3 Arquitectura propuesta.

3.1 Cómo funciona el correo electrónico.

De la amplia gama de servicios que actualmente proporcionan los ISPs (Internet Service Provider, Proveedor de Servicios de Internet), puede que la más crítica sea el correo electrónico, o e-mail. No importa qué otros servicios y calidades pueda ofrecer un ISP; si el correo electrónico no es fiable, sus clientes cambiarán de proveedor.

Para explicar cómo funciona el correo electrónico, comenzaremos con algunas definiciones:

- Sistema de correo: es el conjunto de hardware, software y cualquier otra infraestructura que permiten a un ISP recibir y entregar correos. Por ejemplo, sus componentes son: servidores y sus sistemas operativos, electrónica de red, aplicaciones software de monitorización y gestión, etc.

- Software de correo: son las aplicaciones de software encargadas del enrutamiento y la entrega de correos, así como la administración de los usuarios.

- Servicio de correo: son los procesos y el personal que ponen en marcha todos los componentes por parte del ISP. Esto incluye personal de marketing, ventas, técnicos, etc. Además, contar con un servicio de soporte rápido y con gran capacidad de acción redundará en la satisfacción del cliente final.

3.1.1 Protocolos.

El sistema de correo seguirá una arquitectura de tipo cliente/servidor. A continuación describimos los protocolos que van a ser fundamentales:

- SMTP (Simple Mail Transport Protocol, Protocolo Simple de Transporte de Correo). Es el protocolo estándar de Internet utilizado por los servidores y los clientes de correo para la transmisión de correo electrónico.

- POP (Post Office Protocol, Protocolo de Oficina de Correo). Es el protocolo estándar de Internet utilizado por los servidores y los clientes, que permite a estos últimos descargar un correo desde el servidor.

- IMAP (Internet Message Access Protocol, Protocolo de Acceso a Mensaje de Internet). Es un protocolo flexible para el acceso remoto desde un cliente al servidor de correo.

- LDAP (Lightweight Directory Access Protocol, Protocolo de Acceso Ligero a Directorios). Es un protocolo para buscar diversa información en una base de datos de directorio de usuarios.

- DNS (Domain Name System, Sistema de Nombres de Dominio). Es el protocolo que asocia las direcciones numéricas de Internet (Direciones IP) a nombres más fácilmente recordables (nombres de dominio).

- HTTP[S] (HyperText Transfer Protocol [Secure], Protocolo [Seguro] de transferencia de Hipertexto). HTTP es un protocolo para las transacciones entre un

navegador web y un servidor web. La versión segura (HTTPS) añade seguridad mediante SSL (Secure Sockets Layer, Capa de Conexión Segura).

3.1.2 Proceso de envío y recepción genérico.

Para tener una idea global de que elementos intervienen y cómo lo hacen durante el proceso de envío y recepción de correo, vamos a describir paso por paso un proceso genérico de este tipo. En el ejemplo se utiliza POP como protocolo de descarga de correo.

1. Alicia escribe un mensaje a su hermano Roberto en su cliente de correo electrónico.

2. Alicia pulsa el botón "enviar". Su cliente de correo electrónico traduce el mensaje y lo envía al servidor SMTP de su ISP.

3. El servidor SMTP determina el destinatario del mensaje y lo procesa adecuadamente: lo almacena si es usuario local, lo manda a su correspondiente servidor SMTP si no es local.

4. Roberto arranca su cliente de correo electrónico, el cual hace una petición POP al servidor de correo POP para poder leer el correo. El cliente de Roberto descarga el mensaje y lo almacena en el disco duro local.

A continuación examinaremos cada uno de estos pasos con más detalle.

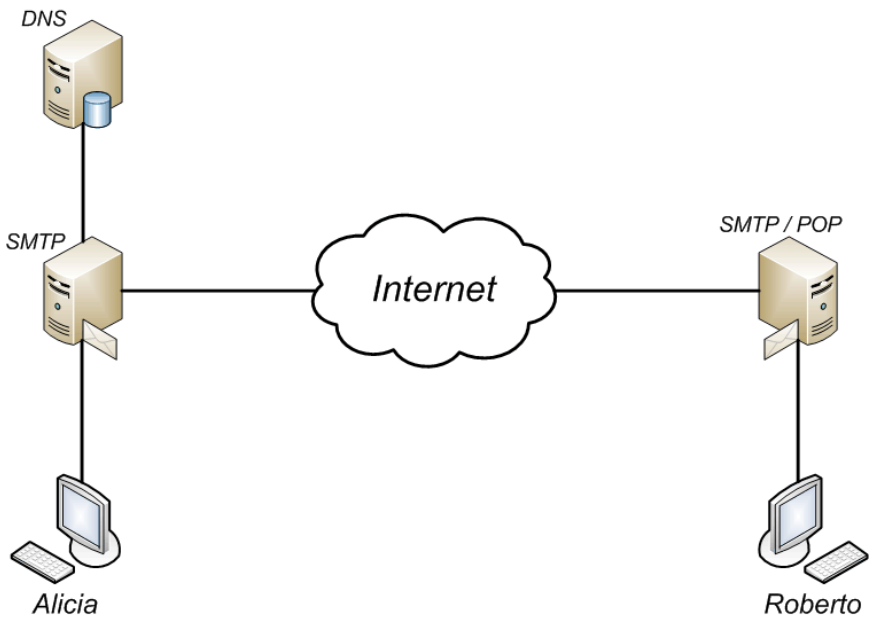

Ilustración 13: Proceso de envío y recepción de correo.

1. Composición del email.

Alicia quiere enviar un correo a Roberto. Los campos existentes para completar en un correo electrónico son:

To (Para) : destinatario o destinatarios.
From (De) : remitente.
CC (Copia), Carbon Copy, Copia de Carbón : destinatario o destinatarios en copia.
BCC (CO); Blind Carbon Copy, Copia Oculta: destinatario o destinatarios en copia no visibles para los otros destinatarios.
Subject (Asunto): texto que debe resumir el objetivo del correo.
Body (Cuerpo): texto.

Para este ejemplo no usaremos los cambios de copia, así como ningún tipo de fichero adjunto, por simplicidad. Por lo tanto, el correo que escribe Alicia es:

To: roberto@isp2.es
Subject: Prueba
Hola, esto es un correo de prueba de Alicia.

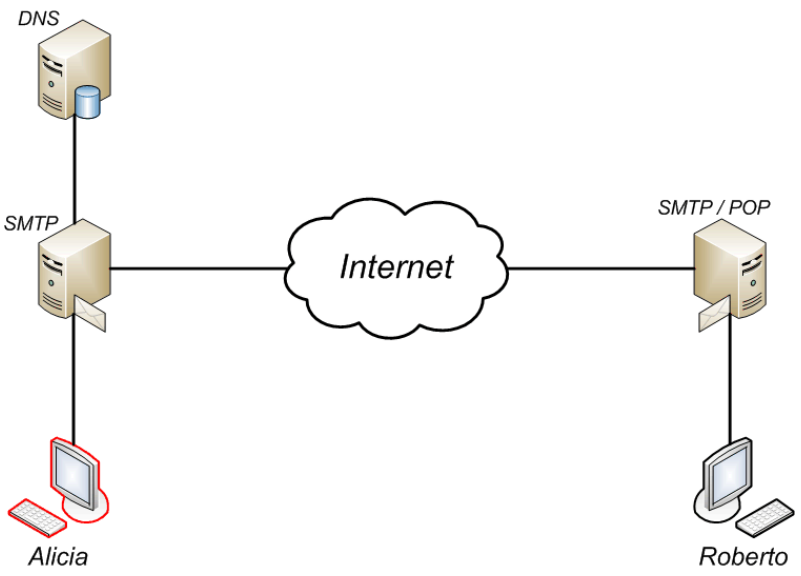

Ilustración 14: Paso 1. Composición del email.

