome 2.1, 2.2 ó 2.3
- Mac OS X: 10.4, 10.5 ó 10.6 o versiones siguientes con cualquiera de los siguientes navegadores:
  - Firefox 3.0, 3.5 ó 3.6
  - Safari 4 ó 5
  - Google Chrome 2.1, 2.2 ó 2.3
- Linux: Red Hat, Ubuntu, Debian, Fedora o SUSE con cualquiera de los siguientes navegadores:
  - Firefox 3.0, 3.5 ó 3.6
  - Google Chrome 2.1, 2.2 ó 2.3

Uso con otros clientes de correo

Sistema de combinaciones POP / IMAP

- Windows: XP SP 3, Vista SP2, Windows 7 con:
  - Outlook Express 6
  - Outlook 2003
  - (MAPI)
  - Thunderbird
- Fedora Core 4 o posterior con:
  - Thunderbird
- Mac OS X 10.4 o posterior con:

  Apple Mail

Teléfonos móviles

- Sincronización con dispositivos Blackberry a través del Zimbra connector para Blackberry Enterprise Server (BES).
- Sincronización en línea para dispositivos iPhone, Windows, Palm, Symbian.
- Aplicación *web* altamente funcional para correos, contactos y archivos en dispositivos compatibles con xHTML.

Se recomienda borrar completamente las claves de seguridad después de acceder al cliente de correo.

3.2.6.4. Componentes

La arquitectura del sistema Zimbra está formada por los siguientes componentes:

- *Zimbra Core*: Es la base de Zimbra debido a que incluye los archivos base de configuración, librerías, utilidades y herramientas de exanimación requeridas para el buen funcionamiento del servidor.
- *Zimbra LDAP*: Base de datos optimizada de solo lectura para el almacenamiento y la gestión de usuarios.
- *Zimbra Zmconfigd*: Gestiona y asegura que se están ejecutando los procesos en cada uno de los nodos.
- *Zimbra Logger*: Agrega la posibilidad de disponer de *logs*, informes, estadísticas gráficas y seguimiento de mensajes en la consola de administración.
- *Zimbra Mailbox*: Almacenamiento de correos de entrada, además de crear una copia de seguridad y archivos de registro.
- *Zimbra MTA*: Encargado de dirigir los correo, basado en Postfix. El MTA Zimbra también incluye *SpamAssassin* como filtro *antispam*, *ClamAV* como antivirus y *Amavis* como filtro de contenidos.
- *Zimbra SNMP*: Monitorea información constante del estado del sistema. Además genera/envía alarmas (*traps* SNMP) cuando ocurren ciertos eventos, como pueden ser: error en la interfaz, la carga de procesos excede un límite, por mencionar algunos.
- *Zimbra Store*: Encargado del almacenamiento de correo electrónico en una base de datos de MySQL.
- *Zimbra Spell*: Utilizará Aspell como programa de revisión ortográfica para el Cliente.

3.2.6.5. Configuración e Instalación

Para que el servidor Zimbra funcione correctamente antes debe de configurarse la red. Al momento de estar instalando Debian, en el menú principal de la instalación, seleccionar la opción Configurar la red después configurar la red manualmente e ingresar la IP, la máscara de red, la pasarela, los DNS, nombre del equipo y el dominio que tendrá el servidor.

Cuando Debian queda instalado se procede a configurarlo para adecuarlo al servidor Zimbra.

Configuración de Debian:

1. Se accede al sistema como super usuario y se ingresa la contraseña.
2. Si por alguna razón no se configuró la conexión de red en Debian, se debe modificar el archivo *interfaces* para agregar los datos de la red y dejar la IP estática.

   ```
   # The primary network interface
   allow-hotplug eth0
   iface eth0 inet static

   address 192.x.x.x
   netmask 255.255.255.0
   network 192.x.x.x
   broadcast 192.x.x.x
   gateway 192.x.x.x

   #dns
   dns-nameservers 132.x.x.x 132.x.x.x
   dns-search ejemplo_dominio.mx
   ```

   Posteriormente se debe reiniciar el servidor con *reboot*. (Si este paso se hizo en Debian no esta de más ingresar en *interfaces* para corroborar que todo está configurado correctamente).
3. En *source.list* se agregan los repositorios donde se descargará el software necesario para la instalación de zimbra.

   ```
   # Multimedia
   deb http://www.deb-multimedia.org/ squeeze main
   deb-src http://www.deb-multimedia.org/ squeeze main
   ```

4. Se agrega la clave *gpg* para poder acceder a los repositorios.

   ```
   gpg --keyserver pgpkeys.mit.edu --recv-key 07DC563D1F41B907 &&
   gpg -a  --export 07DC563D1F41B907 | sudo apt-key add -
   ```

5. Se actualiza la lista de paquetes disponibles y sus versiones con *apt-get update*.
6. Se instala la *key* del repositorio multimedia.

   ```
   apt-get install deb-multimedia-keyring
   ```

7. Se instalan los nuevos paquetes con *apt-get upgrade*.
8. Se instala el servidor DNS y SSH para poder acceder desde otro equipo.

   ```
   apt-get install openssh-server bind9
   ```

9. Se configuran los archivos para el servidor DNS.

   a) Se edita el archivo *hostname* y se agrega el nombre del servidor y del dominio.

   ```
   nombre_servidor.ejemplo_dominio.mx
   ```

b) Se edita el archivo *hosts* y se agrega la IP del servidor, el nombre del servidor y el dominio.

```
127.0.0.1 localhost.localdomain localhost
192.x.x.x nombre_servidor.ejemplo_dominio.mx nombre_servidor
```

c) Se edita el archivo *resolv.conf*. En *search* se agrega el nombre del dominio y en *nameserver* la IP del servidor.

```
search ejemplo_dominio.mx
nameserver 192.x.x.x
```

d) Se edita el archivo *named.conf.local*. En el primer *zone* se agrega el nombre del dominio, después de *db.* se agrega el nombre que tendrá el archivo. En el *zone* siguiente se coloca de manera inversa los tres primeros octetos de la dirección IP del servidor, después de *db.* se agrega el nombre que tendrá el archivo. (Se recomienda nombrar los archivos de la misma manera que esta en *zone* para evitar confusiones al momento de modificarlos).

```
//include "/etc/bind/zones.rfc1918";
zone "ejemplo_dominio.mx" {
type master;
file "/etc/bind/db.nombre_ejemplo_dominio.mx";
};

zone "x.x.x.in-addr.arpa" { //IP inversa
type master;
file "/etc/bind/db.nombre_IP";
};
```

e) Se edita el archivo *named.conf.options*, se agrega el puerto por donde se hará la petición y en *forwarders* se colocan los DNS.

```
// the all-0's placeholder.
query-source address * port 53;

forwarders {
132.x.x.x; 132.x.x.x;
};
```

f) Se copia el archivo *db.local* a *db.nombre_ejemplo_dominio.mx*.

g) Se edita el archivo *db.nombre_ejemplo_dominio.mx*. En *SOA* se coloca el nombre del dominio así como en *root*.

```
;
; BIND data file for local loopback interface
;
$ TTL 604800
@ IN SOA ejemplo_dominio.mx. root.ejemplo_dominio.mx. (
2 ; Serial
604800 ; Refresh
86400 ; Retry
2419200 ; Expire
604800 ) ; Negative Cache TTL
;

IN NS dns.ejemplo_dominio.mx.
IN MX 10 mail.ejemplo_dominio.mx.

nombre_servidor IN A 192.x.x.x
dns             IN A 192.x.x.x
mail            IN A 192.x.x.x
www             IN A 192.x.x.x
```

h) Se copia el archivo *db.127* a *db.nombre_IP*.

i) Se edita el archivo *db.nombre_IP*. En *SOA* se coloca el nombre del dominio así como en *root*.

```
;
; BIND data file for local loopback interface
;
$ TTL 604800
@ IN SOA ejemplo_dominio.mx. root.ejemplo_dominio.mx. (
1 ; Serial
604800 ; Refresh
86400 ; Retry
2419200 ; Expire
604800 ) ; Negative Cache TTL
;

IN NS dns.ejemplo_dominio.mx.

228 IN PTR dns.ejemplo_dominio.mx.
228 IN PTR www.ejemplo_dominio.mx.
228 IN PTR mail.ejemplo_dominio.mx.
228 IN PTR nombre_servidor.ejemplo_dominio.mx.
```

j) Se reinicia el servidor DNS con *restart*.

10. Se instalan las dependencias de Zimbra.

```
apt-get install libc6-i686 sudo libidn11 curl fetchmail libgmp3c2 libexpat1
libxml2 libstdc++6 libpcre3 libgmp3-dev ssh  sysstat libltdl7 libltdl-dev
perl-modules wget lzma
```

11. Dado que Zimbra no tiene una versión estable para Debian Squeeze se descarga e instala la versión más reciente de *i386* del paquete *dpkg*[9] para evitar problemas en la instalación.

```
wget
http://security.ubuntu.com/ubuntu/pool/main/d/dpkg/dpkg_1.15.5.6ubuntu4.5
_i386.deb

dpkg -i dpkg_1.15.5.6ubuntu4.5_i386.deb
```

12. Se descarga y se descomprime el paquete de Zimbra.

```
wget
http://files2.zimbra.com/downloads/7.1.1_GA/zcs-7.1.1_GA_3196.DEBIAN5
.20110527000857.tgz

tar -xzvf zcs-7.1.1_GA_3196.DEBIAN5.20110527000857.tgz
```

Instalación de Zimbra

1. Se cambia al directorio de Zimbra y se procede a su instalación.

```
./install.sh --platform-override
```

2. La instalación pregunta si se aceptan los términos de la licencia, se presiona *enter* o *y*.

```
PLEASE READ THIS AGREEMENT CAREFULLY BEFORE USING THE SOFTWARE. ZIMBRA,
INC. ("ZIMBRA")
WILL ONLY LICENSE THIS SOFTWARE TO YOU IF YOU FIRST ACCEPT THE TERMS OF
THIS AGREEMENT.
THIS AGREEMENT, THEN DO NOT DOWNLOAD, INSTALL OR USE THE PRODUCT.

License Terms for the Zimbra Collaboration Suite:
http://www.zimbra.com/license/zimbra_public_eula_2.1.html

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

[9] *Dpkg*. Base del sistema de gestión de paquetes de Debian GNU/Linux.

3. En la instalación de los componentes de Zimbra se deja todo por defecto, por lo tanto se presiona *enter* o *y*.

```
Install zimbra-ldap [Y]
Install zimbra-logger [Y]
Install zimbra-mta [Y]
Install zimbra-snmp [Y]
Install zimbra-store [Y]
Install zimbra-apache [Y]
Install zimbra-spell [Y]
Install zimbra-memcached [N]
Install zimbra-proxy [N]
```

4. La instalación indica que los paquetes son para Debian 5 y que la versión no es compatible y pregunta si se desea seguir con la instalación. Gracias a la configuración hecha anteriormente no habrá problema con la instalación así que se presiona *enter* o *y*.

```
This platform is DEBIAN6
Packages found: DEBIAN5 This may or may not work.
Using packages for a platform in which they were not designed for may
result in an installation that is NOT usable.
Your support options may be limited if you choose to continue

Install anyway? [N]
```

5. La instalación indica que el sistema va a ser modificado, se presiona *enter* o *y*.

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

6. Se pide cambiar el dominio, se presiona *enter* o *y*. Se quita el *nombre_servidor* que lo antecede para dejar solamente el *nombre del dominio*.

```
DNS ERROR resolving MX for nombre_servidor.ejemplo_dominio.mx It is suggested
that the domain name have an MX record configured in DNS

Change domain name? [Yes]
Create domain: [nombre_servidor.ejemplo_dominio.mx]ejemplo_dominio.mx
```

7. Al llegar al menú, se presiona el número 3 para asignarle una contraseña al administrador y se presiona *enter*.

```
Main menu
1) Common Configuration:
2) zimbra-ldap: Enabled
3) zimbra-store: Enabled
        +Create Admin User: yes
        +Admin user to create: admin@ejemplo_dominio.mx
      ***+Admin Password UNSET
        +Anti-virus quarantine user:
        virus-quarantine.uh5a2s07t@ejemplo_dominio.mx
        +Enable automated spam training: yes
        +Spam training user: spam.vaepsdslhb@ejemplo_dominio.mx
        +Non-spam(Ham) training user:ham.lbl287dw@ejemplo_dominio.mx
        +SMTP host: zimbra.ejemplo_dominio.mx
        +Web server HTTP port: 80
        +Web server HTTPS port: 443
        +Web server mode: http
        +IMAP server port: 143
        +IMAP server SSL port: 993
        +POP server port: 110
        +POP server SSL port: 995
        +Use spell check server: yes
```

```
        +Spell server URL:
         http://zimbra.ejemplo_dominio.mx:7780/aspell.php
        +Configure for use with mail proxy: FALSE
        +Configure for use with web proxy: FALSE
        +Enable version update checks: TRUE
        +Enable version update notifications: TRUE
        +Version update notification email: admin@ejemplo_dominio.mx
        +Version update source email: admin@ejemplo_dominio.mx
4) zimbra-mta: Enabled
5) zimbra-snmp: Enabled
6) zimbra-logger: Enabled
7) zimbra-spell: Enabled
8) Default Class of Service Configuration:
        r) Start servers after configuration yes
        s) Save config to file
        x) Expand menu
        q) Quit

Address unconfigured (**) items  (? - help)
```

8. Dentro de este menú se encuentra la configuración básica del servidor, como los puertos que utiliza para cada servicio, el nombre de administrador, por mencionar algunos. Se presiona el número 4 para asignarle una contraseña al administrador y se presiona *enter*.

```
Store configuration
        1) Status: Enabled
        2) Create Admin User: yes
        3) Admin user to create: admin@ejemplo_dominio.mx
    **  4) Admin Password UNSET
        5) Anti-virus quarantine user:
           virus-quarantine.uh5a2s07t@ejemplo_dominio.mx
        6) Enable automated spam training: yes
        7) Spam training user: spam.vaepsdslhb@ ejemplo_dominio.mx
        8) Non-spam(Ham) training user: ham.lbl287dw@ejemplo_dominio.mx
        9) SMTP host: zimbra. ejemplo_dominio
        10) Web server HTTP port: 80
        11) Web server HTTPS port: 443
        12) Web server mode: http
        13) IMAP server port: 143
        14) IMAP server SSL port: 993
        15) POP server port: 110
        16) POP server SSL port: 995
        17) Use spell check server: yes
        18) Spell server URL:
            http://zimbra.ejemplo_dominio:7780/aspell.php
        19) Configure for use with mail proxy: FALSE
        20) Configure for use with web proxy: FALSE
        21) Enable version update checks: TRUE
        22) Enable version update notifications: TRUE
        23) Version update notification email: admin@ejemplo_dominio.mx
        24) Version update source email: admin@ejemplo_dominio.mx

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

9. Se ingresa la contraseña deseada y se presiona *enter* para regresar al menú anterior.

```
Password for admin@ejemplo_dominio.mx (min 6 characters): [contraseña]
```

10. Se presiona *a* para que se apliquen los cambios hechos. La instalación preguntará si guarda la configuración de los datos.

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

11. Se presiona *enter* o *y* paa salvar la configuración de los archivos.

```
Save configuration data to a file? [Yes]
Save config in file: [/opt/zimbra/config.6520]
Saving config in /opt/zimbra/config.6520...done.
```

12. La instalación indica que el sistema ha sido modificado, se presiona *enter* o *y* para continuar.

```
The system will be modified - continue? [No] y
```

13. La instalación pregunta si se desea notificar a Zimbra de la instalación, se presiona *y* o *n* según se desee (la respuesta no afecta en nada a la instalación).

```
You have the option of notifying Zimbra of your installation. This helps us to
track the uptake of the Zimbra Collaboration Suite. The only information that
will be transmitted is:  The VERSION of zcs installed (7.1.1_GA_3196_DEBIAN6)
The ADMIN EMAIL ADDRESS created admin@ejemplo_dominio.mx)

Notify Zimbra of your installation? [Yes]
```

14. Cuando la instalación finaliza, se presiona *enter*.

```
Configuration complete - press return to exit
```

El servidor automáticamente levanta los servicios.

```
Starting ldap...Done.
Starting zmconfigd...Done.
Starting logger...Done.
Starting mailbox...Done.
Starting antispam...Done.
Starting antivirus...Done.
Starting snmp...Done.
Starting spell...Done.
Starting mta...Done.
Starting stats...Done.
```

Para visualizar la cuenta del administrador, en el navegador se ingresa a la dirección `https://192.x.x.x:7071/zimbraAdmin`. La primera vez que se ingresa a la cuenta del administrador saldrá el el certificado de seguridad, dar en la opción *Continuar de todos modos* para poder acceder la cuenta.

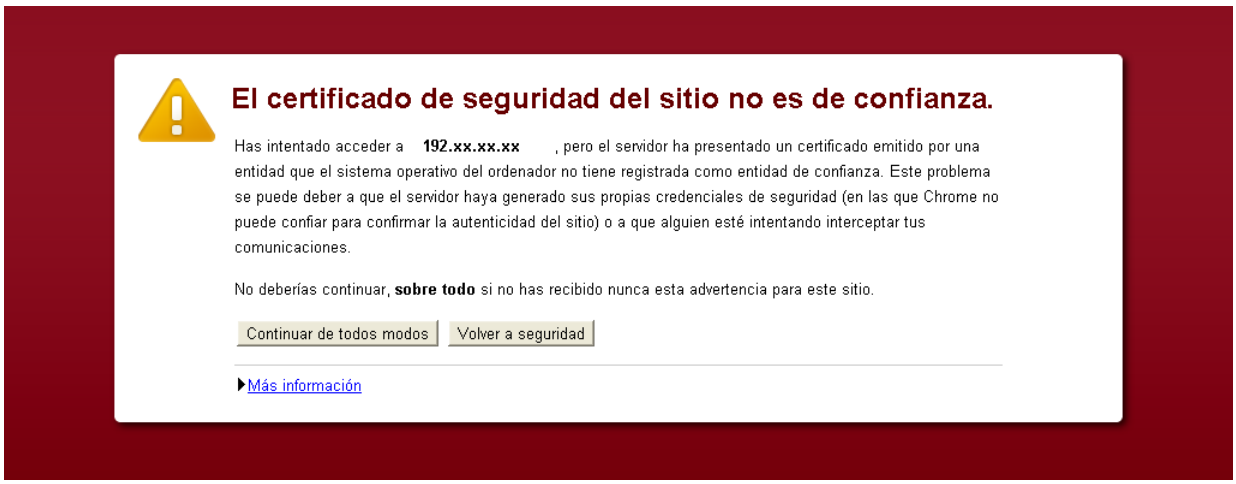


Figura 3.1: Certificado de seguridad bajo el explorador Chrome

Una vez aceptado, se podrá visualizar la pantalla de bienvenida del administrador.

Figura 3.2: Pantalla de bienvenida del administrador

Para visualizar la pantalla de bienvenida del cliente se debe ingresar a la dirección `https://192.x.x.x`.