2. Envío del email al servidor SMTP.

Cuando Alicia da la orden de enviar el correo, su cliente de correo prepara el email antes de enviarlo a su servidor SMTP:

Reply-to: alicia@isp1.es
Date: Mon, 10 Nov 2008 11:41:58 +0100
To: roberto@isp2.es
From: alicia@isp1.es
Subject: Prueba
Hola, esto es un correo de prueba de Alicia.

El cliente crea lo que se denomina encabezado del mensaje, el cual contiene todos los campos excepto el cuerpo, que queda a continuación. En el campo “Date” se especifica la fecha, hora y zona horaria; en el “Reply-to” se especifica la dirección de correo a la que responder este correo, que podría ser distinta a la del remitente, si se configura de esta forma en el cliente de correo.

A continuación, el cliente establece una conexión SMTP (TCP por el puerto 25) con el servidor SMTP configurado en el propio cliente. En esta conexión se transmite el mensaje mediante protocolo SMTP, el cual pasa a manos del servidor.

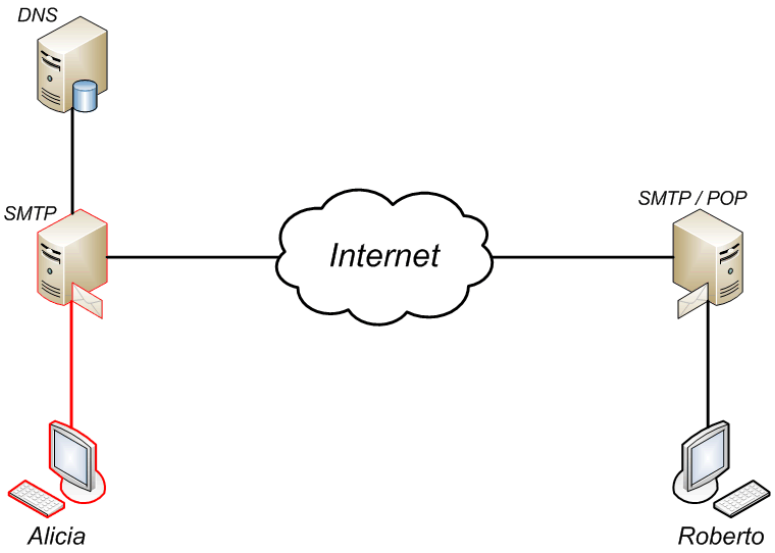

Ilustración 15: Paso 2. Envío del email.

3. El servidor SMTP procesa el email.

Cuando el servidor acepta el email, crea una nueva estructura denominada ‘envelope’ (sobre), consistente en una lista del remitente (‘Mail From’) y destinatarios (‘Rcpt To’), y que servirá para el enrutamiento del mensaje. A dicha estructura le sigue la parte de datos, compuesta a su vez de ‘header’ (cabecera) y ‘body’ (cuerpo).

Mail From: alicia@isp1.es
Rcpt To: roberto@isp2.es
Reply-to: alicia@isp1.es
Date: Mon, 10 Nov 2008 11:41:58 +0100
To: roberto@isp2.es
From: alicia@isp1.es
Subject: Prueba
Hola, esto es un correo de prueba de Alicia.

A continuación comienza en proceso para el enrutamiento del mensaje. En este momento, la cabecera del email es marcada con el campo ‘Received’, anotando el nombre del servidor SMTP y la hora y fecha correspondiente.

De esta forma, el email queda marcado por cada uno de los servidores SMTP que lo van enrutando desde el origen hasta el destino. Además, cada mensaje es marcado con un identificador único por el primer servidor SMTP que lo transmite, en el campo 'Msg-ID' de la cabecera.

Return-Path: <alicia@isp1.es>
Received: from correo.isp1.es by mx.isp1.es; Mon, 10 Nov 2008 11:42:05 +0100
Msg-ID: <3.0.32.19971028153358.01e80e40@correo.isp1.es>
Reply-to: alicia@isp1.es
Date: Mon, 10 Nov 2008 11:41:58 +0100
To: roberto@isp2.es
From: alicia@isp1.es
Subject: Prueba
Hola, esto es un correo de prueba de Alicia.
Ahora llega el momento de decidir adónde entregar el correo. Existen dos posibilidades:

- El destinatario es un usuario local. El mensaje es almacenado en su buzón de correo correspondiente.

- El destinatario no es usuario local. El servidor necesita saber a que servidor SMTP debe mandar el correo. Para ello, mira el registro MX (Mail eXchanger) correspondiente al dominio del destinatario. En nuestro caso, el servidor correo1.isp1.es haría una petición DNS para obtener el registro MX correspondiente al dominio isp2.es; una vez obtenido el servidor (en nuestro caso, correo.isp2.es) se establece una conexión SMTP entre ambos servidores para la transmisión del correo electrónico. Cuando el mensaje llega al servidor local al destinatario, este es almacenado en su buzón de correo correspondiente.

Una vez que el correo se encuentre en su buzón correspondiente, está disponible para que el usuario destinatario pueda recibirlo.

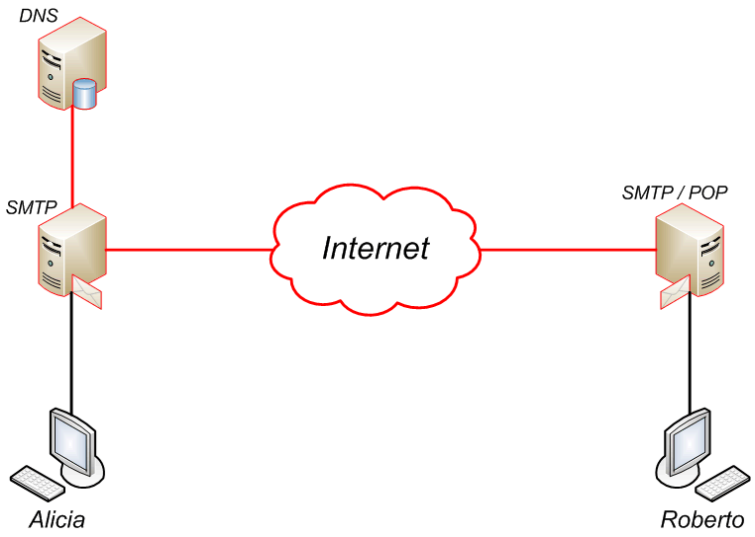

Ilustración 16: Paso 3. Procesado en el servidor.

4. Petición al servidor POP y descarga del email.

El correo electrónico es un servicio asíncrono, en el sentido de que no avisa al destinatario de la llegada de un correo. Es el propio destinatario, mediante conexión IMAP o peticiones POP, el que debe consultar sobre la llegada de un nuevo correo.

En nuestro caso, Roberto ejecuta su cliente de correo electrónico, y habiendo configurado debidamente el servidor POP, lanza un comando de sincronización. El cliente realiza una conexión POP con el servidor, el cual busca en el buzón del usuario, y responde al cliente con una lista de todos los correos disponibles, cada uno de los cuales tiene un ID único (UID, Unique IDentificador) en el buzón.

El cliente de correo compara la lista de correos recibida con la lista de correos que ya ha descargado. De esta forma obtiene los correos que aún no ha descargado, que deben ser los nuevos.

En nuestro caso, el correo de Alicia debe estar en el servidor pero no descargado en el cliente, con lo cual el cliente pedirá al servidor POP descargar el nuevo correo. Una vez completada la descarga, el correo está disponible en el cliente de correo y Roberto puede al fin leerlo.

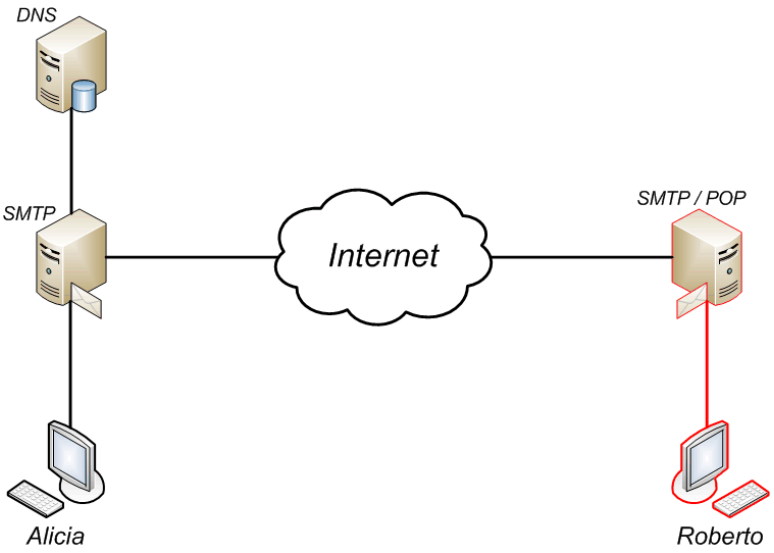

Ilustración 17: Paso 4. Descarga del email.

3.1.3 Request for comments.

Los documentos RFC más importantes para la estandarización del correo electrónico en Internet son los siguientes:

- [1977] RFC 733: "Standard for the format of ARPA network text messages", de Dave Crocker, J. Vittal, K.T. Pogran, D.A. Henderson. Queda obsoleto con el RFC 822.
- [1982] RFC 822, “Standard for the format of ARPA Internet text messages”, de Dave Crocker. Actualizado posteriormente con los RFC 1123, 1138, 1148, 1327, y 2156. Ha quedado obsoleto con la publicación del RFC 2822.

- [1994] RFC 1939, “Post Office Protocol, Version 3”, de Marshall Rose. Puedes consultar la traducción al castellano, en http://www.rfc-es.org/rfc/rfc1939-es.txt.
- [1996] RFC 2045, “Multipurpose Internet Mail Extensions”, de Ned Freed and Nathaniel Borenstein.
- [1996] RFC 2060, “Internet Message Access Protocol, Version 4 Rev 1”, de Mark Crispin.
- [2001] RFC 2821, “Simple Mail Transfer Protocol”, de AT&T Laboratories. Define el protocolo SMTP.
- [2001] RFC 2822, “Internet message format”, P. Resnick, ed., 2001. Actualiza la RFC 822.

Todos estos documentos están disponibles en el sitio web http://www.rfc-editor.org/rfc-index.html.

3.2 Sistema modular.

La arquitectura del sistema de correo propuesta se describirá como un sistema modular, en el cual una serie de componentes (módulos) interaccionan entre si. Dichos módulos tienen un rol definido y exclusivo; además son independientes tanto lógica como físicamente.

Existen un total de 5 módulos, y dependiendo de la complejidad del sistema podrán usarse desde 2 de ellos (obligatorios) hasta el total de 5. Además, la implementación interna de dichos módulos también dependerá de la complejidad del sistema, y podrá estar compuesto desde 1 hasta N nodos, entendiendo por nodo el conjunto compuesto por un servidor, sus periféricos y su correspondiente software.

3.2.1 Relay.

Se trata del módulo que se encarga de enrutar debidamente los correos electrónicos teniendo en cuenta ciertos factores.

Aunque su uso es prescindible en un sistema de correo básico, es recomendable por los siguientes aspectos:

- Proporciona un nivel superior de seguridad, debido a su posible localización en una red DMZ.
- Descarga de proceso a otros módulos del sistema, ya que actúa únicamente como despachador de correos en base a unas condiciones preestablecidas.
- Puede centralizar los procesos de análisis (antivirus y antispam), ya que todos los correos de entrada y de salida al sistema deben pasar por él. No hay que olvidar que hoy en día la mayoría del correo recibido es Spam.

Además, su uso es imprescindible en el caso de que la organización posea diferentes plataformas de correo electrónico. De esta forma todos los correos entrantes llegarían al relay y este decidiría a qué plataforma hay que encaminarlos.

Hay que tener en cuenta que la existencia de un relay puede suponer un potencial problema de seguridad, ya que si no se configura de forma correcta, podría retransmitir un correo enviado por cualquier usuario de cualquier otra red externa. Esto podría ocasionar que el relay se utilizara para enviar correo Spam por parte de terceros.

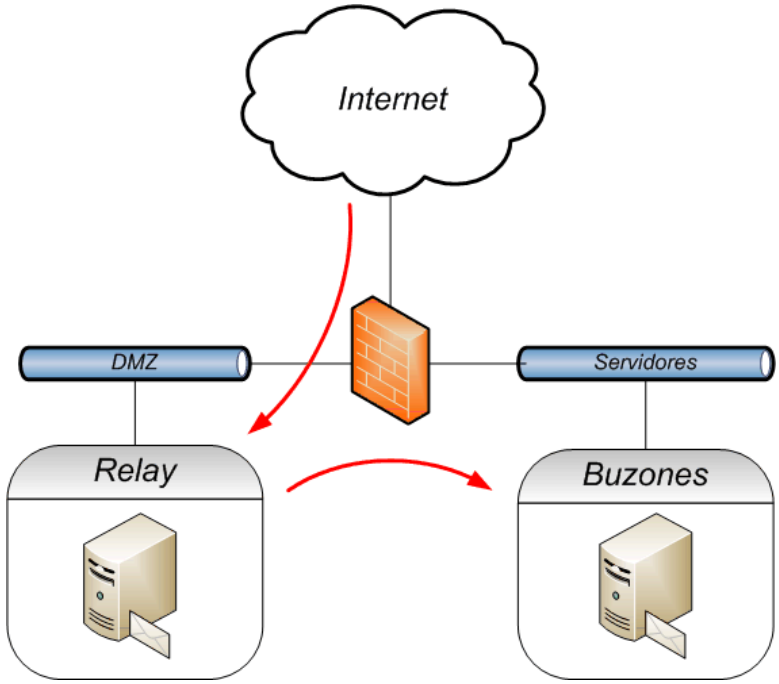

Ilustración 18: Uso del Relay.

3.2.2 Buzones.

Podemos denominarlo estafeta de correo, o simplemente buzón de correo; es el módulo que se encarga de introducir el correo electrónico en el buzón correspondiente de cada usuario del sistema. También es utilizado por el usuario para acceder a los datos de su buzón y por lo tanto, a sus mensajes de correo electrónico. Se trata de un módulo imprescindible en el sistema, que además puede incluir las siguientes funciones adicionales:

- Proporcionar servicio de almacén de datos. En el caso en el que prescindamos de módulo de almacén, el buzón adquiere esa responsabilidad utilizando discos duros locales para tal cometido.