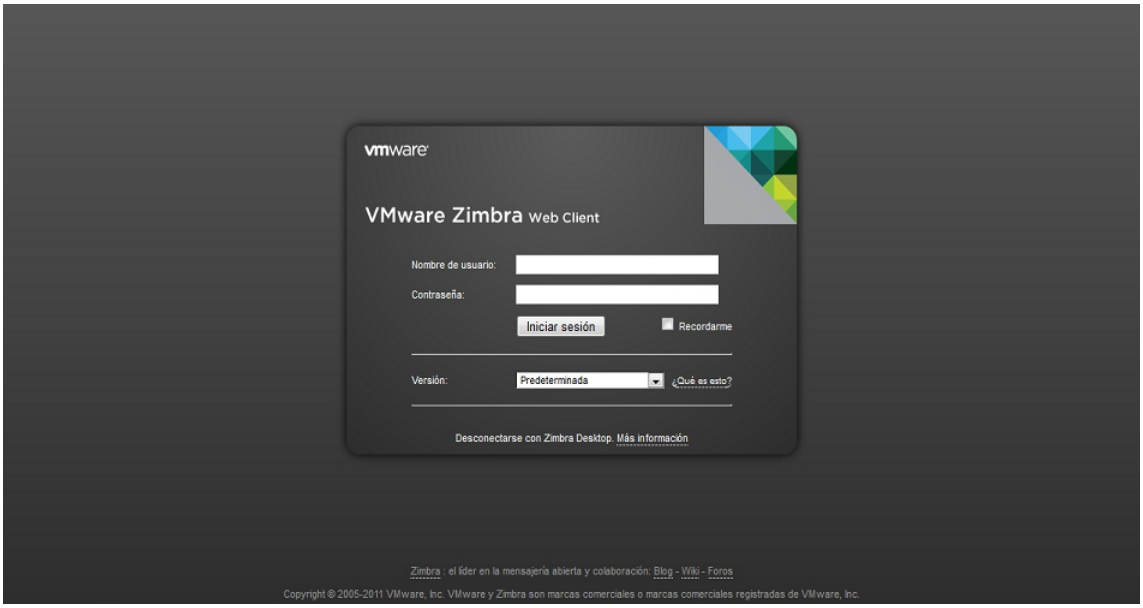


Figura 3.3: Pantalla de bienvenida del cliente

Para apagar el servidor se accede a Zimbra con el comando *su zimbra* y se ingresa el comando *zmcontrol stop*.

Para levantar el servidor se accede a Zimbra con el comando *su zimbra* y se ingresa el comando *zmcontrol start*.

Para visualizar el estado del servidor se accede a Zimbra con el comando *su zimbra* y se ingresa el comando *zmcontrol status*.

Para reiniciar el servidor se accede a Zimbra con el comando *su zimbra* y se ingresa el comando *zmcontrol restart*.

Configuración y actualización del antivirus

Como se ha mencionado anteriormente, Zimbra viene con un antivirus propio que es responsable de brindar la seguridad al servidor. Este antivirus se llama *Clam*. (*ClamAV* por el conjunto de palabras *CLAM Anti Virus*).

ClamAV es un *software* de antivirus de código abierto para UNIX, diseñado especialmente para los análisis de correo electrónico además de detectar virus, troyanos y gusanos. Ofrece una serie de servicios incluidos un demonio multihilo flexible y escalable, un escáner de línea de comandos y una avanzada herramienta para actualizaciones automáticas de la base de datos.

Cada versión de Zimbra viene con una versión de *ClamAV*, por lo tanto es necesario actualizar no sólo la base de virus, sino tener la última versión estable del antivirus.

ZCS viene con la versión 0.97.6 de *ClamAV*, a continuación se mostrará lo que se tiene que hacer para actualizar el antivirus a su versión más reciente y estable. (No es necesario detener el servidor en los primeros pasos).

1. Se accede al sistema como super usuario y se ingresa la contraseña.
2. Se desinstala cron con apt-get remove cron.
3. Se agregan las dependencias para la nueva versión.

   ```
   aptitude install clamav clamav-freshclam clamav-docs  zlib1g-dev libclamav-dev
   check libbz2-dev pkg-config libxfont-dev bash-builtins libc6-dev libssl-dev
   gcc make
   ```

4. Se descarga la versión más estable y se descomprime.

   ```
   wget http://sourceforge.net/projects/clamav/files/clamav/0.97.8/clamav-0.97.8.
   tar.gz

   tar zvxf clamav-0.97.8.tar.gz
   ```

   Nota: Para saber que versiones se encuentran disponibles al siguiente link:

   `http://sourceforge.net/projects/clamav/files/clamav/`

5. Mover la carpeta obtenida a zimbra con *mv /ruta_origen /ruta_destino*.
6. Cambiarse a la nueva carpeta con *cd /carpeta_deseada*.
7. Ligar la nueva carpeta con el usuario zimbra y se realiza el *check*.

   ```
   ./configure --prefix=/.../zimbra/clamav-0.97.8 --with-user=zimbra
   --with-group=zimbra  --enable-check
   ```

8. Se ejecuta el *make*.
9. Para comprobar que todo está bien se ejecuta *make check*.

   ```
   Pass: check_clamav
   Pass: check_freshclam.sh
   Pass: check_sigtool.sh
   Skip: check_unit_vg.sh
   Pass: check1_clamscan.sh
   Pass: check2_clamd.sh
   Pass: check3_clamd.sh
   Pass: check4_clamd.sh
   Skip: check5_clamd_vg.sh
   Skip: check6_clamd_vg.sh
   Skip: check7_clamd_hg.sh
   Skip: check8_clamd_hg.sh
   Skip: check9_clamscan_vg.sh
   ```

```
============================
All 7 tests passed
(6 tests were not run)
============================
```

10. Para instalar la nueva versión en la carpeta se ejecuta *make install*.
11. Se ingresa como usuario zimbra con el comando *su zimbra*.
12. Se detiene el antivirus con el comando *zmamavisdctl stop*.
13. Se sale del usuario zimbra con el comando *exit*.
14. Se hace propietario de la nueva versión al usuario zimbra.

    ```
    ln -s /opt/zimbra/clamav-0.97.8 /opt/zimbra/clamav chown -R zimbra:zimbra
    /opt/zimbra/clamav-0.97.8
    ```

15. Se ingresa al usuario zimbra con el comando *su zimbra*.
16. Se inicia el antivirus con el comando *zmamavisdctl start*.
17. Se sale del usuario zimbra con el comando *exit*.

Consideraciones:

- Para actualizar la nueva base de virus se ejecuta el comando *freshclam*.
- Para escanear se ejecuta el comando *clamscan* o *clamscan -r /carpeta* si se desea una ruta en específico.

Listas Negras

Con el fin de fortalecer al servidor en cuanto a la seguridad, se ingresaron listas negras adicionales para evitar el correo no deseado. Zimbra recomienda varias listas negras que en conjunto evitan los *host* no válidos, *FQDN* falsos, direcciones inválidas de correo, clientes y bandas de *spam*, entre otros.

Primero, se accede al archivo donde se guardarán y usarán las listas.

```
zmprov gacf | grep zimbraMtaRestriction
```

Una vez dentro, se agregan las listas negras con el comando *zmprov mcf*.

```
+zimbraMtaRestriction "reject_invalid_hostname"
+zimbraMtaRestriction "reject_non_fqdn_hostname"
+zimbraMtaRestriction "reject_non_fqdn_sender"
+zimbraMtaRestriction "reject_rbl_client zen.spamhaus.org"
+zimbraMtaRestriction "reject_rbl_client psbl.surriel.com"
+zimbraMtaRestriction "reject_rbl_client dnsbl.dronebl.org"
+zimbraMtaRestriction "reject_rbl_client xbl.spamhaus.org"
+zimbraMtaRestriction "reject_rbl_client sbl.spamhaus.org"
+zimbraMtaRestriction "reject_rbl_client sbl-xbl.spamhaus.org"
+zimbraMtaRestriction "reject_rbl_client list.dsbl.org"
+zimbraMtaRestriction "reject_rbl_client dnsbl.njabl.org"
+zimbraMtaRestriction "reject_rbl_client cbl.abuseat.org"
+zimbraMtaRestriction "reject_rbl_client bl.spamcop.net"
+zimbraMtaRestriction "reject_rbl_client dnsbl.sorbs.net"
+zimbraMtaRestriction "reject_rbl_client relays.mail-abuse.org"
```

3.2.6.6. Verificación de configuraciones

Servidor

Para confirmar que los servicios se han levantado correctamente se puede visualizar directamente en el servidor, el cual mostrará lo siguiente al momento de comprobar su estado.

```
antispam          Running
antivirus         Running
ldap              Running
logger            Running
mailbox  Stopped  Running
mta               Running
snmp              Running
spell             Running
stats             Running
zmconfigd         Running
```

Otra manera de visualizarlo es a través de la interfaz gráfica del administrador, al acceder a la cuenta se visualizarán los servicios y el estado de éstos, si todo es correcto se verán palomeados en verde.

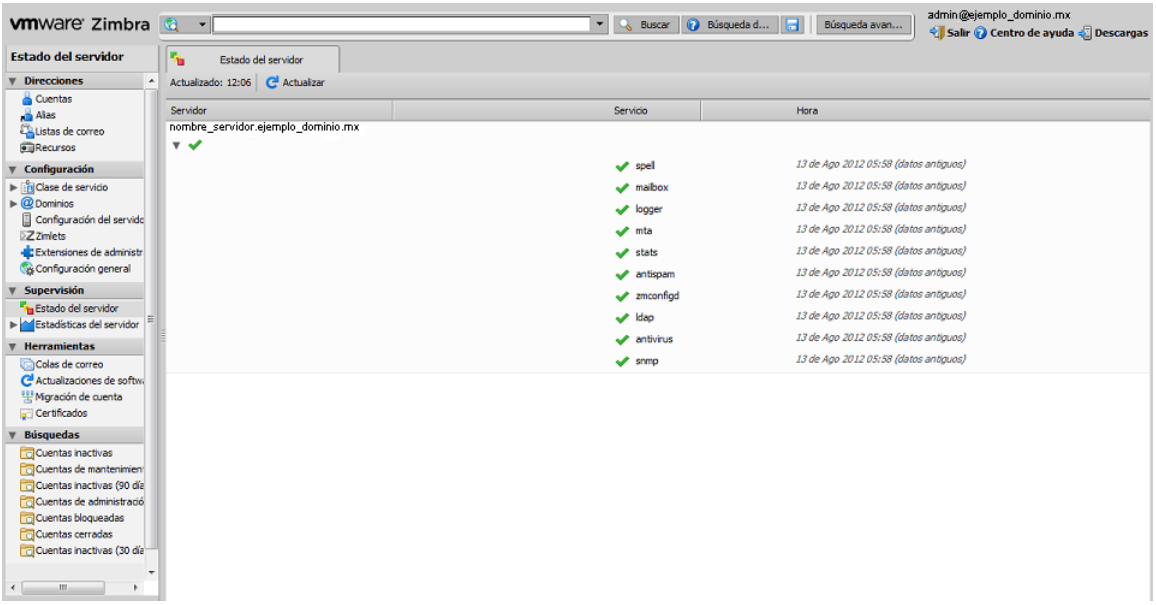


Figura 3.4: Panel de Administración

ClamAV en funcionanamiento

Para verificar que el antivirus está funcionando correctamente se ejecuta *tail -f /.../.../log/clamd.log*, el cual mostrará el estado del antivirus.

```
Wed Aug 28 12:40:25 2013 -> SelfCheck: Database status OK.
Wed Aug 28 13:12:05 2013 -> SelfCheck: Database status OK.
Wed Aug 28 13:46:59 2013 -> SelfCheck: Database status OK.
Wed Aug 28 14:13:33 2013 -> SelfCheck: Database status OK.
Wed Aug 28 15:30:18 2013 -> Reading databases from /.../...
/data/clamav/db Wed Aug 28 15:30:26 2013 -> Database correctly
reloaded (396672 signatures)
Wed Aug 28 16:10:33 2013 -> SelfCheck: Database status OK.
Wed Aug 28 17:35:44 2013 -> SelfCheck: Database status OK.
```

Actualización del *ClamAV*

Para confirmar que la actualización del antivirus fue correcta, se debe ejecutar fleshclam, se mostrará el siguiente mensaje en el servidor, el cual indica, la versión del antivirus, el día que se hizo la actualización así como la versión de la base de datos.

```
ClamAV update process started at Wed Aug 28 12:02:37 2013-08-28
WARNING: Your ClamAv installation is OUTDATED!
WARNING: Local versión: 0.97.8 Recommended versión: 0.97.8
DON'T PANIC! Read http://www.clamav.net/support/fac
Main.cld is up to date (versión: 55, sigs: 2424225, f-level:60, builder:neo)
Daily.cld is up to date (versión:17895, sigs: 376100, f-level:63, builder:neo)
Bytecode.cld is up to date (versión:226, sigs:43, f-level:63,  builder:neo)
```

Cliente

Si el servidor está funcionando correctamente, cuando se acceda a la cuenta del cliente se podrá observar su bandeja de entrada.

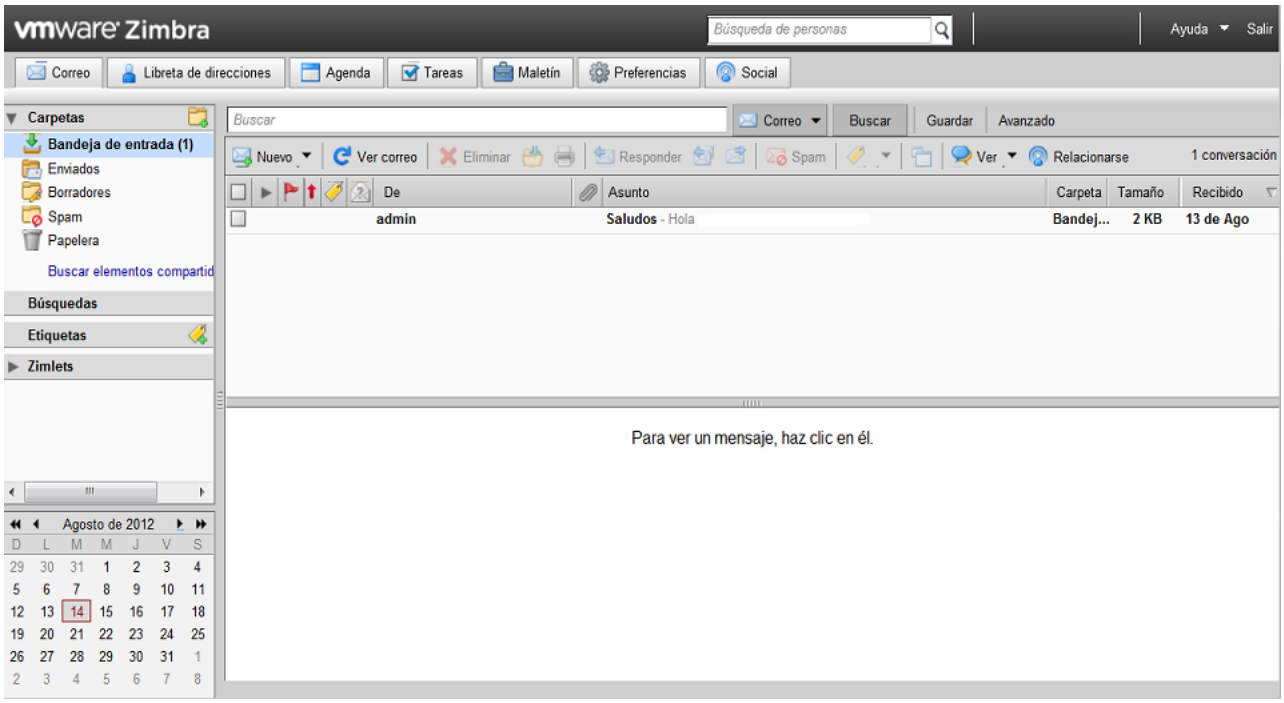


Figura 3.5: Bandeja de entrada del cliente

Tamaño cuenta

Para verificar que el tamaño de las cuotas se está respetando, se le asigno a una cuenta 4GB de espacio y se le enviaron correos con archivos adjuntos para ocupar el mayor espacio posible.

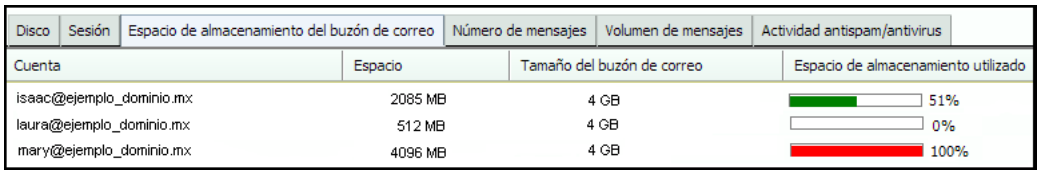


Figura 3.6: Capacidad de las cuotas

El correo se saturó cuando estaba cerca de llegar a los 4 GB, por lo tanto, el tamaño de las cuotas quedó comprobado.

3.2.6.7. Incidencias en la instalación e implementación

Para la instalación de Zimbra se siguieron varios tutoriales, no se tomó uno en particular ya que no venían completos, por lo tanto se presentaban errores o aparecían mensajes que no aparecían en la página consultada.

Entre los errores que se encontraron:

Dirección del repositorio incorrecto

- Error: Al ingresar la dirección, ésta no se encontraba, por lo que se buscó una que aún existiera para poder bajar los archivos necesarios para la instalación.
- Solución: Se utilizó la siguiente dirección para descargar los archivos necesarios para la instalación.

```
# Multimedia
deb http://www.deb-multimedia.org/ squeeze main
deb-src http://www.deb-multimedia.org/ squeeze main
```

No se tienen los permisos para el repositorio multimedia

- Error: Al agregar los repositorios multimedia salía error de *GPG*: las firmas no se pueden verificar porque la llave pública no esta disponible.
- Solución: Ingresar la llave gpg para que el servidor la tuviera disponible. Ejecutar la siguiente línea:

```
gpg --keyserver pgpkeys.mit.edu --recv-key 07DC563D1F41B907 &&
gpg -a  --export 07DC563D1F41B907 | sudo apt-key add -
```

Configuración del *Bind9*

- Error: Al querer reiniciar el *Bind9* se obtenía el mensaje "*missing } in conf.local*" y/o "*missing } in conf.options*"
- Solución: Revisar conf.local y/o conf.options y agregarle la llave o datos faltantes.

Librerías

- Error: Al agregar las librerías que se mostraban en la página muchas no las encontraba el sistema.
- Solución: El sistema indicaba qué librerías eran obsoletas y buscaba la nueva versión, quedando las siguientes:

```
apt-get install libc6-i686 sudo libidn11 curl fetchmail libgmp3c2 libexpat1
libxml2 libstdc++6 libpcre3 libgmp3-dev ssh  sysstat libltdl7 libltdl-dev
perl-modules wget lzma
```

Missing: *libgmp3*

- Error: Al momento de hacer *./install.sh –platform-override* indicaba que no contaba con dicha librería.
- Solución: Se modificaba el archivo utilfunc.sh y se sustituía *libgmp3* por *libgmp3c2*. Para evitar este error, se agregaba la librería al momento de instalar las librerías finales.

No se encuentra el *dpkg*

- Error: Zimbra no tiene una versión estable para Debian Squeeze.
- Solución: Descargar e instalar una versión antigua del paquete *dpkg* con la última versión de *i386* para evitar problemas al momento de la instalación.

```
wget
http://security.ubuntu.com/ubuntu/pool/main/d/dpkg/dpkg_1.15.5.6ubuntu4.5
_i386.deb

dpkg -i dpkg_1.15.5.6ubuntu4.5_i386.deb
```

No encuentran los DNS

- Error: Al llegar al paso, donde el servidor pide cambiar de DNS se mostraba: error DNS. Ésto indicaba que se hizo mal la configuración del *BIND9*.
- Solución: Revisar los archivos: *hostname*, *hosts*, *resolv.conf*, *named.conf.local*, *named.conf.options*, *db.nombre_ejemplo_dominio.mx*, *db.nombre_IP* para detectar donde estuvo el error y evitarlo en el futuro, ya que, llegado a este paso, es necesario volver a ejecutar la instalación de Zimbra.