- Proporcionar servicio de enrutamiento, en el caso de que no exista módulo de relay.

- Proporcionar servicio de análisis antivirus y antispam. Aunque este servicio está especialmente indicado para el caso en el que no exista módulo de relay, puede ser recomendable incluirlo de todas formas.

- Servicio de Webmail. Se trata de la publicación de una interfaz web para el acceso al correo electrónico por parte de los usuarios.

En el caso de utilizar el buzón como almacén de datos, hay que comentar varios aspectos:

- Una posibilidad es utilizar discos locales. En este caso es imperativa la utilización de discos en RAID, ya sea mediante software (a nivel de sistema operativo) o mediante hardware (con una tarjeta controladora dedicada). Esta práctica nos permite superar errores de disco sin pérdida de información gracias a la redundancia de datos. De todos los niveles de protección existentes, destacamos

dos: El RAID 1 (mirroring) que utiliza dos discos los cuales almacenan exactamente la misma información, y El RAID 5 que utiliza al menos tres discos, entre los cuales distribuye información de paridad para una eventual reconstrucción de los datos. El uso de RAID provoca una pérdida del espacio de almacenamiento en bruto, que podemos cifrar en 50% en el caso de RAID 1, y en 20% en el caso de RAID 5.

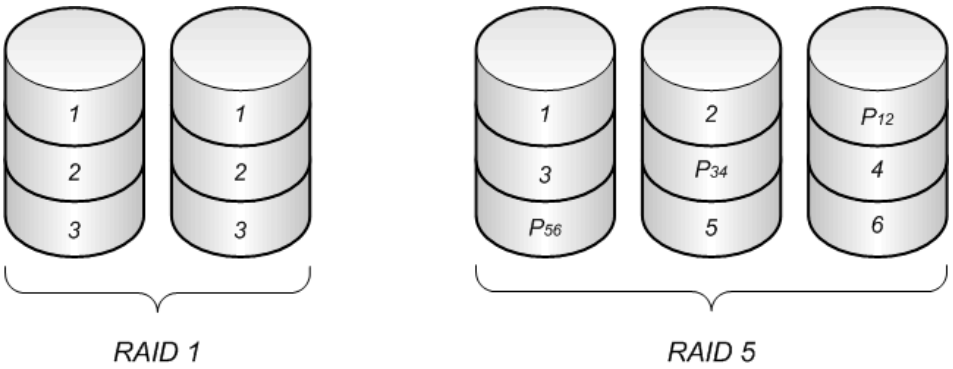

Ilustración 19: Niveles de protección RAID.

- Otra posibilidad es utilizar un dispositivo DAS (Direct Attached Storage), conectado de forma exclusiva al nodo mediante interfaz SCSI, SAS ó FC. Este dispositivo dedicado deberá proporcionar las características de rendimiento, redundancia y disponibilidad deseadas en el almacenamiento.

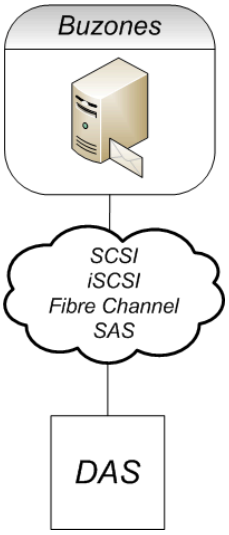

Ilustración 20: Dispositivo DAS.

- La última posibilidad es utilizar una red SAN (Storage Area Network), la cual utiliza tecnología FC ó iSCSI para interconectar de forma fiable dispositivos de almacenamiento y servidores. El concepto es similar a DAS, con el añadido de la escalabilidad y demás ventajas que caracterizan a una red de datos, en este caso dedicada exclusivamente a almacenamiento.

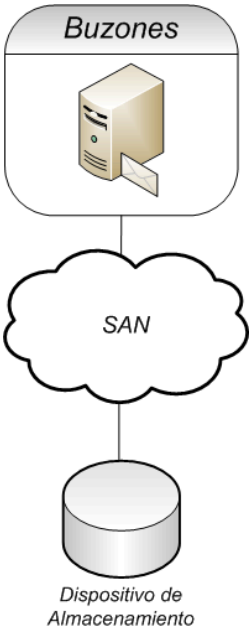

Ilustración 21: Red de Área de Almacenamiento.

- En el caso de implementar más de un nodo en el módulo buzón, todos los nodos deben tener acceso al almacén de datos en modo lectura y escritura. Por lo tanto, es necesario exportar el volumen de datos desde el nodo que haga de almacén al resto de nodos, por ejemplo mediante protocolo NFS (Network File System), lo cual constituye una arquitectura NAS (Network Attached Storage).

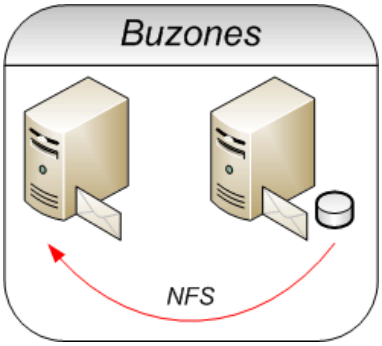

Ilustración 22: Network File System (NFS).

3.2.3 Directorio.

En este módulo reside el directorio de la organización. Se trata básicamente de una base de datos optimizada para lectura (LDAP), en la cual se dispone la información de todos los usuarios del sistema. Se trata de un módulo de implementación obligatoria.

Los atributos de cada usuario pueden ser definidos convenientemente para el sistema de correo, pero el directorio puede tener también otras funciones, como por ejemplo la autenticación de usuarios para diferentes aplicaciones corporativas (como por ejemplo un webmail).

3.2.4 Balanceador.

La existencia de este módulo va a depender de la naturaleza de los otros. Si alguno de ellos estuviera implementado físicamente por más de un nodo, es necesario realizar un balanceo de carga. De esto se encargaría el módulo balanceador. Por tanto, se trata de un componente opcional.

En teoría habría dos implementaciones posibles del balanceador: un único nodo (sin alta disponibilidad en el balanceo) o con dos nodos formando un clúster (con alta disponibilidad en el balanceo). Huelga decir que si se implemente un sistema completo con alta disponibilidad, para lo cual es necesario el balanceo, sería absurdo no incluir un cluster de dos nodos balanceadores ya que se estaría volviendo a crear un punto único de fallo precisamente en el proceso para eliminar puntos únicos de fallo en el sistema. Por lo tanto siempre se empleará un cluster de 2 nodos, exceptuando el caso en el que no se requiera alta disponibilidad y se use más de un nodo en el módulo Buzones.

3.2.5 Almacén.

Se trata del módulo que proporciona servicio de almacén de datos de forma fiable al módulo de buzón. Aunque se trata de un módulo opcional, es altamente recomendable ya que la información que almacena suele ser bastante sensible. En todos los casos es imperativa una política de copias de seguridad en medios extraíbles.

De todas maneras, hay diversas formas de implementación, que variará en función del presupuesto y de la disponibilidad deseada. Las opciones existentes son:

- RAID / NAS. Un nodo utiliza sus discos locales en RAID, y exporta los datos al buzón mediante NFS.

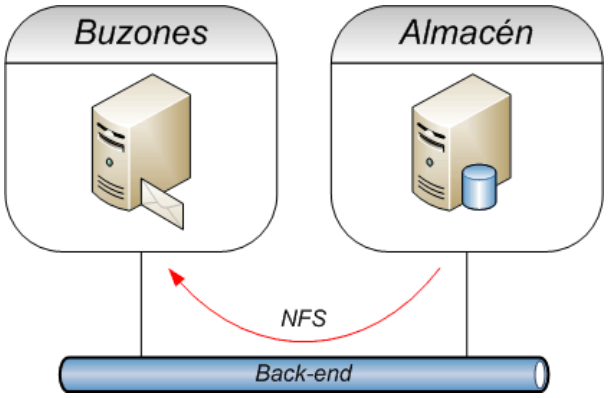

Ilustración 23: Opción RAID / NAS.

- DAS / NAS. Un dispositivo de almacenamiento es conectado punto a punto con el nodo almacén, el cual exporta los datos al buzón mediante NFS.

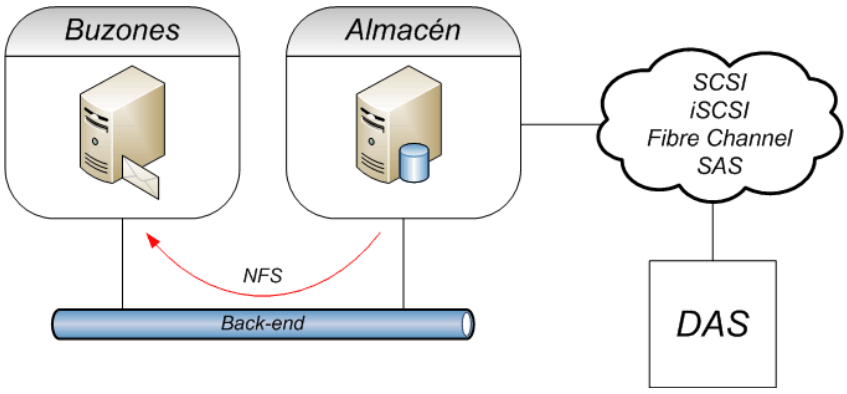

Ilustración 24: Opción DAS / NAS.

- SAN / NAS. El nodo almacén se conecta a una red SAN, obteniendo de esa forma almacenamiento remoto. El almacén exporta los datos al buzón mediante NFS.

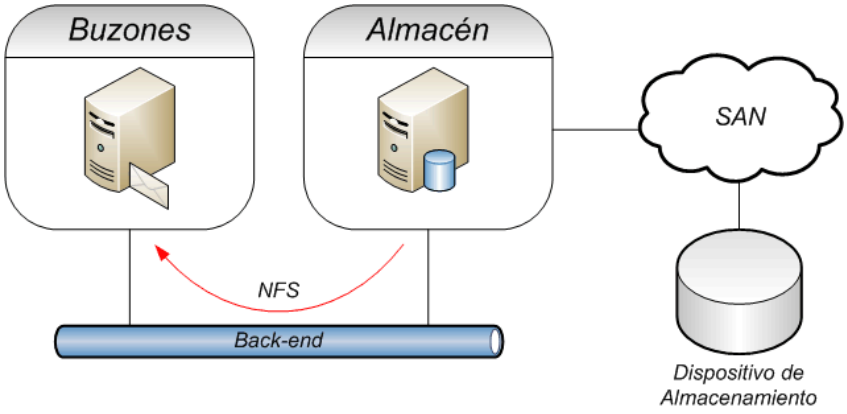

Ilustración 25: Opción SAN / NAS.

- SAN / NAS en cluster. Es la única forma de garantizar la alta disponibilidad del almacenamiento. Dos nodos forman el módulo almacén, formando un cluster que exporta mediante NFS los datos al buzón. El almacenamiento remoto está disponible para ambos nodos del almacén, y el software de cluster se encarga de gestionar el montaje desde la SAN y la exportación al buzón, lo que sólo puede hacer un nodo de almacén de forma exclusiva en el tiempo.

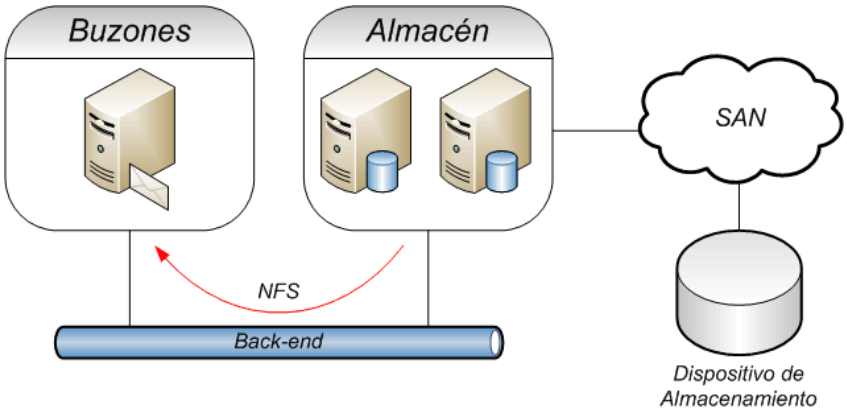

Ilustración 26: Opción SAN / NAS en clúster.

3.2.6 Utilización práctica.

En la siguiente ilustración se presentan esquemáticamente los módulos, incluyendo las redes de datos que hacen la interconexión. Se explicará con más detalle la utilización de estas redes en el apartado 3.3.1.2.

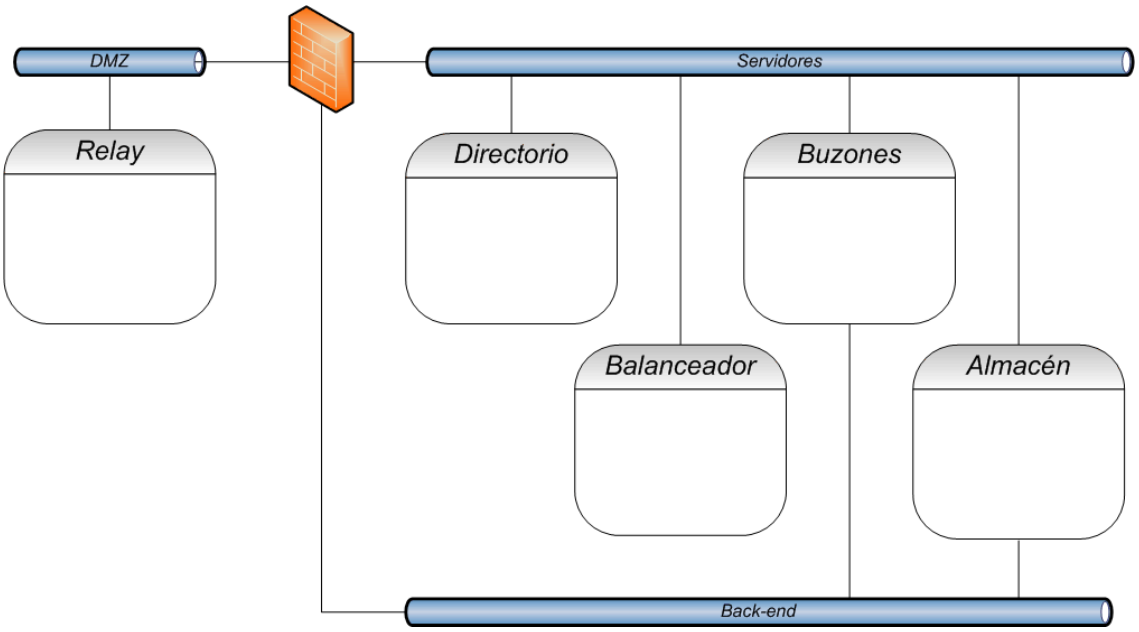

Ilustración 27: Módulos del sistema.