La hora del servidor no coincide con el equipo del cliente

- Error: Al momento de configurar la hora en Debian, al elegir una zona incorrecta, el reloj se desfasaba por 8 horas aproximadamente.
- Solución: Ejecutar en el servidor *date - -set "aaaa-mm-dd hora"* para cambiar la hora en el sistema y *hwclock - -set - -date="aaa-mm-dd* hora para cambiar la hora de la bios.

  Para comprobar la hora ejecutar *hwclock* en el servidor y enviar correos para comprobar que la hora de envío coincida con la hora mostrada.

No acceptable C compiler found in $PATH

- Error: Al momento de cambiar la versión del antivirus, al ejecutar ./ configure para la compilación no reconocía ese comando.
- Solución: Instalar gcc para que pueda compilar.

Al ejecutar *freshclam*: *Freshclam.log is locked by another process*

- Error: *Freshclam* no puede ejecutarse ya que un proceso lo está utilizando.
- Solución: Ejecutar los siguientes comandos:

```
/etc/init.d/clamav-freshclam stop
freshclam -v
/etc/init.d/clamav-freshclam start
freshclam
```

Al ejecutar freshclam: *Detected duplicate databases daily.cvd* and *daily.cld*

- Error: El servidor tiene bases de virus duplicados.
- Solución: Dado que actualiza la base más reciente, no hay problema con eliminar la base duplicada. Al momento de dar *freshclam* se ejecuta la ruta de la base que está actualizando e indica la ruta de la base que es obsoleta, por lo tanto se borra la base duplicada con *rm /ruta_de_la_base/base_duplicada*.

Al levantar los servicios: *clamavis not running*, *freshclam not running*

- Error: Se intenta actualizar la base de virus y se mostraba: *missing daily.cvd.init* y *main.cvd*, lo cual indica que no se encuentran los archivos en la ruta en que se ha instalado la base.

- Solución: Mover los archivos a las carpetas correctas.

  La ruta que se tenía era */.../zimbra/clamav/db/* , se movieron a la ruta */.../zimbra/data/clamav/db/*.

No se puede utilizar cerraduras con tablas logarítmicas.

- Error: Se quiere saber el estado de la base y se ejecuta el comando *zmdbintegrityreport* para ello. MySQL marca lo siguiente: *mysql.general_log* y *mysql.slow_log* ambos antecedidos de "No se puede utilizar cerraduras con tablas logarítmicas".
- Solución: Reparar o Eliminar los archivos
  - Se actualiza la versión anterior a la más reciente con *migrate20100913-Mysql51.pl*
  - Se ejecuta *zmdbintegrityreport*
  - Si el error persiste repararlo con *zmdbintegrityreport -r*
  - Si el error persiste es un error interno de Mysql
    - Se detiene el servidor con *zmcontrol stop*
    - Ir a la carpeta *mysql* y borrar los archivos dañados con *rm*
    - Se levanta el servidor con *zmcontrol start*
  - Se ejecuta *zmdbintegrityreport*

Servidor lento y marcando *java kill process*

- Error: El servidor cuenta con un espacio mínimo para funcionar.

  La primera prueba que se hizo al implementar el servidor de correo electrónico de la DICyG fue en una máquina con las siguientes características:

  - Procesador Intel Pentium 4 de 2.0GHz
  - 256MB de Memoria RAM
  - Unidad de disco duro 80GB
  - Unidad de CD-RW

  Como se mencionó anteriormente en los requerimientos mínimos para la implementación del servidor Zimbra se requiere 1GB de memoria RAM para el correcto funcionamiento del mismo, al contar sólo con 256MB se presentaron diversos errores como:

  1. El servidor no levantaba todos los servicios.
  2. En determinado momento el servidor mataba procesos sin razón aparente.
  3. El servidor no podía permanecer encendido más de un día.
  4. Una vez levantados los servicios, al querer abrir el correo electrónico éste se tardaba varios minutos para hacerlo.
  5. El servidor no respondía o se tardaba un tiempo considerable para enviar un correo electrónico, adjuntar un archivo o crear una tarea.
  6. En ocasiones no enviaba correos.

- Solución: Para no volver a presentar estos errores fue necesario:

  - Aumentar la capacidad de la memoria RAM ya que, el servidor Java de los *mailboxes* hace un uso extensivo de la caché con el fin de mejorar el rendimiento evitando accesos a disco. Por defecto, Zimbra viene configurado para reservar un 40 % de la RAM disponible para este proceso, y un 30 % de la RAM para MySQL
  - Aumentar la capacidad de disco duro.

  Los recursos proporcionados por la División para poder solucionar este inconveniente, fue brindar un disco duro con 160 GB de capacidad y una memoria RAM de 4 GB.

3.2.7. Implementación y adecuación de interfaz gráfica

Una vez levantado el servidor y comprobar que funciona correctamente se procede a adecuarlo para transformarlo en un distintivo institucional de la División.

3.2.7.1. Interfaz Gráfica

Como se ha mencionado en capítulos anteriores, una interfaz gráfica es la que permite al usuario interactuar con el equipo, es a través de ella que el usuario le da instrucciones a la máquina de las acciones que desea que sean realizadas.

Zimbra muestra una interfaz gráfica amigable que permite al usuario localizar y usar sus herramientas de forma eficiente, sencilla y rápida al presentar una interfaz intuitiva, las herramientas básicas están a la vista o cuentan con íconos que son fácilmente relacionados con la acción que brindan, evitando así que su atención se disperse buscando lo que necesita.

En cuanto a la visualización de la página de bienvenida y de la bandeja de entrada, Zimbra ofrece varios temas para poder personalizar la interfaz, cada uno con sus colores y características propios.

Dado que es un servidor institucional se buscó arreglar la interfaz para que tuviera un color que le diera cierta formalidad, además de agregarle imágenes que, al momento de ingresar a la página *web* del cliente, se viera a simple vista que pertenece a la División. Todo este conjunto le brinda al servidor de la DICyG un estilo propio.

Para poder adecuar la interfaz se investigó sobre:

- Permisos para ello.
- Carpetas que contenían las imágenes a modificar.
- El tamaño de las imágenes a modificar.
- El contenido de los archivos que tuvieran que ver con los temas.
- Los archivos que se tenían que modificar y donde editarlos.

Primeramente se hizo la imagen que iría en la pantalla de bienvenida la cual, redirecciona a la página principal de la DICyG, por lo tanto, se buscó que se mostrara: nombre de la institución, nombre de la facultad y nombre de la División a la que pertenece el servidor, además de elegir un color de fondo que no lastimará la vista y que luciera bien junto con las imágenes que iban a ir sobre él.

La pantalla de bienvenida quedó de la siguiente forma:

De encabezado, la facultad a la que pertenece la División:

Figura 3.7: Encabezado de la página de bienvenida

Como imagen principal, la institución y la División a la que pertenece el servidor:

Figura 3.8: Imagen principal de la página de bienvenida

Una vez teniendo la imagen principal, se buscó un color frío ya que éstos le dan más formalidad a las interfaces, se eligió un tono gris y quedó como se muestra a continuación.

Figura 3.9: Interfaz del cliente de correo de la División

Para la bandeja de entrada, se buscaron colores que resaltaran las herramientas y que que a la vez, le dieran una buena vista a la aplicación, quedando el azul para las herramientas y el amarillo pastel para la selección de éstas.

Al tener los colores se modificó la imagen de la bandeja de entrada, cambiándola por el escudo y las iniciales de la División, ésta también redirecciona a la página principal de la DICyG.

Figura 3.10: Escudo e iniciales de la División

Por lo tanto, la bandeja de entrada quedó de la siguiente manera:

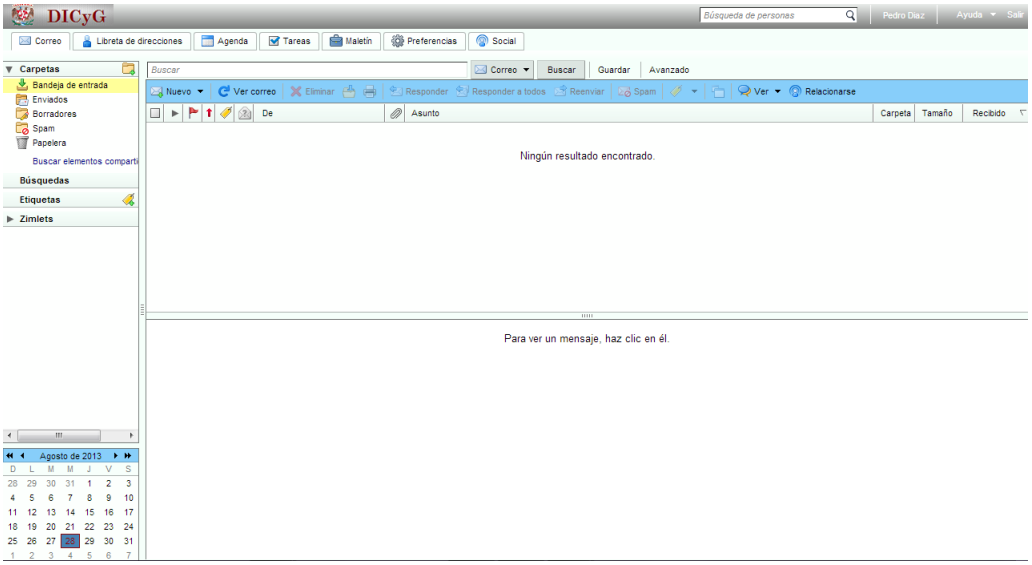


Figura 3.11: Bandeja de entrada de la DICyG

Todos los temas incluidos en Zimbra fueron modificados para que muestren la imagen y el encabezado de la División y la facultad respectivamente así como la imagen de la DICyG en la bandeja de entrada.

La interfaz no es lo único importante para los usuarios (administradores y clientes), la capacidad de almacenamiento y la seguridad de los mensajes son cruciales para una adecuada implementación.

Nota: Dentro de las políticas de Zimbra se menciona que si se está utilizando una versión gratuita no es permitido modificar las imágenes, sin embargo, dado que no se está lucrando con el servidor ni vendiendo nada, se modificó tanto el tema de bienvenida como de la bandeja de entrada, respetando y mostrando en la página de bienvenida los derechos de autor de Zimbra.

3.2.7.2. Implementación de las cuentas

La DICyG utiliza el correo electrónico como el principal medio de comunicación.

El servidor de correo electrónico debe ser capaz de almacenar todos los mensajes que el usuario envíe y reciba al día así que, para evitar que el servidor llegue a un punto de almacenamiento crítico, se tomó la decisión de limitar el espacio total de cada cuenta. Estos límites son los que se denominan cuotas. Éstas fueron establecidas tomando la cantidad de usuarios que están actualmente en la DICyG y la cantidad total de memoria con la que cuenta el servidor.

A continuación se muestran los límites y la cantidad asignados a ellos para cada cuenta:

Límite en	Descripción	Valor
Cuotas de correo electrónico	El espacio máximo de alojamiento de mensajes en la cuenta de correo electrónico	4 GB
Archivos adjuntos	Tamaño máximo de un archivo adjunto	9 MB
Cuerpo del mensaje	Tamaño máximo del cuerpo del mensaje	5 MB
Tamaño del mensaje	Tamaño total máximo de un correo electrónico, el cual incluye: encabezado del mensaje, cuerpo del mensaje y archivos adjuntos	14 MB
Archivos adjuntos dentro de un mensaje	El número máximo de archivos adjuntos permitidos dentro de un correo electrónico (siempre y cuando no sobrepasen los 9 MB)	100 archivos adjuntos
Longitud del asunto	El número máximo de caracteres de texto permitidos en la línea de asunto	255 caracteres

Tabla 3.3: Límites de las cuentas de correo

El usuario debe tener en cuenta los siguientes puntos:

Es su responsabilidad borrar los mensajes enviados y recibidos que no le sean relevantes para tener espacio en su cuenta.

- Si la cuenta se queda sin espacio, el usuario no podrá enviar ni recibir mensajes (todos ellos estarán esperando en la cola del servidor). Cuando la cuenta cuente con espacio los mensajes volverán a llegarle al usuario y podrá enviar mensajes.
- Con la finalidad de informarle al usuario que se está quedando sin espacio y tome las medidas correspondientes como: respaldar y eliminar mensajes, el usuario recibirá un mensaje cuando el tamaño de su cuota llegue al 85 %. En caso de no hacerlo en un tiempo considerable, el administrador, siguiendo las políticas de seguridad de la DICyG, puede bloquear o eliminar su cuenta sin previo aviso.

Capítulo 4

Seguridad en el Correo Electrónico

Las políticas definen un conjunto de requisitos que establecen un límite entre lo que está permitido a los usuarios dentro y fuera de la institución y lo que no está, esto es con el propósito de proteger la información almacenada en los sistemas y el acceso a éstos. Las políticas de seguridad son las reglas y procedimientos que regulan la forma adecuada del uso de recursos de cualquier sistema, previene, protege y maneja los riesgos de diferentes daños que tanto usuarios como administradores tienen. Mientras las políticas indican el "qué", los procedimientos indican el "cómo". Los procedimientos son los que nos permiten llevar a cabo las políticas. Algunos ejemplos que necesitan de un procedimiento son:

- Otorgar una cuenta.
- Dar de alta un usuario.
- Actualización del navegador a utilizar.

Para poder llevar a cabo lo anterior, las políticas deben ser:

Apoyadas por el administrador.

- Únicas.
- Claras (explícitas).
- Concisas (breves).
- Bien estructuradas.
- Escritas.
- Dadas a conocer.
- Entendidas por los usuarios.
- Firmadas por los usuarios.
- Mantenerse actualizas.

Las políticas son parte fundamental de cualquier esquema de seguridad eficiente, debido a que éstas nos permiten acciones adecuadas para el uso del correo electrónico, así como, lo que se puede evitar al utilizar el servicio. Entre las principales características a considerar para establecer las políticas durante su desarrollo, se encuentran:

- Ámbito de aplicación. Indica el alcance de la política, que puede relacionarse con la infraestructura, aplicaciones, información, personas u otro activo de la organización que se desee proteger.

- Enunciados de políticas. Son las declaraciones que deben cumplirse en la División, es decir, todos los enunciados que deben ser acatados por los miembros de la organización.
- Sanciones: Detalla el incumplimiento de la política, considerado como una violación. Además se debe incluir información detallada acerca de las acciones correctivas que se aplicarán como resultado de una falta.
- Sección de uso ético del recurso de correo electrónico.
- Glosario de términos: Aclara cualquier término que sea desconocido para el lector. Políticas de seguridad. La política que se seguirá en la DICyG será prohibitiva: "**Lo que no esté explícitamente permitido queda prohibido**".

4.1. Políticas de seguridad en correo electrónico de la Facultad de Ingeniería

Establece tanto el uso adecuado como inadecuado del servicio de correo electrónico, los derechos y obligaciones que el usuario debe hacer valer y cumplir al respecto. Políticas

- *El usuario es la única persona autorizada para leer su propio correo, a menos que él mismo autorice explícitamente a otra persona para hacerlo, o bien, que su cuenta esté involucrada en un incidente de seguridad de cómputo, donde el administrador del sistema podrá auditar dicha cuenta.*
- *Está estrictamente prohibido usar la cuenta de correo electrónico proporcionada por la organización para propósitos ajenos a sus actividades académicos o laborales según sea el caso.*
- *Está prohibido enviar correos conteniendo injurias, falsedades y malas palabras.*
- *Está prohibido enviar correos sin remitente y sin asuntos.*
- *Está prohibido enviar por correo virus, archivos o información que ponga en peligro la seguridad del sistema.*
- *Está prohibido enviar correos SPAM.*
- *Está prohibido enviar correos de publicidad personal o con intereses personales.*
- *Está prohibido enviar correos haciéndolos pasar por otra persona*
- *Está prohibido reenviar cadenas, chistes y toda clase de información intrascendente, ajena a la actividad académica o laboral del usuario.*

4.2. Políticas de seguridad en correo electrónico específicas en la DICyG

Establece lineamientos del uso adecuado e inadecuado del servicio de correo electrónico, así como los derechos y obligaciones que el usuario debe hacer valer y cumplir al respecto.

- *Para efecto de asignación de cuenta de correo, el usuario deberá solicitar dicha cuenta al responsable del departamento de cómputo de la DICyG, presentando el formato para ello, en el cual se le piden: el nombre, la firma del usuario, motivo por la cual la solicita, entre otros datos.*
- *La cuenta de correo electrónico de la DICyG es personal, intransferible e insustituible por el usuario.*
- *Queda prohibido usar a cuenta de correo electrónico proporcionada por la DICyG para propósitos ajenos a sus actividades académicos o laborales según sea el caso.*

- *Queda prohibido suplantar y falsificar la identidad de otra persona.*
- *Queda prohibido enviar por correo virus, archivos o información que ponga en peligro la seguridad del sistema.*
- *Queda prohibido reenviar "cadenas" y toda clase de información inadecuada a la actividad académica o laboral del usuario.*

Anexos

Es responsabilidad del usuario, el mantener la confidencialidad de la contraseña de su cuenta.

El administrador del departamento de cómputo de la DICyG podrá cancelar de forma temporal o permanente las cuentas de usuario si detecta un uso no adecuado de las mismas.

Si la cuenta llega a su límite de almacenamiento se bloqueará e impedirá el envió y recepción de archivos.

Es deber de todo usuario de correo electrónico de la DICyG, la buena administración del espacio asignado a su cuenta de correo y por lo tanto, es su responsabilidad, cualquier anomalía que se presente, derivada de la mala administración del espacio asignado para su cuenta.

Evitar abrir los correos en los que exista duda de su procedencia, no solicitados o bien un remitente no reconocido.

Es responsabilidad del usuario resguardar su información y datos que considere importantes.

A continuación se presentan las actividades ilícitas así como sus respectivas sanciones:

Actividad ilícita	**Sanciones**	
	Por primera vez	**En caso de reincidencia**
Utilizar una sesión ajena que se encuentre activa	Suspensión por una semana de la cuenta de correo electrónico a quien no es dueño de la misma	Suspensión de su cuenta de correo por un mes
Permitirle a otra persona acceder a su cuenta de correo	Suspensión por un mes de la cuenta de correo del usuario que la brindó	Suspensión a los involucrados de la cuenta de correo por un semestre
Ejecución de programas que intenten obtener información, privilegios, cuentas de correo o ingreso a la cuenta de manera ilícita de forma local o remota	Suspensión de la cuenta de correo por un semestre	Cese definitivo de la cuenta de correo, durante la estancia en la DICyG
Envíos de cualquier tipo de mensajes o propaganda que atenten contra la integridad física o moral de las personas	Suspensión de la cuenta de correo por un año	Cese definitivo de la cuenta de correo, durante la estancia en la DICyG
Envío de cadenas o utilización de la cuenta para redes sociales	Suspensión de la cuenta de correo por un semestre	Cese definitivo de la cuenta de correo, durante la estancia en la DICyG

Tabla 4.1: Actividades y sanciones para el uso indebido del correo de la DICyG

4.3. *Black List*

Listas Negras son listas en donde se registran las direcciones IP que generan *spam*, es decir, mensajes no solicitados, generalmente de tipo publicitario, enviados en grandes cantidades. A estas listas negras se les clasifica de la siguiente manera:

- RBL (*Real Time Blackhole List*), esta lista fue la primera que se uso, contiene una base de datos de direcciones desde donde se genera el *spam*, son altamente efectivas y diariamente bloquean mas allá de 30.000 correos no deseados.

- DNSBL (*DNS Black List*), es un acuerdo entre servidores DNS para bloquear dominios que generan *spam* por medio de su IP, los cuales son almacenados dentro de una base de datos.
- DRBL (*Distributed Realtime Block List*), difiere de DNSBL en el entorno de la distribución, ya que permite a cada red establecer su base de datos.
- DNSWL (*DNS White List*), lista de direcciones que indica quien envía *spam*, puede ser rara vez o inclusive nunca.
- RHSBL (*Right Hand Side Blacklist*), es similar a DNSBL, pero a diferencia de éste tiene en cuenta el nombre de los dominios más no la IP.
- URiBL (*Uniform Resource Identifier Blacklist*), sirve para identificar objetos como las imágenes, que son incluidas en los correos electrónicos, los cuales tratan de esta manera hacer visitar un sitio *web*, enumera los nombres del dominio usados en URLs en vez de direcciones de correo electrónico

4.4. Estimación de vulnerabilidades

El principal factor de la seguridad depende de contar con las medidas necesarias para algún riesgo o amenaza. Si bien es cierto la seguridad total es muy difícil de lograr, puesto que implicaría describir todos los riesgos y amenazas a que puede verse sometido el sistema. Lo que se manifiesta en los sistemas no es la seguridad, sino más bien la inseguridad o vulnerabilidad.

Una vulnerabilidad es un punto del sistema que es susceptible de ser atacado o de dañar la seguridad del mismo, es decir, representan las debilidades o aspectos atacables en el sistema informático. Se trata de una debilidad que puede ser fácilmente explotada para violar la seguridad.

No se puede hablar de un sistema informático totalmente seguro, sino más bien de uno en el que no se conocen tipos de ataques que puedan vulnerarlo, debido a que se han establecido medidas contra ellos.

La estimación de vulnerabilidades del servidor de correo electrónico de la División de Ingenierías Civil y Geomática a la que está expuesto son las siguientes:

- Física: Se refiere al control de acceso físico al sistema. Depende de la posibilidad de acceder físicamente al lugar donde se encuentra el servidor y así poder robarlo, destruirlo o modificarlo. También puede ser el robo de información a través de algún medio físico que almacena datos como puede ser un CD-ROM, USB, por mencionar algunos.
- Natural: Se refiere al grado en que el sistema puede verse afectado por desastres naturales o ambientales por ejemplo: incendios, inundaciones, rayos, terremotos.

  También se refiere al entorno donde se encuentra el sistema: no disponer de reguladores, *no-breaks*, mala instalación eléctrica, fallas eléctricas o picos altos de potencia (en caso de rayos), polvo, humedad, mal sistema de ventilación y calefacción.
- De *Hardware*: Se refiere a no verificar las características técnicas de los dispositivos y sus respectivas especificaciones, además de la falta de mantenimiento del equipo, adquirir un equipo de mala calidad o que no cumpla con las especificaciones adecuadas para llevar a cabo su tarea.
- De *Software*: Incluye todos los errores de programación en el Sistema Operativo u otro tipo de aplicaciones que permitan atacar al SO.
- De red: La conexión de las computadoras a la red incrementa la cantidad de gente que puede tener acceso al mismo o intenta tenerlo, haciendo que el sistema no pueda brindar su mejor rendimiento.
- Humana: Toda la seguridad del sistema recae sobre las personas que usan el sistema debido a que tiene acceso a él y, por tanto, pueden darle mal uso o dañarlo de alguna forma posible.

Entre las vulnerabilidades más comunes del correo electrónico se encuentran:

- De doble extensión: Son archivos maliciosos que tienen doble extensión, de esta forma engañan al usuario para ejecutarlo, ejemplo *archivos.rar.exe*.
- Usurpación del dominio: Permite a los spammers y phishers engañar usuarios para que visiten un sitio *web* malicioso en cambio del legítimo.
- Ejecución de archivos: Permite a los atacantes infectar automáticamente versiones de Internet Explorer/Outlook (Express) que no estén actualizadas al momento de descargar y ejecutar código desde un sitio HTTP.

Un ataque, hablando de equipos de cómputo, es aquel que busca la manera de acceder, controlar o dañar uno o varios equipos o redes.

Entre los ataques más comunes al correo electrónico se encuentran:

- Envío masivo (*spam*): El atacante utiliza al servidor de correo de manera indiscriminada para el envío de grandes cantidades de correo.
- *Malware*: El atacante envía archivos maliciosos que pueden alentar o provocar un comportamiento extraño en el equipo o recopilar información del usuario cómo sus contraseñas u otras cuentas.
- Robo de identidad o *phising*: El atacante solicita al usuario información confidencial por ejemplo, claves de banco, nombre completo, números de su tarjeta de crédito, entre otros, con el fin de meterse a sus cuentas y usarlas a su conveniencia.
- Fuerza bruta. El sistema de ataque, trata de recuperar una clave probando todas las combinaciones posibles hasta encontrar la que se busca, permitiendo así, el acceso a la cuenta.

Capítulo 5

Pruebas en la Implementación del Correo en la DICyG

5.1. Plan de pruebas sobre el correo en la DICyG

Se realizaron diversas pruebas para comprobar que el servidor de correos estaba funcionando correctamente.

Envío y recepción

La principal función del correo electrónico es mantener la comunicación entre los usuarios a través de mensajes, es por ello que, una vez levantado el servidor, se comprobó si realizaba dicha función.

Se crearon dos cuentas sirviendo una como remitente y otra como receptor con el fin de comprobar el envío y recepción de los mensajes.

Primeramente se envío un texto sin formato y a los pocos segundos el correo llegó satisfactoriamente a la cuenta destino.

Posteriormente se adjuntaron archivos y se enviaron a varias cuentas dentro del mismo servidor llegando todas a las cuentas receptoras.

Envío y recepción hacia dominios externos

Una vez comprobado el servicio de manera interna se realizó el envío y recepción de mensajes hacia otros servidores de correo, como por ejemplo: *gmail*, *hotmail*, *yahoo*, *oracle*, *unam.mx*, entre otros, los mensajes de entrada y salida llegaron exitosamente en pocos segundos, sin embargo, se tuvieron algunos inconvenientes con los dominios *oracle* y *unam.mx*.

Cuando se envió el mensaje a *oracle*, llegaba sin problema a su destino, pero al querer responder al servidor salía que el dominio era bloqueado por la lista negra *dnsbl.sorbs.net* que se implementó en el servidor.

Para resolver el problema, se eliminó la lista negra y se pudo recibir correos de *oracle* sin problemas.

En cuanto al dominio *unam.mx*, llego una notificación de Microsoft comunicando que dicho dominio estaba dentro de sus listas negras, por lo tanto, si se deseaba una eliminación del bloque de ésta se debía mandar un correo a una dirección proporcionada por la empresa.

Se obtuvo respuesta al siguiente día así como el retiro del dominio de la lista negra, por lo tanto, se logró recibir y enviar correos de manera satisfactoria a *unam.mx*.

Antivirus

Para comprobar que se tiene un servicio seguro se probo el antivirus y las listas negras.

Se descargo un archivo de prueba de la página *www.eicar.com* y se envió a una cuenta del servidor. El correo no llega a su destino, en su lugar llega un mensaje de alerta notificándole al usuario receptor que una determinada dirección de correo ha intentado mandarle un virus y que el mensaje se ha removido a la cuarentena del servidor.

Una vez hecho esto, se hizo un escaner del equipo con el comando *clamscan -r*, saliendo el siguiente resultado:

```
----------- SCAN SUMMARY -----------
Known viruses: 858610
Engine version: 0.97.8
Scanned directories: 20065
Scanned files: 1265134
Infected files: 1
Data scanned: 180.347,26
MB Data read: 66,560.21 MB (ratio 2.81:1)
Time: 38126.616 sec (635 m 6 s)
```

Se despliega una lista con la información de los archivos escaneados, su estado y si encontró infecciones, como se puede visualizar encontró el falso virus, por lo tanto, se ejecuta el siguiente comando para que todos los archivos que haya detectado como maliciosos los mueva a una carpeta determinada.

```
clamscan --log=/opt/zimbra/log/clamd.log --move=cuarentena -r /
```

Posteriormente se elimina dicha carpeta con el comando *rm -r /nombre_carpeta*.

Adjuntos

Se hicieron pruebas para corroborar que el servidor estaba adjuntando archivos de manera satisfactoria.

El tamaño máximo de un archivo adjunto en el correo de Zimbra por defecto es de 10Mb, pero al querer adjuntar un archivo de este tamaño el servidor indica que el tamaño del archivo es superior al permitido:

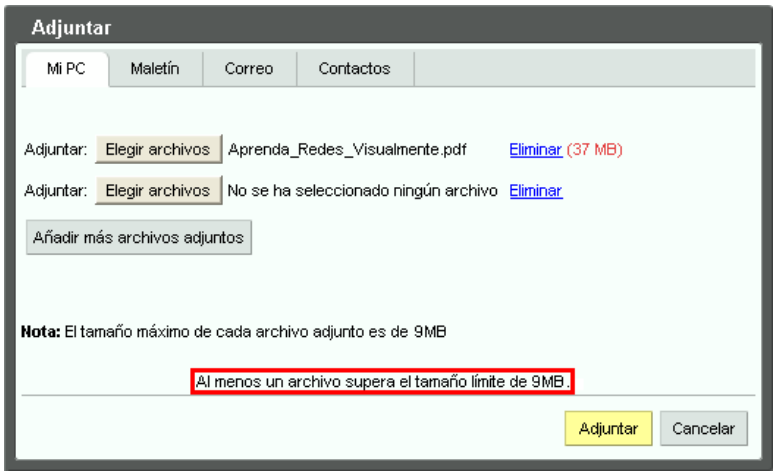


Figura 5.1: Tamaño de los archivos adjuntos

Esto es debido a que Zimbra de manera interna codifica los datos en un formato llamado *base64-encoding* por lo que dicha codificación hará que un adjunto ocupe un poco más (alrededor de 4Mb) de su peso real.

Por lo tanto, el tamaño máximo de los adjuntos debe ser no mayor a 5 Mb.

Informe *Daily Mail*

Un reporte diario acerca del uso y el flujo de correo electrónico de la DICyG permite llevar un mejor control sobre el servidor. El reporte diario no representa un trabajo adicional y es parte de las funciones y responsabilidades que se debe de llevar a cabo, para poder actuar si llegase a presentar cualquier anomalía.

Por tal motivo se verificó que el correo electrónico de la DICyG enviara un reporte diariamente al buzón del administrador.

El informe diario electrónico incluye la siguiente información:

- Número total de mensajes enviados y recibidos.
- El tiempo de espera en segundos para la entrega de mensajes.
- Errores internos que se han generado por Zimbra Postfix.
- Cuentas remitentes más activos y el número de mensajes.
- Cuentas receptoras más activos y el número de mensajes.
- Número total de envíos rechazados.

5.2. Medición de desempeño

Para verificar el buen funcionamiento del servidor implementado en la DICyG es necesario aplicar pruebas de rendimiento para determinar el tiempo que tarda en realizar una tarea en condiciones particulares de trabajo. Además dichas pruebas permiten verificar otros atributos de la calidad del servidor, tales como la escalabilidad, fiabilidad y uso de los recursos. Para ello se descargó algunas herramientas que permiten conocer el desempeño del servidor.

Entre las herramientas elegidas se encuentran:

- *Uptime* (Tiempo de actividad): Muestra la calidad o estabilidad del sistema así como el tiempo que ha permanecito encendido sin ser reiniciado, la hora actual, el número de usuarios conectados en el momento y el promedio de carga durante el intervalo de 1, 5 y 15 minutos.

  Los datos relevantes de este análisis son los últimos 3 ya que reflejan la carga del sistema en un lapso de tiempo, mientras más bajo sea el valor de la carga mejor es el rendimiento del equipo. La carga son procesos que se están ejecutando actualmente en el CPU o que están en espera de hacerlo (cola). A la suma de estos dos se le llama *recorrido-cola*.

  La carga se encuentra entre los siguientes rangos:

  - Menos de 1.00 (ideal, mantenerlo bajo de 0.70): Significa que no hay carga, el procesamiento del equipo es óptimo. Se puede tener unos picos (más de uno) pero no debe ser algo constante.
  - 1.00-1.50 Significa que la carga es exactamente lo que puede soportar el sistema, el procesamiento del equipo es bueno, pero si llegará más carga, el sistema empezará a alentarse.
  - Más de 1.50: Significa que la carga es más de lo que el sistema puede soportar, el sistema trabajará lento ya que los procesos están a la espera, el procesamiento del equipo no es óptimo.

  El promedio que se debe tener en mayor consideración es el de 5, si se sobre pasa el 1.00 de carga durante este lapso es recomendable hacer una corrección al sistema.

- *Saidar*: Muestra las estadística del sistema:

  - El nombre del servidor, así como el tiempo que ha estado en ejecución y la fecha actual.
  - La carga del CPU en 1,5 y 15 minutos, su uso, el estado de los procesos que están corriendo en ese momento, el número total de procesos y el número de usuarios que están utilizando el equipo.
  - El espacio total, usado y libre, de la memoria física y el área de intercambio

- El uso de los procesos de I / O.

- *Htop*: Muestra en tiempo real el estado de los procesos del sistema. Sus campos se actualizan cada cinco segundos.

  Esta herramienta se divide en tres secciones. La superior-izquierda muestra un resumen del uso del CPU y el área de intercambio, así como breves estadísticas del sistema y sus procesos, mientras que la parte superior-derecha muestra las tareas, el tiempo de carga y la fecha. La parte media muestra un listado de procesos que se encuentran en ejecución dentro del sistema. La parte inferior muestra un menu con opciones para ejecutar dentro de la herramienta, como pedir ayuda, realizar búsquedas, enviar señales a los procesos, entre otros.

  La información que muestra *htop* es:

  - 1 y 2: Representan el número de núcleos en el sistema. Las barras de colores junto a estos números representan la carga sobre los núcleos. (azul: procesos de baja prioridad, verde: procesos usados por el usuario, rojo: tiempo de *kernel*, naranja: tiempo de *virt*)
  - *mem* (memoria física): Muestra el uso de la memoria física: total, usada, libre y en caché.
  - sw*a*p (área de intercambio): Muestra el uso del área de intercambio: total, usada, libre y en caché.
  - *tasks* (tareas): Muestra el número total de procesos y tareas que se están ejecutando así como los procesos que se encuentran dormidos (*sleeping*), detenidos (*stopped*) o muertos (*zombies*).
  - *uptime* (tiempo de actividad)
  - *Load average* (carga)
  - *processes list* (lista de procesos): Muestra los procesos que se encuentran actualmente en uso:
    - *PID*: Muestra el número de identificación del proceso
    - *USER*: Muestra al propietario del proceso
    - *PRI*: Muestra la prioridad del proceso
    - *NI*: Muestra el valor ideal de un proceso
    - *VIRT*: Muestra la memoria virtual utilizada por el proceso
    - *RES*: Muestra la memoria física utilizada en el proceso
    - *SHR*: Muestra la memoria compartida que utiliza el proceso
    - *S*: Muestra el estado del proceso (R correr, S sueño, Z zombie)
    - *CPU %*: Muestra el porcentaje de CPU utilizado por el proceso
    - *MEM %*: Muestra el porcentaje de memoria RAM utilizada por el proceso
    - *TIME+*: Muestra el tiempo total de la actividad del proceso
    - *COMMAND*: Muestra el nombre del proceso

- *Atop*: Muestra la actividad de todos los procesos en intervalos regulares (por defecto: 10 segundos) a través de un monitor interactivo para ver la carga del equipo a nivel sistema.

  Esta herramienta se divide en dos partes: la parte superior muestra información sobre los recursos (CPU, memoria, discos y capas de red) y la parte inferios muestra la lista de procesos.

  Tabla de procesos:

  - *PID*: Muestra el identificador del proceso.
  - *SYSCPU*: Muestra el consumo de tiempo que ha hecho el proceso al CPU en modo sistema.
  - *USRCPU*: Muestra el consumo de tiempo del proceso en modo usuario.
  - *VGROW*: Muestra la cantidad de memoria virtual que el proceso ha utilizado.
  - *RGROW*: Muestra la cantidad de memoria física que el proceso ha utilizado.
  - *RDDSK*: Muestra la transferencia de datos de lectura emitidos físicamente en el disco.
  - *WRDSK*: Muestra la transferencia de datos de escritura emitidos físicamente en el disco.

- *ST*: Muestra el estado del proceso, la primera posición indica si el proceso se ha iniciado durante el último intervalo (*N* nuevo proceso) y la segunda posición. Muestra si el proceso ha terminado durante el último intervalo (*E* salida, *S* y *C* el proceso ha terminado involuntariamente por una señal), si la segunda posición no se ha terminado correctamente el número de señal aparecerá en la columna de *EXC*.
- *S*: Muestra el estado actual de un subproceso: *R* corriendo (*run*), *S* dormir esperando que ocurra algún evento (*sleeping*), *D* dormir sin interrupciones, *Z* en espera de sincronización con el proceso padre (*zombie*), *T* detenido (*stopped*), *W* intercambio (*swapping*) y *E* terminado (*exit*).
- *CPU*: Muestra el porcentaje que el proceso está utilizando del sistema.
- *CMD*: Muestra el nombre del proceso que se está ejecutando.

- *Ntop*: Muestra el uso de la red actual ofreciendo una interfaz gráfica donde el administrador del servidor puede visualizar el tráfico enviado y recibido por cada host, los protocolos más utilizados por el servidor, el tamaño de los paquetes, por mencionar algunos.

5.3. Análisis de Resultados

El análisis del equipo permite una evaluación del sistema local para verificar si todo funciona correctamente y, en caso de detectar algún problema, corregirlo rápidamente.

Los aspectos que se deben tener en cuenta para un análisis completo son:

1. Procesamiento. Indica el número de instrucciones que se están realizando en el microprocesador al momento de ejecutar un programa.

   Los estados de un proceso son:

   a) En ejecución (*running*). El proceso está utilizando el procesador.

   b) Bloqueados (*waiting*). El proceso no puede ejecutarse hasta que otro concluya.

   c) Listo (*ready*). El proceso ha liberado al procesador para que pueda ser usado por otro proceso.

   Si un gran número de procesos están ejecutándose o en espera de ejecución, el rendimiento del equipo será de menor calidad.

2. Memoria. Componente indispensable de la computadora la cual mantiene la disponibilidad de los datos y programas que utiliza el microprocesador, además de almacenar temporalmente la información de los procesos que se han ejecutado así como almacenar y recuperar información. En los dispositivos de memoria se realizan dos tipos de acciones: obtener información que se encuentra almacenada (lectura) y modificar o almacenar nueva información (escritura).

   La memoria puede ser volátil (mantiene información únicamente si está alimentada constantemente por una fuente eléctrica) o no volátil (mantiene la información indefinidamente).