En la siguiente tabla se presentan los 5 módulos con el posible número de nodos que lo conforman y el carácter de obligatoriedad, tanto en formato básico como en formato de alta disponibilidad (HA, High Avalaibility, en inglés). Definimos un sistema HA como aquel en el cual no existe un punto único de fallo en cuanto a hardware se refiere. Es decir, es capaz de soportar un fallo hardware de cualquier componente del sistema:

Módulo	Nodos	Obligatorio básico	Obligatorio HA
Relay	1 ó 2	No	No
Buzones	1 a N	Sí	Sí
Almacén	1 ó 2	No	Sí
Directorio	1 ó 2	Sí	Sí
Balanceador	1 ó 2	No	Sí

Tabla 1: Módulos del sistema.

Por ejemplo, un sistema básico con pocos usuarios consistiría en 2 módulos (Buzones y Directorio) con 1 nodo cada uno, lo que hace un total de 2 nodos.

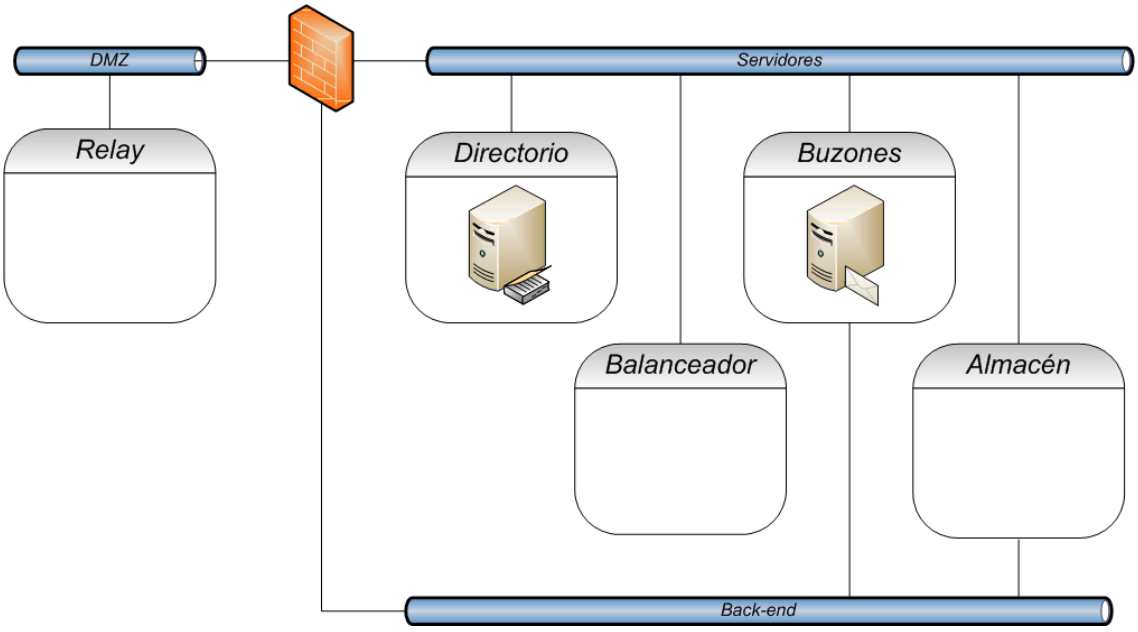

Ilustración 28: Sistema básico.

Si el número de usuarios fuera superior, habría que introducir un número mayor de nodos en el módulo Buzones, lo que además obligaría a introducir el módulo Balanceador. En ese caso serían 3 módulos con un total de 4 ó más nodos.

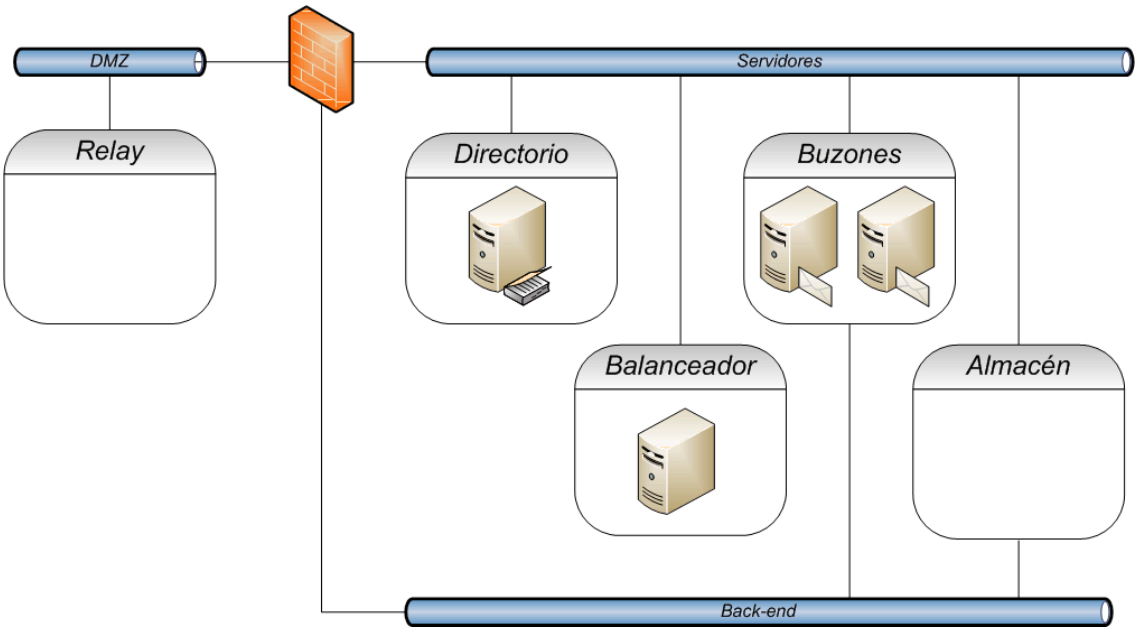

Ilustración 29: Sistema con alto número de usuarios.

Sin embargo, un sistema HA requerirá al menos 4 módulos, y en un número mínimo de 2 nodos por módulo, lo que haría un total de 8 ó más nodos.