   Entre las memorias que son analizadas por las herramientas se encuentran:

   a) Principal (central, primaria, interna o real): Almacena temporalmente los datos y programas que están siendo procesados por el equipo.

   b) Virtual (MV o *swap*): Permite al Sistema Operativo disponer de mayor cantidad de memoria de la que está físicamente disponible.

3. *I/O* (*Input/Output*, en español E/S Entrada/Salida). Permite la comunicación entre el usuario y el equipo de procesamiento a través de los datos que el usuario ingresa al equipo y, a su vez, éste los convierte en información entendible para el usuario.

   Los datos que las herramientas de análisis examinan son:

   a) Almacenamiento. Velocidad en la transferencia de datos entre ambas partes.

   b) Red. Flujo y velocidad de datos transferidos del equipo a Internet.

Los resultados obtenidos con las herramientas del tema anterior fueron:

- *Uptime*

  Se obtuvieron los siguientes resultados:

  La primera columna representa el tiempo en que el servidor ha estado encendido, la hora actual, los usuarios conectados al servidor y la carga en 1, 5 y 15 minutos.

Figura 5.2: Uptime

  La carga media tanto en los tres intervalos de tiempo es menor a 1.00, el sistema está utilizando el 0.0001 % de su capacidad. El rendimiento del equipo es óptimo.

- *Saidar*

  Se obtuvieron los siguientes resultados:

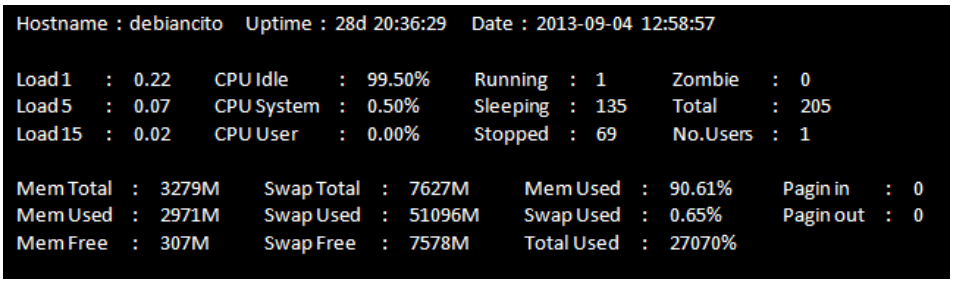


Figura 5.3: Saidar

  La carga en el sistema se mantiene bajo 1 en los tres tiempos, el uso del CPU por parte del sistema y de los usuarios es casi nulo, no se presentan procesos en estado zombie, tanto la memoria física como el área de intercambio cuentan con espacio libre, no hay procesos de E/S. El sistema funciona correctamente.

- *Htop*

  Se obtuvieron los siguientes resultados:

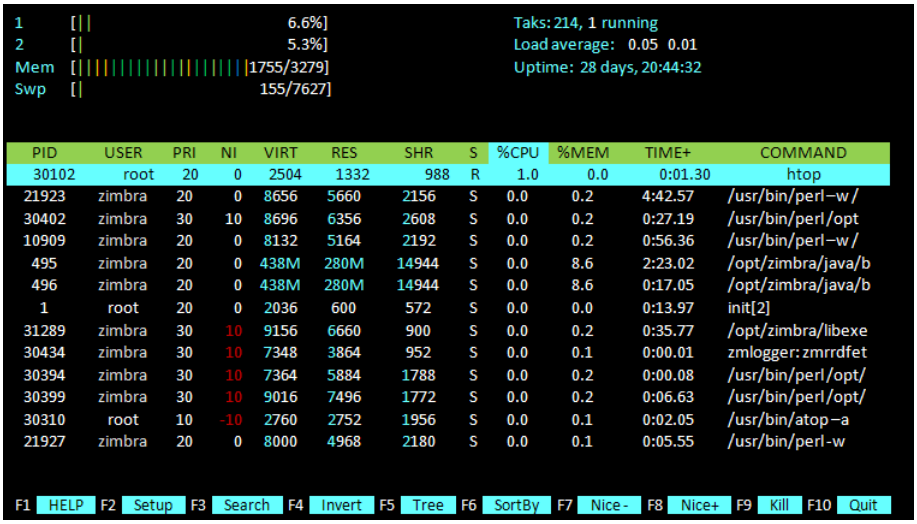
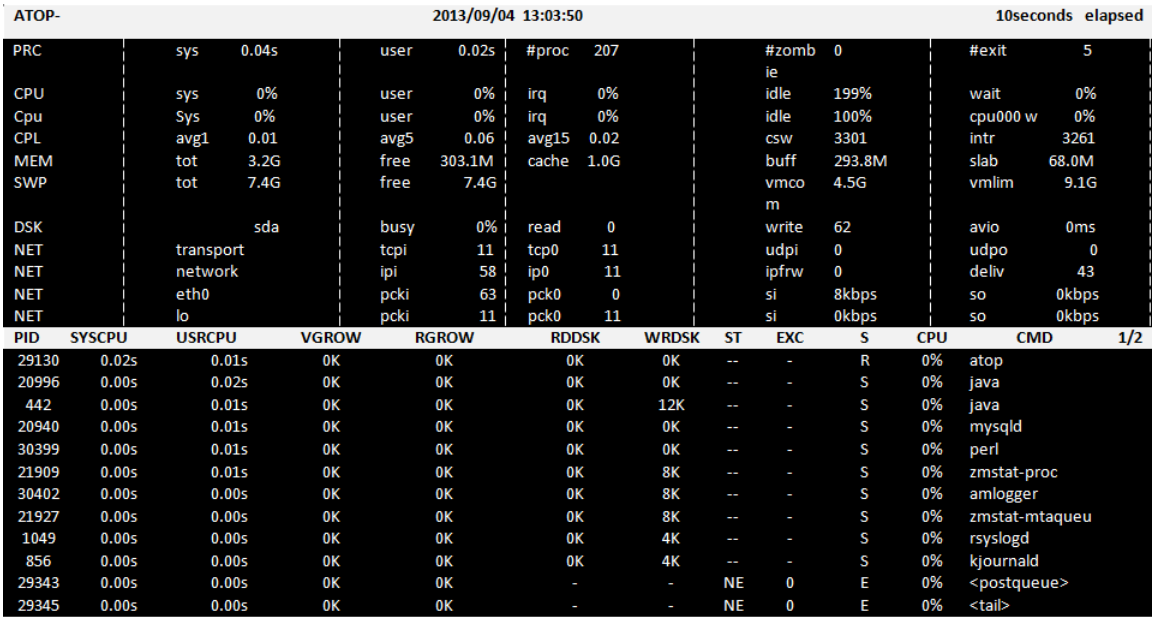


Figura 5.4: Top

Se comprueba que el uso del disco duro y la memoria RAM es mínimo, el CPU cuenta con suficiente espacio libre, no hay procesos en espera y el tiempo de ejecución de los procesos es rápido. El sistema trabaja de forma óptima.

- *Atop*

  Se obtuvieron los siguientes resultados:



ATOP-											2013/09/04 13:03:50										10seconds elapsed
PRC		sys	0.04s		user	0.02s	#proc	207			#zombie	0			#exit	5				
CPU		sys	0%		user	0%	irq	0%			idle	199%			wait	0%				
Cpu		Sys	0%		user	0%	irq	0%			idle	100%			cpu000 w	0%				
CPL		avg1	0.01		avg5	0.06	avg15	0.02			csw	3301			intr	3261				
MEM		tot	3.2G		free	303.1M	cache	1.0G			buff	293.8M			slab	68.0M				
SWP		tot	7.4G		free	7.4G					vmcom	4.5G			vmlim	9.1G				
DSK			sda		busy	0%	read	0			write	62			avio	0ms				
NET		transport			tcpi	11	tcp0	11			udpi	0			udpo	0				
NET		network			ipi	58	ip0	11			ipfrw	0			deliv	43				
NET		eth0			pcki	63	pck0	0			si	8kbps			so	0kbps				
NET		lo			pcki	11	pck0	11			si	0kbps			so	0kbps				
PID	SYSCPU		USRCPU	VGROW		RGROW		RDDSK		WRDSK	ST	EXC	S	CPU	CMD						1/2
29130	0.02s		0.01s	0K		0K		0K		0K	--	-	R	0%	atop						
20996	0.00s		0.02s	0K		0K		0K		0K	--	-	S	0%	java						
442	0.00s		0.01s	0K		0K		0K		12K	--	-	S	0%	java						
20940	0.00s		0.01s	0K		0K		0K		0K	--	-	S	0%	mysqld						
30399	0.00s		0.01s	0K		0K		0K		0K	--	-	S	0%	perl						
21909	0.00s		0.01s	0K		0K		0K		8K	--	-	S	0%	zmstat-proc						
30402	0.00s		0.00s	0K		0K		0K		8K	--	-	S	0%	amlogger						
21927	0.00s		0.00s	0K		0K		0K		8K	--	-	S	0%	zmstat-mtaqueu						
1049	0.00s		0.00s	0K		0K		0K		4K	--	-	S	0%	rsyslogd						
856	0.00s		0.00s	0K		0K		0K		4K	--	-	S	0%	kjournald						
29343	0.00s		0.00s	0K		0K		-		-	NE	0	E	0%	<postqueue>						
29345	0.00s		0.00s	0K		0K		-		-	NE	0	E	0%	<tail>						

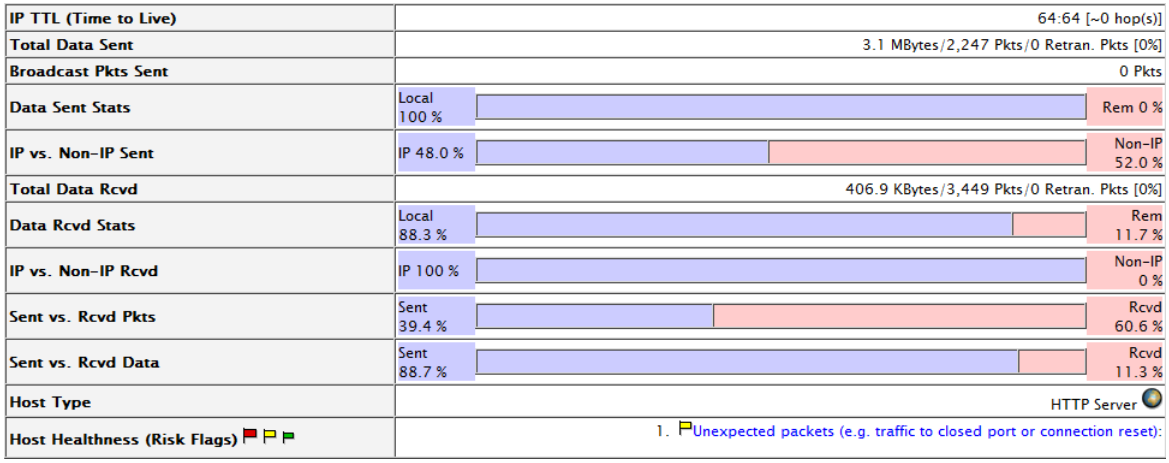
Figura 5.5: Atop

El tiempo total consumido en modo sistema, de usuario, el total de procesos presentados en el momento, el porcentaje de tiempo de CPU gastado en el modo kernel por todos los procesos activos del sistema y porcentaje de tiempo de CPU consumido en modo de usuarios, indican que no hay saturación. El sistema funciona correctamente.

- *Ntop*

  Se obtuvieron los siguientes resultados:

  - Datos generales del funcionamiento del servidor fueron:



IP TTL (Time to Live)	64:64 [~0 hop(s)]
Total Data Sent	3.1 MBytes/2,247 Pkts/0 Retran. Pkts [0%]
Broadcast Pkts Sent	0 Pkts
Data Sent Stats	Local 100 % — Rem 0 %
IP vs. Non-IP Sent	IP 48.0 % — Non-IP 52.0 %
Total Data Rcvd	406.9 KBytes/3,449 Pkts/0 Retran. Pkts [0%]
Data Rcvd Stats	Local 88.3 % — Rem 11.7 %
IP vs. Non-IP Rcvd	IP 100 % — Non-IP 0 %
Sent vs. Rcvd Pkts	Sent 39.4 % — Rcvd 60.6 %
Sent vs. Rcvd Data	Sent 88.7 % — Rcvd 11.3 %
Host Type	HTTP Server
Host Healthness (Risk Flags)	1. Unexpected packets (e.g. traffic to closed port or connection reset):

Figura 5.6: Ntop - Datos generales

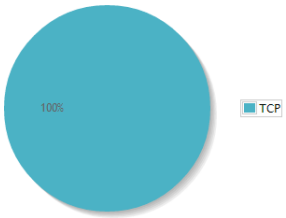
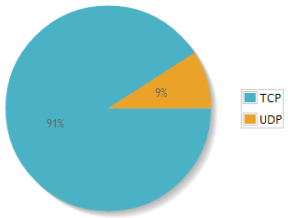
- Sesiones activas:

Proto	Client	Server	Data Sent/Rcvd		Active Since	Duration	Inactive	Client/Server Nw Delay		L7 Proto
UDP	192.xx.xx.xx :domain	dns2.xx.xx :domain	2.1 KBytes	9.8 KBytes	Wed Sep 25 15:19:14 2013	2:01	12 sec			DNS
TCP	192.xx.xx.xx :50226	192.xx.xx.xx :3000	811	13.4 KBytes	Wed Sep 25 15:20:52 2013	0 sec	35 sec	0.48 ms	0.01 ms	HTTP
TCP	192.xx.xx.xx :50227	192.xx.xx.xx :3000	618	215	Wed Sep 25 15:20:52 2013	0 sec	35 sec	1.09 ms	0.01 ms	HTTP
TCP	192.xx.xx.xx :50228	192.xx.xx.xx :3000	604	215	Wed Sep 25 15:20:52 2013	0 sec	35 sec	0.51 ms	0.00 ms	HTTP
TCP	192.xx.xx.xx :50229	192.xx.xx.xx :3000	608	215	Wed Sep 25 15:20:52 2013	0 sec	35 sec	0.50 ms	0.00 ms	HTTP
TCP	192.xx.xx.xx :50230	192.xx.xx.xx :3000	626	215	Wed Sep 25 15:20:52 2013	0 sec	35 sec	0.50 ms	0.00 ms	HTTP
TCP	192.xx.xx.xx :50231	192.xx.xx.xx :3000	639	215	Wed Sep 25 15:20:52 2013	0 sec	35 sec	0.51 ms	0.00 ms	HTTP
TCP	192.xx.xx.xx :50232	192.xx.xx.xx :3000	639	215	Wed Sep 25 15:20:52 2013	0 sec	35 sec	0.38 ms	0.00 ms	HTTP
TCP	192.xx.xx.xx :50235	192.xx.xx.xx :3000	646	215	Wed Sep 25 15:20:52 2013	1 sec	34 sec	0.45 ms	0.01 ms	HTTP
TCP	192.xx.xx.xx :50236	192.xx.xx.xx :3000	648	215	Wed Sep 25 15:20:52 2013	1 sec	34 sec	0.62 ms	0.00 ms	HTTP
TCP	192.xx.xx.xx :50237	192.xx.xx.xx :3000	639	215	Wed Sep 25 15:20:52 2013	1 sec	34 sec	0.51 ms	0.00 ms	HTTP
TCP	192.xx.xx.xx :50238	192.xx.xx.xx :3000	638	215	Wed Sep 25 15:20:52 2013	1 sec	34 sec	0.51 ms	0.00 ms	HTTP
TCP	192.xx.xx.xx :50239	192.xx.xx.xx :3000	624	215	Wed Sep 25 15:20:53 2013	0 sec	34 sec	0.47 ms	0.01 ms	HTTP
TCP	192.xx.xx.xx :50240	192.xx.xx.xx :3000	692	5.5 KBytes	Wed Sep 25 15:20:53 2013	0 sec	34 sec	0.81 ms	0.01 ms	HTTP
TCP	192.xx.xx.xx :50241	192.xx.xx.xx :3000	611	215	Wed Sep 25 15:20:53 2013	0 sec	34 sec	0.48 ms	0.01 ms	HTTP
TCP	192.xx.xx.xx :50242	192.xx.xx.xx :3000	608	215	Wed Sep 25 15:20:53 2013	0 sec	34 sec	0.49 ms	0.01 ms	HTTP
TCP	192.xx.xx.xx :50243	192.xx.xx.xx :3000	607	215	Wed Sep 25 15:20:53 2013	0 sec	34 sec	2.66 ms	0.01 ms	HTTP

Figura 5.7: Ntop - Sesiones activas en el servidor

El servidor, cumple con el envío y recepción de información, no hay inconvenientes entre la comunicación del cliente y el servidor.

- Protocolos:

Protocol	Data Sent	Data Rcvd
TCP	1.9 MBytes	595.5 KBytes
UDP	16.5 KBytes	63.9 KBytes
(R)ARP	0.0 KBytes	0.8 KBytes
Protocol Distribution		

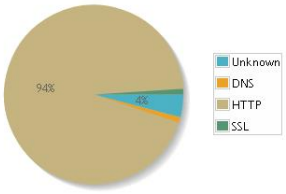
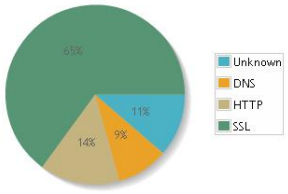
L7 Protocol	Data Sent	Data Rcvd
Unknown	49.6 KBytes	89.6 KBytes
DNS	18.1 KBytes	76.0 KBytes
HTTP	1.1 MBytes	113.9 KBytes
SSL	22.2 KBytes	480.6 KBytes
IP Distribution		

Figura 5.8: Ntop - Protocolos

- Paquetes:

TCP Connections	Directed to		Rcvd From	
Attempted	125	dns1.xx.xx jake.xx.xx dns2.xx.xx dns2.xx.xx dns1.xx.xx	1,210	192.xx.xx.xx 192.xx.xx.xx 192.xx.xx.xx dns2.xx.xx dns1.xx.xx 192.xx.xx.xx 192.xx.xx.xx 192.xx.xx.xx
Established	124 [99 %]	dns1.xx.xx jake.xx.xx dns2.xx.xx dns2.xx.xx dns1.xx.xx	665 [55 %]	192.xx.xx.xx 192.xx.xx.xx 192.xx.xx.xx dns2.xx.xx dns1.xx.xx 192.xx.xx.xx 192.xx.xx.xx 192.xx.xx.xx
Terminated	0		5	192.xx.xx.xx 192.xx.xx.xx 192.xx.xx.xx
SYN	125	dns1.xx.xx jake.xx.xx dns2.xx.xx dns2.xx.xx dns1.xx.xx	1,210	192.xx.xx.xx 192.xx.xx.xx 192.xx.xx.xx dns2.xx.xx dns1.xx.xx 192.xx.xx.xx 192.xx.xx.xx 192.xx.xx.xx
RST|ACK	0		6	192.168.xx.xx 192.168.xx.xx 192.168.xx.xx
SYN	128	dns1.xx.xx jake.xx.xx dns2.xx.xx dns2.xx.xx dns1.xx.xx	1,210	192.xx.xx.xx 192.xx.xx.xx 192.xx.xx.xx dns2.xx.xx dns1.xx.xx 192.xx.xx.xx 192.xx.xx.xx 192.xx.xx.xx
RST|ACK	0		8	192.168.xx.xx 192.168.xx.xx 192.168.xx.xx
NULL	126	dns1.xx.xx dns2.xx.xx dns2.xx.xx dns1.xx.xx	126	dns1.xx.xx dns2.xx.xx dns2.xx.xx dns1.xx.xx
Closed Empty TCP Conn.	0		5	192.168.xx.xx 192.168.xx.xx 192.168.xx.xx

Figura 5.9: Ntop - Estadísticas de los paquetes

Se llevo a cabo una buena comunicación entre el cliente y el servidor.

- Datos enviados y recibidos:

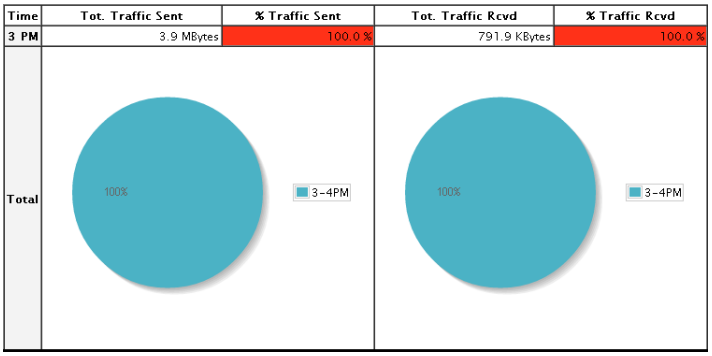


Figura 5.10: Ntop - Datos enviados y recibidos en una hora

Todos los datos se enviaron y se recibieron correctamente.

El conjunto de todas estas herramientas indican que el sistema funciona correctamente, sin sobrecargas ni exceso en el tráfico de red, el espacio de memoria es óptimo por lo que se asegura que el sistema no colapsará debido a una cantidad considerable de mensajes.

5.4. Programa de mantenimiento

Los servidores a diferencia de los equipos terminales, trabajan todo el tiempo y prácticamente no tienen descanso. Es por esta razón, que cada cierto tiempo es necesario realizar mantenimiento preventivo para que el funcionamiento del servidor continúe siendo óptimo y evitar errores o situaciones que puedan reducir el funcionamiento de la red y, con ello, del servicio. Por ello se menciona el programa de mantenimiento que se debe de llevar a cabo tanto por parte del administrador como del cliente.

Preparando el servidor para el mantenimiento:

Hardware

Este paso es simple, pero muy importante, ya que mientras el equipo esté limpio por dentro la temperatura se elevará menos y los sistemas de enfriamiento trabajarán con menos esfuerzo.

Por lo menos cada dos meses realizar lo siguiente:

- Apagar el equipo.
- Desconectarlo de los sistemas de conexiones hacia el resto de los equipos de la red.
- Una vez que el servidor se encuentre libre de conexiones, retirarlo del rack en donde se encuentra alojado físicamente y colocarlo sobre una superficie plana, segura y completamente aislante.
- Se comienza con la limpieza del servidor retirando el polvo tanto de manera interna como externa. De forma externa es recomendable realizar la limpieza con un trapo húmedo y limpio, de manera interna utilizar aire comprimido.
- Nota: Antes de tocar el equipo, tocar una superficie metálica para descargar la posible electricidad estática que el cuerpo llegue a tener y usar una pulsera antiestática.
- Cerrar el equipo y conectarlo a un regulador de voltaje para evitar que le llegue una sobrecarga y se averíe.
- Encenderlo.

Software

Cuentas de correo

Es muy importante el mantenimiento de las cuentas de correo, si los mensajes pasados no son eliminados del equipo, la memoria empezará a llenarse ocasionando que el servidor trabaje de manera lenta y llegue el punto en que no se puedan recibir correos.

Para evitar esta situación, el servidor le mandará un mensaje automáticamente al usuario cuando su capacidad de almacenamiento esté en un 75 % de uso, de esta forma, se hará consciente al usuario para que tome las medidas necesarias para seguir haciendo uso de su cuenta.

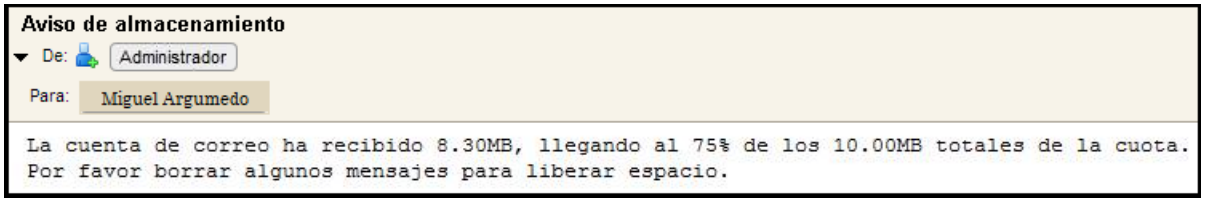


Figura 5.11: El espacio llego al 75 %

En caso de que ignore el mensaje de advertencia la cuenta recibirá la sanción estipulada en las reglas del correo de la DICyG.

Espacio de almacenamiento

El administrador debe estar al pendiente de que el servidor cuente con el espacio suficiente para brindar el servicio, por lo tanto, debe conocer el espacio que las cuentas tienen ocupado.

Para visualizar ésto de forma sencilla, debe ingresar a la interfaz del administrador y revisar el *Espacio de almacenamiento del buzón de correo*, posteriormente identificar las que estén en un 75 %. Estas cuentas serán localizadas fácilmente ya que en la opción *Espacio de almacenamiento utilizando* se muestra el porcentaje y una barra en color verde del espacio que la cuenta ha consumido. Cuando la cuente llegue al 75 % la barra cambiará a color rojo:

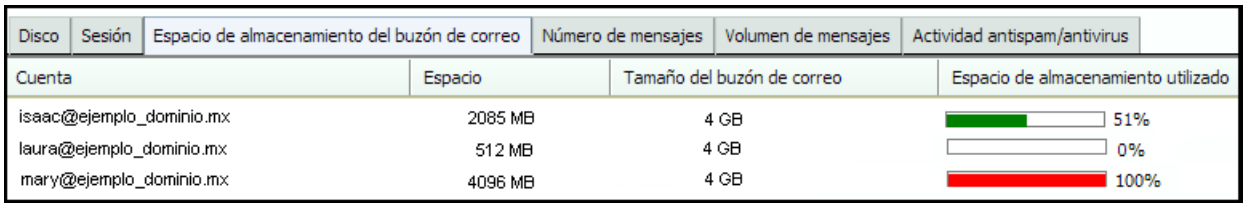


Figura 5.12: Espacio de almacenamiento

Colas de correo

Si los mensajes no están llegando a su destino puede ser problema de la cuenta y no del servidor, si la cuenta ha llegado al límite de su espacio o el mensaje es demasiado pesado para el espacio que le queda, los mensajes se quedarán en la cola del servidor hasta que la cuenta en cuestión elimine mensajes.

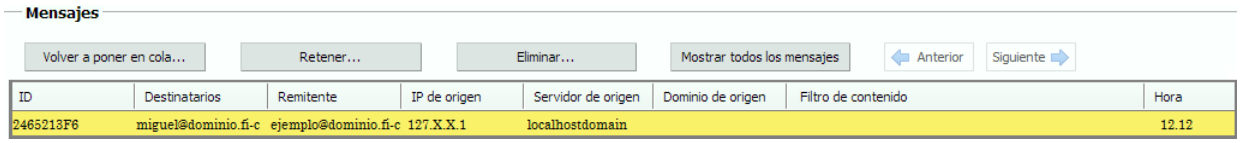


Figura 5.13: Colas de correo

Si el usuario ha hecho caso omiso del mensaje de advertencia, el administrador borrará los mensajes que se localicen en cola para evitar uso de recursos del servidor y saturación de la red

Lista de usuarios

Es importante tener una lista completa de todos los usuarios registrados en el servidor para llevar un control físico de todas las cuentas.

Para ello se realiza lo siguiente mediante línea de comandos:

- Ingresar el comando *zmprov -l gaa -v nombre_del_servidor* para obtener la lista de los usuarios así como de la configuración de la cuenta. Puede elegirse la ruta así como la extensión del archivo con el comando *>>/tmp/nombre_de_la_lista.extensión*.

  Donde:

  - *zmprov*: Realiza todas las tareas de aprovisionamiento de zimbra LDAP.
    - *gaa*: Lista todas las cuentas del servidor.
    - *-l*: Lista en pantalla las cuentas del servidor.
    - *-v*: Lista todas las cuentas y configuraciones del servidor.
  - Mandar el archivo al correo del administrador para posteriormente imprimirlo.

  De esta forma se tendrá un control de los usuarios que actualmente están dados de alta en el servidor.

Papelera

Para evitar que los mensajes eliminados ocupen espacio en el servidor, se recomienda vaciar la papelera. Puede darse el caso que los usuarios no estén conscientes de esta acción, por lo tanto, el servidor borrará automáticamente el contenido de la papelera después de 30 días.

Respaldo de información

Para evitar la pérdida total de la información de las cuentas, se recomienda tener un servidor de respaldo en el cual se crearán las cuentas existentes y se exportará la información de los usuarios.

Realizar lo siguiente mendiante línea de comandos:

- Para exportar la cuenta se ingresar el comando */.../.../bin/zmmailbox -z -m cuenta_origen@test.org getRestURL* y para darle el formato de salida ingresar *"//?fmt (formato inicial)=tgz* (formato de salida)". Puede elegirse la ruta (dentro de zimbra) así como la extensión del archivo con el comando *> /ruta/nombre_archivo.tgz* (se recomienda *.tgz* ya que *.zip* no cuenta con metadatos).
- Para importar la cuenta se ingresa el comando */.../.../bin/zmmailbox -z -m cuenta_destino@test.org postRestURL* para obtener el formato inicial se ingresa *"//?fmt=tgz&resolve=reset" /ruta/nombre_archivo.tgz.*

  Donde:

  - *-z*: Utilizar nombre y contraseña del administrador zimbra.
  - *-m*: Abrir buzón de la cuenta.
  - *resolve*: Resuelve conflictos en la importación, puede tener los siguientes parámetros:
  - *skip*: Ignora los conflictos.
  - *modify*: Cambia los archivos antiguos.
  - *replace*: Elimina los archivos antiguos y crea unos nuevos.
  - *reset*: Elimina todo lo que tiene la cuenta antes de importar la información.

  De esta manera, la información de la *cuenta_origen* quedará guardada en *cuenta_destino*, así, si al servidor le llega a ocurrir algo, la información estará a salvo.

También se puede hacer el respaldo de las cuentas mandando la información a una carpeta y posteriormente guardarla en una usb.

Cuando el servidor esté nuevamente en funcionamiento importar las dos datos a sus respectivas cuentas.

Lo antes mencionado se trata de tareas de control y mantenimiento preventivo que se deben realizar periódicamente para mantener la mayor disponibilidad y rendimiento del servidor adelantándose a los problemas y previniendo los posibles fallos futuros.

5.4.1. Manual de operaciones

Para el correcto uso de la aplicación se realizaron manuales tanto para el administrador como para el usuario, en los cuales se explica el funcionamiento de las herramientas y como realizar ciertas tareas, como por ejemplo, la creación de cuentas, enviar mensajes, entre otros.

De esta forma, se pretende agilizar el uso del servicio y brindarle a los usuarios la información necesaria para que utilicen las herramientas de forma efectiva.

Estos manuales se encuentran en los anexos *A* y *B*, el primero para el cliente y el segundo para el administrador del correo.

También en el anexo *C*, se encuentra el formato de solicitud de la cuenta así como las políticas de seguridad del servidor.

Capítulo 6

Conclusiones y Trabajos a Futuro

El correo electrónico tiene gran importancia en la actualidad destacando en los ámbitos laboral, académico y personal, toda persona que cuenta con Internet tiene, al menos, una cuenta de correo para mandar y recibir mensajes, poder recibir información de los foros, noticias o inscribirse a ciertos grupos, redes sociales y foros.

Es una herramienta que permite estar comunicado con personas de cualquier parte del mundo, el envío y recepción de un mensaje es inmediato logrando una rápida comunicación, además de ser fácil de utilizar y se puede acceder a través de cualquier equipo con conexión a Internet, sin duda, el correo electrónico es un servicio económico comparándolo con otros servicios de comunicación.

La información que se envía y recibe en un correo electrónico es variada, desde texto simple a archivos como música, video, imágenes, entre otros.

El personal docente y administrativo de la División de Ingenierías Civil y Geomática de la Facultad de Ingeniería utiliza el correo electrónico diariamente para realizar diferentes tareas así como para mantenerse comunicado con alumnos, familiares, conocidos, entre otros.

La implementación del servidor se realizó con los recursos y requerimientos propios ofrecidos por la DICyG los cuales fueron la base para la creación de las primeras cuentas así como la determinación del espacio de almacenamiento que tendrían, de esta forma se garantiza un servicio eficiente y rápido, evitando que el servidor se sature de mensajes o se quede sin espacio para crear más cuentas.

En cuanto a las medidas de seguridad, se actualizó el antivirus del servidor, así como la implementación de listas negras para evitar virus, troyanos o correos basura. La gestión de las cuentas y contraseñas depende únicamente del administrador del servicio, por lo tanto la información de los usuarios estará a salvo de terceros.

Referente al mantenimiento, el equipo se mantendrá en un lugar seco, con temperatura óptima para evitar el calentamiento y aislado de los usuarios, para prevenir golpes o desconexión de los cables.

Se puede concluir que se han logrado con éxito los objetivos planteados y las metas propuestas al implementar y configurar satisfactoriamente el servidor de correo electrónico. El conjunto de seguridad, mantenimiento y administración de las cuentas hacen del servicio una herramienta segura y eficaz de comunicación. La DICyG cuenta ahora con un servicio de correo propio, el personal docente y administrativo ya no necesitará utilizar su cuenta personal o tener varias cuentas con diferentes usos dentro de un mismo servidor para brindar u obtener información de la misma. Además, cuando se esté navegando en Internet y se ingrese la cuenta a algún foro, empresa u otros servicios que requieran de una cuenta se sabrá que viene de la División de Ingenierías Civil y Geomática de la Facultad de Ingeniería de la UNAM. Cabe mencionar que este servicio de correo es una herramienta para el intercambio de información institucional, y no, una herramienta de difusión masiva e indistinta de información.

Trabajos a futuro

El trabajo presentado fue desarrollado con las versión más estable de Zimbra y de su antivirus, pero con el paso del tiempo, las versiones van cambiando mejorando sus aplicaciones, seguridad, entorno, entre otras cosas y por lo tanto, como trabajos a futuro, se recomiendan los siguiente:

La actualización para cualquier sistema es fundamental, ya que permite mejorar el rendimiento del sistema y sacarle el mayor provecho posible, por ello se considera importante migrar a la versión de Zimbra actual y más estable, permitiendo así una gran mejora para el mismo.

La DICyG cuenta con un número determinado de personal académico y administrativo pero es posible que la lista aumente con el paso del tiempo, creciendo los usuarios para el servidor. Si esto sucediera es fundamental incrementar la capacidad del equipo, tanto del disco duro como la RAM para tener una mayor capacidad y seguir ofreciendo un servicio óptimo.

Para poder incrementar la robustez de seguridad en el servidor, se debe actualizar el antivirus a su versión más reciente y estable, así como instalar un nuevo antivirus u otras herramientas de seguridad, evitando con ello el acceso no-autorizado de usuarios a los recursos propios del sistema, y proteger la exportación privada de información sin consentimiento del mismo.

El implementar un programa que realice el upgrade automático del antivirus, simplificaría el trabajo del administrador siempre y cuando se lleve a cabo un proceso de planeación y análisis del mismo, puesto que de ello depende el éxito de la operación.

El implementar un programa que mueva automáticamente los archivos maliciosos encontrados en el servidor a una carpeta determinada para su posterior eliminación permitirá que el administrador tenga plena seguridad de que el sistema no tiene ningún tipo de virus que pueda afectar el rendimiento del mismo.

El implementar un programa para apoyar las listas negras con las que cuenta el servidor, facilitando la detección de correos basura o de dominios falsos, esto mejoraría la detección y eliminación de correo basura así como reducción de tiempo al no tener que eliminarlos manualmente.

Tener un respaldo de la lista de contactos registrados en el sistema permitiría tener un control y registro de las cuentas actuales que se encuentran en el servidor, por lo tanto, se considera importante implementar un programa que obtenga de manera automática, en un intervalo de tiempo, la lista de contactos almacenados el servidor y que la envíe al correo del administrador para que tenga acceso a esta información y pueda manipular la gestión de las cuentas si es necesario.

El implementar un programa que obtenga de manera automática, en un intervalo de tiempo, la información de las cuentas de los contactos y lo envíe al servidor de respaldo, permitirá que cualquier incidente que llegase a presentar el servidor (por mínimo que este sea) no perjudique a la información de las cuentas ni el uso del servicio.

Anexo A

Guía rápida del Usuario

Esta guía explica brevemente las funciones que puede realizar el usuario del correo de la DICyG.

Para acceder a la interfaz, se debe ingresar a la IP del servidor, aparecerá el aviso de certificado de seguridad, dar en la opción añadir excepción para poder acceder a la cuenta para que se muestre la pantalla de bienvenida del cliente de correo.

Para ingresar a la cuenta se tendrá que ingresar el usuario y contraseña proporcionados por el administrador del servicio.

Figura 6.1: Acceso a la cuenta del usuario

Una vez dentro se mostrará la Bandeja de entrada, en ella se encuentran los correos que se han recibido y su estado: leídos y no leídos. Indica también si se ha hecho algún seguimiento en los mensajes, si tiene etiqueta, su prioridad, el asunto, en que carpeta se localiza, su tamaño y hora de llegada.

También se puede visualizar las carpetas que se han creado, las etiquetas, las aplicaciones que se pueden utilizar, entre otras cosas.

Este panel consta de ocho partes las cuales se enlistan a continuación:

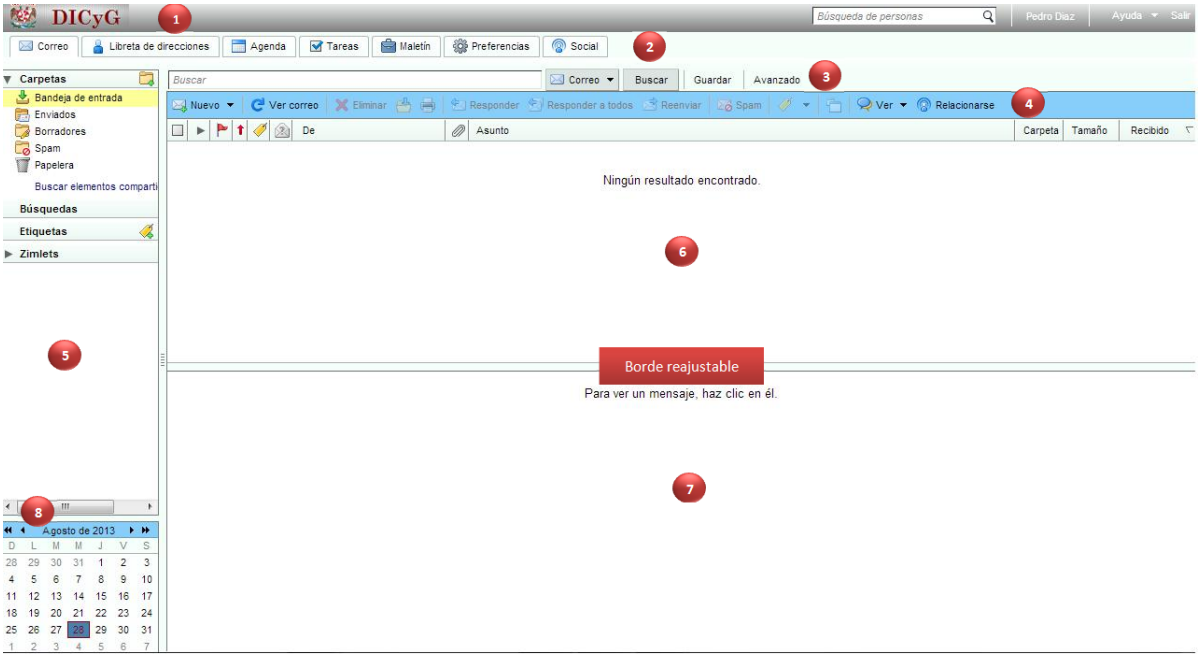


Figura 6.2: Bandeja de entrada

1. *Cabecera de la página*. En esta zona se encuentra el ícono de la institución, el panel de búsqueda, el nombre de usuario, el ícono de ayuda y salir.