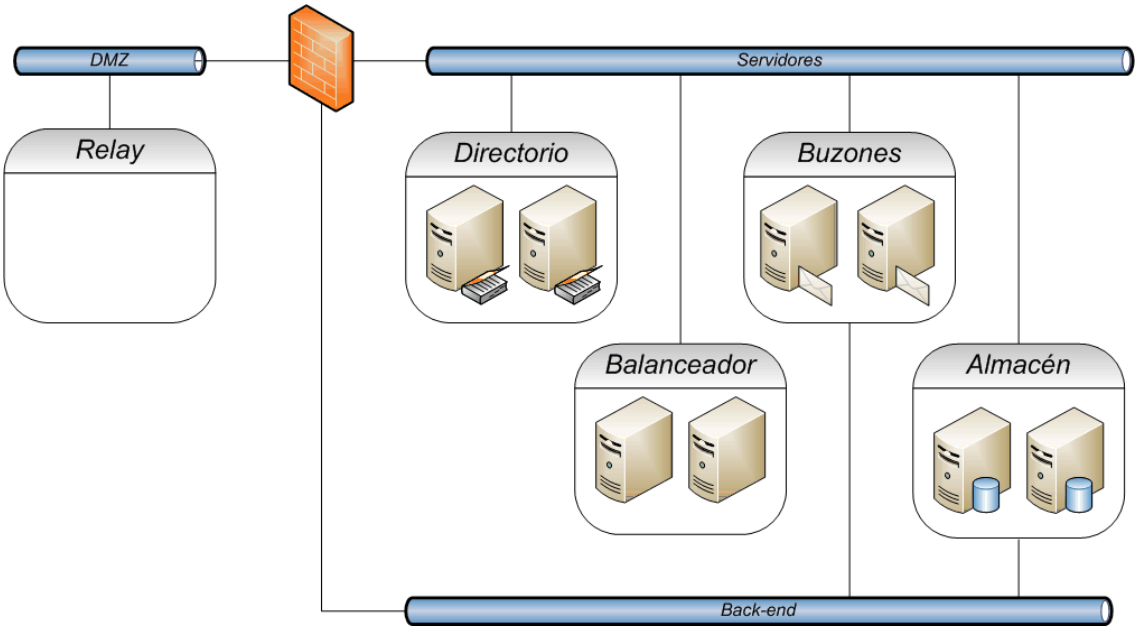

Ilustración 30: Sistema con alta disponibilidad.

3.3 Infraestructura necesaria.

En los siguientes apartados se van a exponer los requisitos tanto de hardware como de software que serían óptimos para la implementación del sistema de correo electrónico. Además, se van a exponer la justificación de la elección del software entre las diferentes opciones que existen.

3.3.1 Hardware.

Entendiendo por hardware todas las partes físicas y tangibles de un sistema informático, hemos dividido éste en dos grupos diferenciados:

- Sistema informático de proceso de datos: Servidores.
- Sistema de interconexión de datos y almacenamiento: Redes de datos.

3.3.1.1 Servidores.

La informática de hoy en día sigue mayoritariamente la arquitectura cliente/servidor, en la cual el usuario final utiliza el componente 'cliente', quien hace peticiones que procesa y resuelve el componente 'servidor'. Por lo tanto, el servidor es el componente que debe aglutinar una mayor capacidad de proceso para dar repuestas al cliente.

En la actualidad nos encontramos con 3 tipos de máquinas informáticas, que aunque pueden parecer similares (y lo son en arquitectura), tienen unas características determinadas en función del uso al que están destinadas. Son:

- Ordenadores personales (PCs).
- Estaciones de trabajo (workstations).
- Servidores.

Es obvio que para nuestro sistema de correo electrónico necesitaremos servidores, cumpliendo los requisitos en los siguientes aspectos, que son los que los diferencian de los 'PCs' y las 'workstations':

1. Microprocesadores. En arquitecturas x86 y su extensión x64, la gama de servidores la cubren los chips Intel Xeon y AMD Opteron, que llegan a integrar hasta 6 cores en cada pastilla. Para workstations y pcs, existen otros modelos menos potentes como Intel Core2 ó AMD Athlon. Cabe destacar que en servidores también se trabaja con la arquitectura IA64, con procesadores Intel Itanium, destinada fundamentalmente a sistemas UNIX.
2. Memorias. Se utiliza indiscriminadamente la memoria de tipo SDRAM DDR, con la salvedad de que en servidores se añade la tecnología ECC (Error Correcting Code) que proporciona corrección de errores por hardware.
3. Discos. Tradicionalmente la tecnología SCSI reinaba en los servidores, siendo esta hoy desplazada poco a poco por SAS, en ambos casos usando controladoras RAID para redundancia de datos. En workstations se suele implementar RAID y en algún caso se utiliza SCSI (SAS). Sin embargo en pcs siempre se utiliza SATA debido fundamentalmente a su bajo coste.
4. Controladora gráfica y de sonido. Mientras en servidores la importancia de estas controladoras es escasa, y se suelen integrar en placa, en Workstations puede llegar a ser el componente fundamental de la máquina dependiendo de la labor a la que está destinada, por lo que suelen ser dispositivos dedicados conectados en buses PCI, SCSI ó Firewire. En pcs, además de ser integrados, suelen utilizar memoria principal para su uso.
5. Fuentes de alimentación. Mientras en workstations y pcs no es excesivamente importancia que la máquina esté siempre encendida, en los servidores suele ser todo lo contrario, por lo que se emplean fuentes de alimentación redundantes para que el fallo en una de ellas no implique un apagado de la máquina.
6. Disponibilidad. Se define como el tiempo total de funcionamiento ordinario del sistema respecto al tiempo total transcurrido. Todos y cada uno de los componentes del servidor influirán en la disponibilidad final conseguida, que sea cual sea su aplicación debería ser de al menos 99.99%. En la siguiente tabla se ven los valores de disponibilidad más comunes con los tiempos de no disponibilidad correspondientes.

Disponibilidad	Tiempo no disponible por año.	Tiempo no disponible por mes.	Tiempo no disponible por semana.
90%	36.5 días	72 horas	16.8 horas
95%	18.25 días	36 horas	8.4 horas
99%	3.65 días	7.20 horas	1.68 horas
99.9%	8.76 horas	43.2 minutos	10.1 minutos
99.99%	52.6 minutos	4.32 minutos	1.01 minutos
99.999%	5.26 minutos	25.9 segundos	6.05 segundos
99.9999%	31.5 segundos	2.59 segundos	0.605 segundos

Tabla 2: Disponibilidad de un sistema.

7. Medio ambiente. Normalmente para Workstations y pcs no se tenga en cuenta el entorno de trabajo, pero para servidores es algo fundamental. La obra civil del CPD, la colocación de los armarios racks, la ventilación, la temperatura o el consumo eléctrico son conceptos muy a tener en cuenta a la hora de poner en servicio servidores. Por eso mismo, el precio del servidor puede suponer sólo un 20% del TCO (Total Cost of Ownership) del mismo, que incluye la adecuación de su entorno, su consumo y su administración.

En la siguiente tabla veremos a modo de repaso y de forma esquemática, las diferencias entre servidores y el resto de máquinas teniendo en cuenta los aspectos señalados:

	Servidores	Workstations	PCs
Microprocesadores	Intel Xeon Intel Itanium AMD Opteron	Intel Core2 AMD Opteron AMD Phenom	Intel Core2 Intel Celeron Intel Atom AMD Athlon AMD Sempron AMD Turion
Memorias	DDR ECC	DDR	DDR
Discos	SCSI RAID SAS RAID	SATA RAID SCSI RAID	SATA
Gráficos y sonido	Integrados, dedicada.	PCI, SCSI, Firewire.	Integrados, compartida.
Alimentación	Redundante	Redundante / Simple	Simple
Disponibilidad	99.99%	N/A	N/A
Medio	CPD Armario rack Ventilación Control temperatura	Oficina / Casa	Oficina / Casa

Tabla 3: Diferencias entre servidores / workstations / PCs.