2. *Pestañas de las aplicaciones*. En esta zona se encuentran las aplicaciones a las que se puede acceder: Correo, Libreta de direcciones, Agenda, Maletín, Preferencias y Social.

3. *Barra de búsqueda*. En esta zona se encuentran las búsquedas: búsqueda, búsqueda avanzada y guardar las búsquedas.

4. *Barra de herramientas*. En esta zona se encuentran las acciones de la aplicación actual. Al acceder a la cuenta, se visualiza la barra de herramientas de la aplicación de correo.

5. *Panel de resumen*. Esta zona contiene:

   a) *Carpetas*: Muestra las carpetas principales: Bandeja de entrada, enviados, borradores, *spam*, papelera y las carpetas creadas por el usuario, además de mostrar el recuento de los mensajes no leídos (número al lado de la carpeta entre paréntesis) y el tamaño en kb que tiene cada carpeta.

   b) *Búsquedas*: Muestra las búsquedas que se hayan realizado y guardado.

   c) *Etiquetas*: Muestra las etiquetas creadas por el usuario.

   d) *Zimlet*: Muestra aplicaciones que han sido creadas por terceros y que pueden integrarse al buzón de correo.

6. *Panel de contenido*. Esta zona muestra el contenido de la aplicación que se esté utilizando.

7. *Panel de lectura*. En esta zona se puede previsualizar los mensajes.

8. *Calendario*. Esta zona muestra el calendario. También puede mostrar la agenda.

Correo

La pestaña de *Correo* es la primera que se visualiza al momento de ingresar a la cuenta, ya que lo primero que se muestra es la *bandeja de entrada*. Para crear un nuevo correo dar clic en la opción *Nuevo*, se desplegará una nueva ventana.

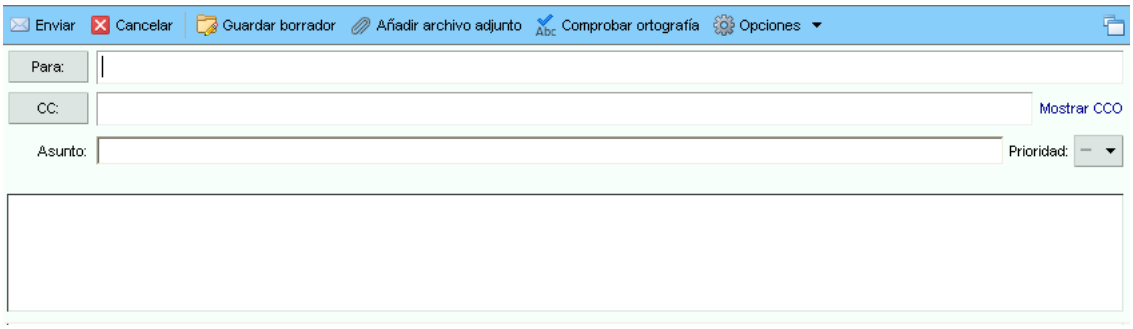


Figura 6.3: Nuevo correo

En esta ventana se pide ingresar la o las cuentas a las que se desea enviar el correo electrónico, el *asunto* del mensaje (breve explicación de lo que trata el mensaje) y su contenido.

Es necesario que el mensaje lleve un destinatario, de lo contrario, el mensaje no será enviado y, aunque el campo *asunto* no es obligatorio, se recomienda ponerlo, para darle una idea al receptor del contenido y, si en un tiempo futuro se desea volver a consultar el mensaje, encontrarlo rápidamente.

(Para responder, reenviar y reenviar a todos, se abrirá la misma ventana).

Herramientas del usuario

El usuario cuenta con varias herramientas, una de ellas es el maletín, el cual le permite guardar en el servidor información que considere importante y pueda consultarla rápidamente sin necesidad de llevar un equipo de almacenamiento de información.

También cuenta con un una agenda donde podrá anotar sus citas y el servidor se encargará de recordárselas, pasa lo mismo con las tareas.

Puede personalizar su interfaz cambiando el tema, crear firmas y personalizarlas a su gusto, como desea visualizar su bandeja de entrada, entre otros.

Esta es una explicación general de lo que puede hacer el usuario del correo electrónico, la guía del usuario completa se encuentra en la DICyG y por motivos de seguridad solamente el personal docente y administrativo de la DICyG tiene acceso a él.

Anexo B

Guía rápida del Administrador

Esta guía se explica brevemente las funciones que puede realizar el administrador del correo de la DICyG.

Para acceder a la interfaz, se debe ingresar a la IP del servidor, se mostrará la pantalla de bienvenida del servidor en donde tendrá que ingresar su usuario y contraseña para acceder a la consola de administración.

Figura 6.4: Acceso a la cuenta del administrador

Una vez dentro, se podrá visualizar el estado del servidor y los servicios que se encuentran levantados.

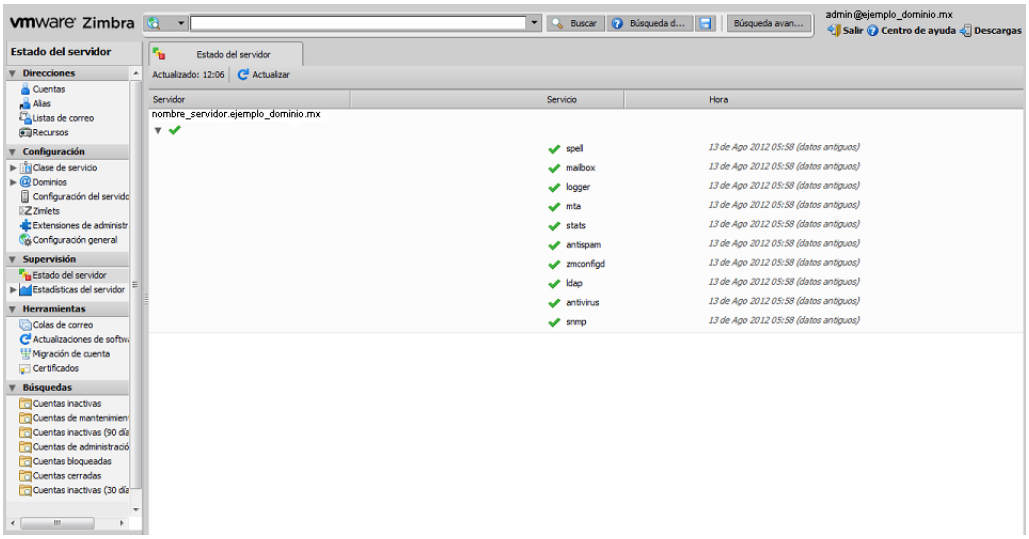


Figura 6.5: Consola de administración

Panel del administrador

El panel consta de 4 partes las cuales se enlistan a continuación:

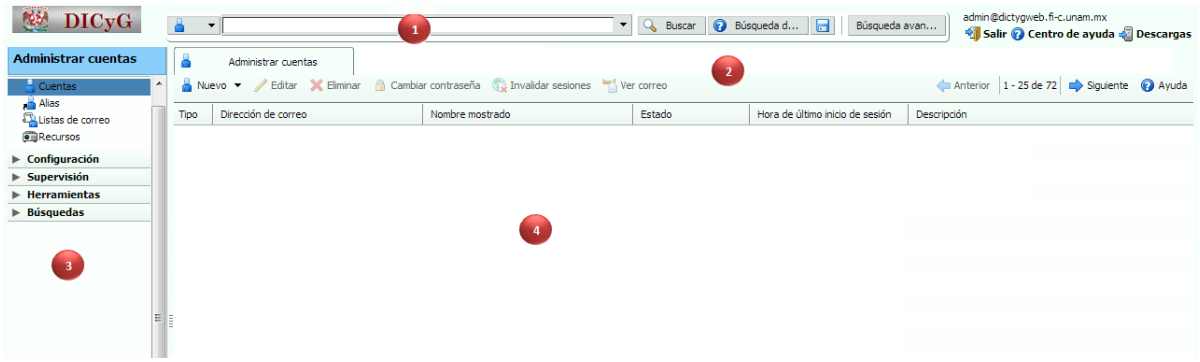


Figura 6.6: Panel de administración

1. *Panel de búsqueda*: Permite realizar una búsqueda de manera rápida, se puede realizar por cuentas específicas, alias, listas de distribución, recursos, y dominios. Buscar Ayuda es una eficaz búsqueda unificada que localiza información en los foros, wiki y documentos de Zimbra. También se puede dar clic en Búsqueda Avanzada para construir una búsqueda más personalizada.

   También cuenta con las opciones de salida (salir de la consola de administración), centro de ayuda (brinda explicación sobre las herramientas, la información varia dependiendo de la pestaña seleccionada) y descargas de aplicaciones.

2. *Panel de herramientas*: Permite realizar acciones dependiendo de la opción que tenga seleccionada.

3. *Panel de resumen*: Contiene las aplicaciones de:

   a) *Administrar cuentas*: Permite crear o modificar los datos de las cuentas, agregarles alias, crear una lista de correos e implementar recursos para las cuentas.

   b) *Configuración*: Permite modificar el contenido del servidor, como agregarle *zimlets*, otros dominios, el tipo de servicio que se está brindando así como la configuración del servidor.

   c) *Supervisión*: Permite visualizar de manera gráfica el estado del servidor, asi como el flujo de correos entrantes y salientes.

   d) *Herramientas*: Permite visualizar las colas de correo, realizar una actualización a la versión del servidor, migrar la cuenta y actualizar el certificado del servicio.

   e) *Búsquedas*: Permite visualizar más ordenadamente el estado de las cuentas: en mantenimiendo, bloqueadas, cerradas e inactivas.

4. Panel de contenido: Permite visualizar el contenido de la aplicación que se esté utilizando. Se puede abrir múltiples paneles de Contenido para una función específica. Por ejemplo, seleccionar de la lista de cuentas. Cada cuenta es abierta en una nueva pestaña detrás de la pestaña de Administración de Cuentas.

Entre las acciones que puede crear el administrador es la creación de cuentas, para esto dirigirse a *Administrar cuentas* y dar click en *Cuentas*.

Una vez ahí dar clic en la opción de *Nuevo*, que se encuentra en la *Barra de herramientas* se desplegará un menú con campos para ingresar la información del nuevo usuario. Esta información va desde los datos básicos como lo son el nombre de la cuenta, nombre del usuario, apellido y contraseña, así como datos más personales como lo son el teléfono, oficina, dirección, fax, entre otros.

A continuación se muestra la información que se puede ingresar cuando se crea una nueva cuenta:

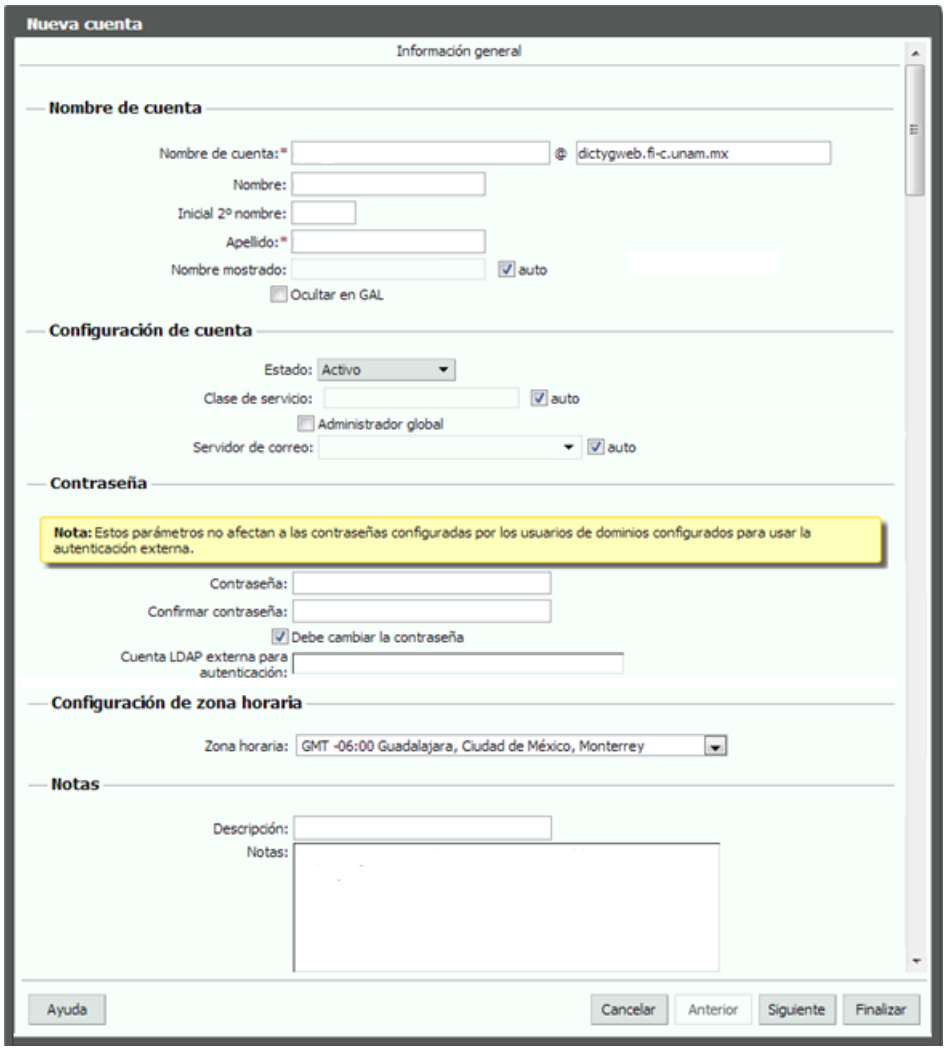


Figura 6.7: Crear cuenta

Una vez creada la cuenta con los datos mínimos (nombre y apellido del usuario, nombre de la cuenta y contraseña) se le notifica al usuario de que su cuenta está activa y puede hacer uso de ella en el momento que lo desee.

En la consola de administrador también se puede privar al usuario de ciertas aplicaciones, temas, entre otros, por lo que el administrador es totalmente responsable de las herramientas que puede visualizar y, por ende, utilizar el usuario.

Estado del servidor

Dentro de las ventajas que ofrece la consola de administración al administrador es poder visualizar gráficamente el estado actual del servidor, así como del almacenamiento que tiene cada cuenta y el espacio que ha utilizado, el flujo de mensajes en un lapso de tiempo, mensajes en cola y el estado de las cuentas.

Esta es una explicación general de lo que puede hacer el administrador del correo electrónico, la guía de administración completa se encuentra en la DICyG y por motivos de seguridad solamente el administrador del servicio tiene acceso a él.

Anexo C

Formato de solicitud de la cuenta

La División de Ingeniería Civil y Geomatica se encargará de las cuentas para el personal académico y administrativo de la misma. Para la obtención de una cuenta, el interesado deberá pedir el formato[1] para la misma y llenar los campos solicitados.

Una vez hecha la petición deberá firmarse tanto por la persona que hizo la solicitud como por el Jefe de la unidad de cómputo, posteriormente el formato será entregado al administrador quien será el encargado de dar de alta la cuenta. Esto se hace con el fin de tener un control en la asignación de cuentas al personal de la División y, como medida de seguridad, todo tipo de actividad que se realice al servidor será responsabilidad del administrador.

UNAM

DIVISIÓN DE INGENIERÍAS CIVIL Y GEOMÁTICA
UNIDAD DE CÓMPUTO

FORMATO DE SOLICITUD PARA CUENTA DE CORREO DE LA DICyG

Fecha: _____

Nombre: _____

Cargo: _____

Correo electrónico alternativo: _____

Solicitud:

- ☐ Alta
- ☐ Baja
- ☐ Restablecer contraseña
- ☐ Desbloqueo / Activación

Motivo de la solicitud: _____

Nombre de usuario sugerido: _____ @dicyg.fi-c.unam.mx

☐ Conozco y acepto los términos establecidos en las políticas de seguridad de la División de Ingenierías Civil y Geomática de la Facultad de Ingeniería.

Firma del solicitante

M. en I. Tanya Itzel Arteaga Ricci
Jefa de la Unidad de Cómputo

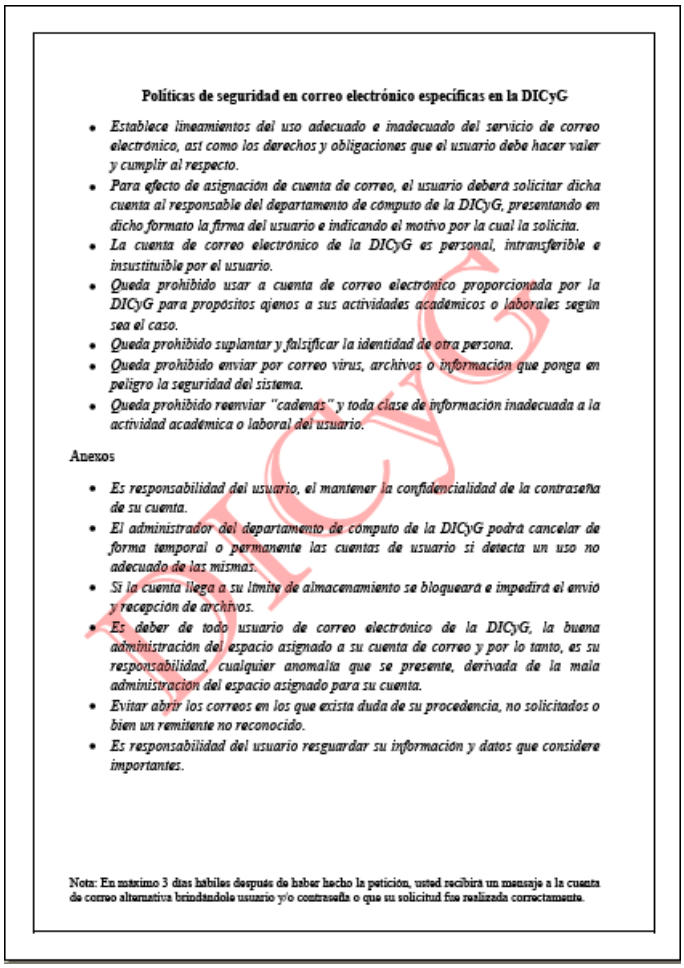
Nota: En máximo 3 días hábiles después de haber hecho la petición, usted recibirá un mensaje a la cuenta de correo alternativa brindándole usuario y/o contraseña o que su solicitud fue realizada correctamente.

DICyG

Figura 6.8: Formato de solicitud de cuenta

[1] El formato debe pedirse al Jefe de la Unidad de Cómputo.

También, junto con el formato de solicitud, vienen incluidas las políticas de seguridad que el usuario debe tener en cuenta al momento de hacer uso de la cuenta de correo electrónico.



Políticas de seguridad en correo electrónico específicas en la DICyG

- *Establece lineamientos del uso adecuado e inadecuado del servicio de correo electrónico, así como los derechos y obligaciones que el usuario debe hacer valer y cumplir al respecto.*
- *Para efecto de asignación de cuenta de correo, el usuario deberá solicitar dicha cuenta al responsable del departamento de cómputo de la DICyG, presentando en dicho formato la firma del usuario e indicando el motivo por la cual la solicita.*
- *La cuenta de correo electrónico de la DICyG es personal, intransferible e insustituible por el usuario.*
- *Queda prohibido usar a cuenta de correo electrónico proporcionada por la DICyG para propósitos ajenos a sus actividades académicos o laborales según sea el caso.*
- *Queda prohibido suplantar y falsificar la identidad de otra persona.*
- *Queda prohibido enviar por correo virus, archivos o información que ponga en peligro la seguridad del sistema.*
- *Queda prohibido reenviar "cadenas" y toda clase de información inadecuada a la actividad académica o laboral del usuario.*

Anexos

- *Es responsabilidad del usuario, el mantener la confidencialidad de la contraseña de su cuenta.*
- *El administrador del departamento de cómputo de la DICyG podrá cancelar de forma temporal o permanente las cuentas de usuario si detecta un uso no adecuado de las mismas.*
- *Si la cuenta llega a su límite de almacenamiento se bloqueará e impedirá el envió y recepción de archivos.*
- *Es deber de todo usuario de correo electrónico de la DICyG, la buena administración del espacio asignado a su cuenta de correo y por lo tanto, es su responsabilidad, cualquier anomalía que se presente, derivada de la mala administración del espacio asignado para su cuenta.*
- *Evitar abrir los correos en los que exista duda de su procedencia, no solicitados o bien un remitente no reconocido.*
- *Es responsabilidad del usuario resguardar su información y datos que considere importantes.*

Nota: En máximo 3 días hábiles después de haber hecho la petición, usted recibirá un mensaje a la cuenta de correo alternativa brindándole usuario y/o contraseña o que su solicitud fue realizada correctamente.

Figura 6.9: Políticas de seguridad de la División

Glosario

A

Antispyware. Programa o aplicación de seguridad, encargado de la lucha contra los programas espía (*spyware*).

API (*Application Programming Interface* - Interfaz de Programación de Aplicaciones). Conjunto de funciones o métodos usados para acceder a ciertas funcionalidades.

ARPANET (*Advanced Research Projects Administration Network* - Red de la Agencia de Proyectos de Investigación Avanzada). Sistema de red informática del cual nació Internet.

ASCII (*American Standard Code for Information Interchange* - Código Estándar Estadounidense para el Intercambio de Información). Código estándar definido y establecido para representar los caracteres (letras, números, signos de puntuación, caracteres especiales, etc.) de forma numérica.

Atenuación. Pérdida de la potencia de una señal.

B

BIOS. Conjunto de programas que permite arrancar la computadora (parte del sistema de arranque).

Bits (*Binary digit* - Dígito binario). Unidad más pequeña de la información digital con la que trabajan las computadoras.

Bluethoot. Tecnología de comunicación inalámbrica que posibilita la transmisión de voz y datos entre diferentes dispositivos mediante un enlace por radiofrecuencia segura en un rango pequeño.

Broadcast. Envía la información a todos los elementos de una subred.

Broadcast ID (Dirección de broadcast). Dirección que tiene los bits del host iguales a 255.

Bucle. Sentencia que permite ejecutar de forma repetitiva un comando o grupo de comandos un número determinado de veces.

Buffer. Espacio de memoria, en el que se almacenan datos para evitar que el programa o recurso que los requiere, ya sea *hardware* o *software*, se quede sin datos durante una transferencia.

Bus. Sistema digital que transfiere datos entre los componentes de una computadora o entre computadoras.

Byte. Unidad que mide la cantidad de información, tamaño y capacidad de almacenamiento. Un Byte, equivale a 8 Bits.

C

Caracteres. Símbolos utilizados para escribir como: letras, números y signos especiales.

Computadora. Aparato electrónico que recibe datos de entrada y los procesa para convertirla en información útil.

Conmutación. Técnica que sirve para hacer un uso eficiente de los enlaces físicos en una red de computadoras.

D

Datagramas. Archivo que se envía por Internet; puede ser un archivo entero o una parte de él, pero con la suficiente información para que la red pueda simplemente encaminar el fragmento hacia el equipo terminal de datos receptor, de manera independiente a los fragmentos restantes.

Demonio (*Daemon, Disk And Execution Monitor* - Disco y Seguimiento de la ejecución). Proceso informático no interactivo, es decir, que se ejecuta en segundo plano en vez de ser controlado directamente por el usuario. Este tipo de proceso continua en el sistema, es decir, que puede ser ejecutado en forma persistente o reiniciado si se intenta matar el proceso dependiendo de su configuración.

Dispositivos de red. Aparato que mueve y controla el tráfico de la red.

DNS (*Domain Name System* – Sistema de Nombres de Dominio). Conjunto de protocolos y servicios (base de datos distribuida) que permite a los usuarios utilizar nombres en vez de tener que recordar direcciones IP numéricas.

Dpkg. Base del sistema de gestión de paquetes de Debian GNU/Linux.

E

E-gobierno (*Internetworked Government* - Gobierno Electrónico). Transforma las operaciones gubernamentales utilizando las Tecnologías de la Información para mejorar la efectividad y la eficiencia de los poderes del Estado y, de esta manera, ponerlos de manera efectiva al servicio del ciudadano.

Ethernet. Estándar de comunicación establecido por el Instituto de Ingenieros Eléctricos y Electrónicos (IEE) conocido como IEEE 802.3. Este estándar es utilizado en las redes de área local o LAN para transmitir información.

F

Firewall. Colección de componentes colocados entre una red interna y una red externa para que sólo el tráfico que es autorizado por la política de seguridad de la red interna éste permitido para pasar.

Formatear. Dar formato a una unidad de disco, eliminando todo su contenido.

FQDN (*Fully Qualified Domain Name* - Nombre de Dominio Plenamente Calificado). Señala la posición jerárquica más importante en el DNS. Se distingue de un nombre regular porque lleva un punto al final.

FSF (*Free Software Foundation* - Fundación de Software Libre). Fundación dedicada a eliminar las restricciones sobre la copia, redistribución, entendimiento, y modificación de programas de computadoras, promocionando el desarrollo y uso del software libre en todas las áreas de la computación, pero muy particularmente, ayudando a desarrollar el sistema operativo GNU.

G

GB (Gigabyte). Unidad de almacenamiento de información cuyo símbolo es el GB.

GPL (*General Public License* -Licencia Publica General). Licencia creada por la Free Software Foundation (FSF) y orientada principalmente a los términos de distribución, modificación y uso de software libre.

GSM (*Groupe Special Mobile* - Sistema Global para las comunicaciones Móviles). Especifícación de telefonía móvil digital que busca consolidarse como el estándar europeo de telefonía celular, de forma que se pueda utilizar un mismo teléfono en cualquier país del continente.

Gusanos. Programa similar a un virus que, a diferencia de éste, solamente realiza copias de sí mismo, o de partes de él.

H

Hardware. Componentes y dispositivos físicos y tangibles que forman una computadora.

HLR (*Home Location Register* - Registro de Localización Local). Base de datos de todos los números de teléfono móvil en una red GSM.

Host (Anfitrión). Equipo directamente conectado a una red y que efectúa las funciones de un servidor.

Hub (Concentrador). Dispositivo que permite conectar varios equipos entre sí retransmitiendo los paquetes de datos desde cualquier equipo hacía todos los demás usando una misma conexión.

I

Infrarrojo. Emisión de ondas electromagnéticas a corta distancia que permiten la comunicación entre dos nodos, usando leds infrarrojos para ello.

Internet. Conjunto de redes descentralizadas comunicadas entre sí que operan a través de un protocolo en común.

IP (*Internet Protocol* - Protocolo Internet). Protocolo no orientado a conexión cuyo objetivo principal es transmitir los datagramas (también llamados paquetes) a través de las redes desde su origen a su destino, asignando a cada equipo un número único que le sirve como identificador dentro de la red.

L

Log (Registro en inglés). Archivo que hace un seguimiento de las conexiones de red.

M

Malware (Abreviatura de *Malicious Software*). Software malicioso que tiene como objeto instalarse en un equipo sin autorización y realizar funciones no deseadas.

Mb (Megabyte). Unidad que sirve para medir cantidad de datos informáticos.

Memoria caché. Sistema especial de almacenamiento de alta velocidad. Puede ser tanto un área reservada de la memoria principal como un dispositivo de almacenamiento de alta velocidad independiente.

Metadatos. Datos altamente estructurados que describen información, describen el contenido, la calidad, la condición y otras características de los datos.

Microprocesador. Circuito integrado fundamental de un CPU.

Modelo OSI. Arquitectura formada por siete capas, las cuales se encargaran de descomponer el proceso de la comunicación en varios problemas más sencillos, de manera que cada capa resolverá un problema en específico.

Modelo TCP/IP. Permite la comunicación entre diferentes computadoras con distinto sistema operativo sobre redes de área local (LAN) o redes de área extensa (WAN).

MS-DOS (*MicroSoft Disk Operating System* - Sistema Operativo de Disco de Microsoft). Sistema operativo, anterior a Windows, en el que se trabaja escribiendo órdenes para todas las operaciones que se desean realizar.

Multicast. Comunicación entre un solo emisor y múltiples receptores en una red.

Multimedia. Combinación de dos o más medios para transmitir información tales como texto, imágenes, animaciones, sonido y video que llega al usuario a través de la computadora u otros medios electrónicos.

N

No-breaks. Regulador de corriente con una batería de respaldo en caso de ausencia de energía. Este respaldo se mantiene hasta que la energía de las baterías se agota o hasta que el suministro de energía normal se restablece; al ocurrir esto último el sistema recarga las baterías.

Nodo. Punto de intersección en el que coinciden dos o más elementos de una red.

O

Onda electromagnética. Expansión de radiaciones electromagnéticas mediante el espacio

P

Paquete. Porción de información que viaja por la red.

Parche. Actualización de un programa usado para solucionar problemas, vulnerabilidades o defectos de funcionamiento.

Pasarela. Dispositivo que conecta dos o más redes permitiendo que la información de una pase a otra según criterios predeterminados.

Periférico. Dispositivo electrónico o unidad externa que se conecta a una computadora a través de los puertos.

Phishing. Consiste en el envío masivo de mensajes que, aparentando provenir de fuentes fiables, intentan conseguir que el usuario proporcione datos confidenciales. El caso más típico de phishing es el envío de correos electrónicos que se hacen pasar por procedentes de una entidad bancaria online, para conseguir que el usuario introduzca sus contraseñas en una página web falseada.

Plugin. Aplicación informática que añade funcionalidades específicas a un sistema ya existente.

Programa. Conjunto de instrucciones que se dan a una computadora para que ejecute una determinada tarea.

Protocolo. Reglas estándar que rigen la forma en que las computadoras se comunican entre sí.

Proxy. Sistema intermediario entre anfitriones internos de una red y los anfitriones de Internet de forma tal que recibe las requisiciones de unos y se las pasa a los otros previa verificación de accesos y privilegios.

R

Red. Conjunto de computadoras conectadas entre sí por medio de dispositivos físicos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos para compartir información, recursos y ofrecer servicios.

Reiniciar. Sentencia que indica volver a iniciar la computadora.

RFC (*Request for Comments* - Solicitud de Comentarios). Cconjunto de documentos que describen los protocolos de Internet o propuestas para un nuevo protocolo.

Root. Término utilizado para definir a la cuenta de usuario que posee todos los derechos para modificar lo que ocurre en el sistema. Usuario principal o administrador.

Routers. Dispositivo de *hardware* para interconexión de red de computadoras, el cual permite asegurar el camino de paquetes entre redes o determinar la mejor ruta que debe tomar el paquete de datos.

S

Software. Equipamiento lógico e intangible como los programas y datos que almacena la computadora.

Spam. Correo electrónico no solicitado, normalmente con contenido publicitario, que se envía de forma masiva.

Spyware. *Software* espía que suele mostrar anuncios emergentes, recopilar información sobre el usuario o cambiar la configuración del equipo sin consentimiento del usuario.

SSL. Protocolo de red de cifrado de datos que permite efectuar una transmisión segura entre un servidor y un cliente.

Switch. Dispositivo digital que permite interconectar redes de computadoras.

T

TCP (*Transmission Control Protocol* - Protocolo de Control de Transmisión). Protocolo orientado a conexión, cuyo objetivo principal es entregar los datagramas a su destino sin errores ni duplicados, entregando los datos en el mismo orden en que fueron enviados.

Token. Cadena de bits que viaja por las redes token ring.

Topología. Arreglo físico o lógico en el cual los dispositivos o nodos de una red se interconectan entre sí mediante un medio de comunicación.

Troyanos. *Software* malicioso capaz de alojarse en computadoras y permitir el acceso a usuarios externos, a través de una red local o de Internet, con el fin de recabar información.

U

USB (*Universal Serial Bus* - Bus Universal en Serie). Puerto que sirve para conectar periféricos a una computadora.

URL (*Uniform Resource Locator* - Localizador Uniforme de Recursos). Dirección que identifica de forma única a los recursos que se encuentran en Internet como por ejemplo: una imágen, una página, entre otros.

V

Virus. Programa que infecta documentos o sistemas mediante la inserción o la agregación de una copia de sí mismo o mediante la reescritura de archivos completos. Los virus trabajan sin el conocimiento ni la autorización del usuario.

W

Web. Sistema de distribución de información a través de hipertexto accesible vía Internet.

X

XML (*Extensible Markup Language* - Lenguaje de Marcas Extensible). Formato de texto estandarizado que sirve para representar información estructurada en la Web.

Z

Zombie. Equipo informático que ha sido infectado por algún tipo de malware y que como consecuencia es usado remotamente sin el consentimiento del dueño de la misma, para realizar ataques informáticos y otro tipo de actividades delictivas.

Bibliografía

Libros:

[1] Andrew S. Tanenbaum. Redes de computadoras. Universidad Libre de Ámsterdam, Prentice-Hall, Tercera Edición,1998. Páginas: 35, 523-525, 658-660.

[2] Douglas E. Comer. Redes Globales de Información con Internet y TCP/IP: principios básicos, protocolos y arquitectura. Prentice-Hall, Tercera Edición, 1996. Páginas: 93-96, 168, 169, 193-197, 389, 390, 447, 449, 573.

[3] Enrique Herrera Pérez. Tecnologías y redes de transmisión de datos. México, Limusa, 2003. Páginas: 60-67.

[4] Francisco Solsona, Elisa Viso Gurovich, Mauricio Aldazosa. Manual de Supervivencia en Linux. México, UNAM, Facultad de ciencias, 2007. Páginas: 3, 77-79.

[5] Jorge Lázaro Laporta, Marcel Miralles Aguiñiga. Fundamentos de telemática. España, Universidad Politécnica de Valencia, 2005. Páginas: 18, 19, 24-54.

[6] José Antonio Carballar Falcón. VoIP : la telefonía de Internet. Paraninfo, 2007. Páginas: 58-70.

[7] June Jamrich Parsons. Conceptos de Computación: Nuevas Perspectivas. Cengage Learning, Décima Edición, 2008. Páginas: 13, 15-23.

[8] María Carmen España Boquera. Servicios avanzados de telecomunicación. España, Díaz de Santos. 2003. Páginas: 175-187, 196-200.

[9] María Jaquelina López Barrientos y Cintia Quezada Reyes. Fundamentos de seguridad informática. México, UNAM, Facultad de Ingeniería, 2006. Páginas: 100-103, 207-218.

[10] Pablo Gil Vázquez, Jorge Pomares Baeza, Francisco A. Candelas Herías. Redes y transmisión de datos. Universidad de Alicante, 2010. Páginas: 18, 22-28, 82-90.

[11] Sonia Silva Salinas, Catherin López Sanjurjo. Internet y correo electronico. España, Vigo. 2003. Páginas: 2-5, 8, 9, 11, 67,68, 70, 71-82,99,100,105-113.

[12] William Stallings. Comunicaciones y Redes de Computadores. Sexta Edición. Páginas: 30-23, 41-44, 47, 51, 52, 103-109, 112-118.

Apuntes de clase:

[13] Apuntes de la materia Arquitectura Cliente/Servidor.

Profesor: Ing. Anaid Guevara Soriano. Semestre 2011-2.

[14] Apuntes de la materia Redes de Computadoras.

Profesor: M.C. María Jaquelina, López Barrientos .Semestre 2010 - 2.

Referencias:

[15] Comparativa: Windows y Linux. Consultado el día 27 de abril de 2013.
http://es.scribd.com/doc/60501230/Comparacion-y-Caracteristicas-Windows-vs-Linux#download

[16] Correo electrónico. Consultado el día 11 de febrero de 2013.
http://www.maestrosdelweb.com/editorial/emailhis/

[17] Dominios Genéricos. Consultado el día 26 de marzo de 2013.
http://www.pyme.net.uy/documentos/codigos_dominios.htm

[18] Instalación de Zimbra. Consultado el día 10 de agosto de 2013.
http://www.zimbra.com/forums/spanish/48767-instalacion-zimbra-desde-cero-para-novatos.html

[19] Medios de Transmisión. Consultado el día 25 de enero de 2013.
http://arquitecturapc.blogspot.es/1207606620/

[20] Origen de Internet. Consultado el día 05 de enero de 2013.
http://www.tuobra.unam.mx/publicadas/010815132146-Title.html

[21] Partes de un correo electrónico. Consultado el día 11 de febrero de 2013.
http://briyit.blogspot.mx/2007/11/partes-de-una-direccion-de-correo.html

[22] Políticas de Seguridad. Consultado el día 15 de agosto de 2013.
http://www.ingenieria.unam.mx/cacfi/documentos/politicasseguridad.pdf

[23] Puertos. Consultado el día 25 de febrero de 2013.
http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-sg-es-4/ch-ports.html

[24] Redes MAN, LAN, WAN, CAN. Consultado el día 19 de enero de 2013.
http://www.eveliux.com/mx/redes-lan-can-man-y-wan.php

[25] Registros DNS. Consultado el día 10 de abril de 2013.
http://www.chile-dominios.com/ai/93/gestin-de-registros-de-recursos-dns

[26] Registros de Recursos (RR). Consultado el día 10 de abril de 2013.
http://es.scribd.com/doc/50704342/9/Registros-de-Recursos-RR

[27] RFC. Consultado el día 05 de marzo de 2013.
http://www.rfc-editor.org/search/rfc_search.php

[28] Servidor DNS. Consultado el día 13 de marzo de 2013.
http://www.ite.educacion.es/formacion/materiales/85/cd/linux/m2/servidor_dns_bind9.html

[29] Sistema Operativo. Consultado el día 25 de abril de 2013.
http://www.uclm.es/profesorado/licesio/Docencia/IB/IBTema3a.pdf

[30] Tecnologías de Información. Consultado el día 10 de enero de 2013.
http://webdelprofesor.ula.ve/ciencias/sanrey/tics.pdf

[31] Windows y Linux. Consultado el día 27 abril de 2013.
http://tecnoblogy.wordpress.com/2006/12/18/comparativa-windows-vs-linux/