3.3.1.2 Redes de datos.

Un aspecto fundamental para la arquitectura propuesta es la interconexión de todos los elementos que la componen, de lo que se encargarán las redes de datos. Se van a utilizar dos tipos de redes:

- Red LAN (Local Area Network, Red de Área Local).
- Red SAN (Storage Area Network, Red de Área de Almacenamiento).

3.3.1.2.1 LAN.

LAN usa TCP/IP y Ethernet para la interconexión de dispositivos informáticos, con el fin de compartir recursos e intercambiar datos y aplicaciones.

La implementación de LAN más común es una Ethernet 100Mbps ó 1Gbps. Siempre se recomendará la opción de 1Gbps, contando además con mecanismos de redundancia tanto a nivel de electrónica de red (switches) cómo de tarjetas de red en los servidores (teaming, bonding).

Se entiende como óptima la utilización de 3 redes LAN para el sistema de correo:

1. DMZ. (DeMilitarized Zone, zona desmilitarizada). Se trata de una red que se sitúa lógicamente entre la red externa y las redes internas, de forma que el acceso desde ambas redes a la DMZ esté permitido, pero el acceso desde la DMZ a las redes internas no, y a la externa sí. De esta forma, los equipos de la DMZ pueden dar servicio al exterior (por ejemplo servidores web, de correo, etc.) pero no comprometen la seguridad de los equipos de las redes internas. Todo esto se implementa en las políticas del cortafuegos.

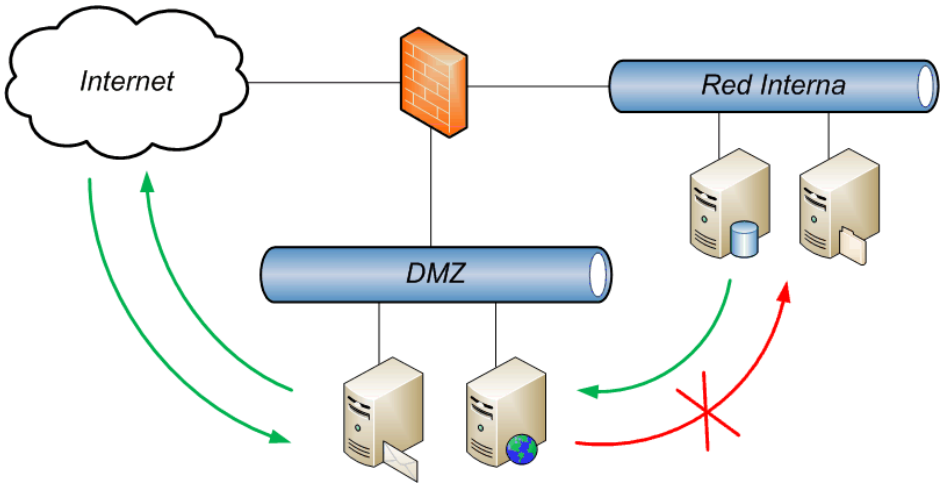

Ilustración 31: Zona Desmilitarizada.

2. Servidores. Es la red en la que trabajan la mayoría de los servidores, concretamente los que no dan servicio directo al exterior. A priori es la red con más carga de trabajo.

3. Back-End. Se trata de una red interna implementada con el propósito de transmitir datos de almacenamiento. Se puede optar a crear este tipo de redes para una mejor optimización del ancho de banda de la red de propósito general de servidores.

3.3.1.2.2 SAN.

Las redes de almacenamiento SAN interconectan de manera rápida, segura y fiable servidores, cabinas de disco y librerías de cintas.

En nuestro caso, el uso de una red SAN quedará reservado únicamente en el caso de que se utilicen cabinas de disco para ofrecer almacenamiento remoto a los servidores.

Las redes SAN usan mayoritariamente tecnología Fibre Channel a 1, 2, 4 ó 8 Gbps, siendo recomendable la velocidad de 4Gbps al menos. También se deben contar con mecanismos de redundancia en electrónica de red y en las tarjetas HBA (Host Bus Adapter) de los servidores.

3.3.2 Software.

La utilización del software ha sido determinada principalmente por el objetivo del proyecto. Aún así, en algunos casos se han presentado ciertas alternativas en la elección del mismo, las cuales vamos a tratar de justificar en este apartado.

- Sistema operativo: debian.
- Servidor SMTP: exim.
- Servidor POP/IMAP: courier.
- Antivirus: clamav.
- Antispam: spamassassin.
- Directorio LDAP: openldap.

- Webmail: squirrelmail.
- Cluster: Linux-HA: heartbeat.
- Balanceo de carga: LVS.

3.3.2.1 Debian.

Dejando a un lado magníficas distribuciones de pago como Red Hat o SuSE, las opciones entre las cuales elegir eran básicamente: debian, Fedora, o ubuntu, por ser las más extendidas.

Debian puede considerarse como el padre de todas las distribuciones de GNU/Linux, y las primeras razones de la elección de debian son históricas y sociales: la comunidad debian, el manifiesto histórico y el modelo colaborativo.

La estabilidad de debian es otra razón fundamental, así como la cantidad de software disponible en sus repositorios y su correspondiente facilidad de instalación y gestión de paquetes.

Por si fuera poco, debian es masivamente utilizado en las principales universidades de todo el planeta, y en ella se basan multitud de distribuciones de gran éxito.

3.3.2.2 Exim.

La elección de exim es una consecuencia directa de debian. Se trata del servidor de correo que se incluye en la instalación básica, y por lo tanto el más integrado con la distribución GNU/Linux elegida. Otras opciones hubieran sido sendmail, qmail o postfix, pero usando debian, creemos que lo más acertado es seguir con exim.

Además, determinadas características de exim como su simplicidad en la configuración y su flexibilidad, confirmaron su elección.

3.3.2.3 Courier.

Partiendo de la base de querer trabajar con formato maildir como modelo de organización de las cuentas de correo, la elección de Courier es imperativa. Hay otras opciones como Binc o Dovecot pero se descartaron por su poca utilización frente a Courier.

Maildir es un formato de almacenaje de correo que no bloquea los ficheros para mantener la integridad de los mismos. Se organiza en directorios de usuarios y los correos electrónicos son ficheros independientes. Esto provoca que este sistema sea más fácil de administrar, y sobre todo más rápido que otros ampliamente usados como mailbox.

3.3.2.4 ClamAV y Spamassassin.

ClamAV es el único software antivirus de licencia GPL diseñado especialmente para correo electrónico. Su comunidad de desarrolladores y las continuas actualizaciones hacen de él la mejor elección para una herramienta de este tipo.

Spamassassin, con varios premios en diversas conferencias de software libre, es la herramienta anti-spam más usada en entornos linux. Utiliza distintas ténicas (DNS inverso, listas negras, análisis bayesiano,...) que la convierten en una de las soluciones más robustas existentes en la actualidad, independientemente de la plataforma.

3.3.2.5 Openldap.

La elección de openldap como implementación del directorio LDAP fue relativamente fácil, pues se trata de la única herramienta libre de este tipo con cierto tipo de permanencia en la comunidad. Últimamente han surgido otros proyectos, pero no pensamos que sean suficientemente maduros como para plantearse usarlos en aplicaciones de este tipo.

3.3.2.6 Squirrelmail.

La oferta de herramientas webmail libres es bastante amplia, con ejemplos como Horde, Zimbra, RoundCube, squirrelmail,…
La elección de squirrelmail viene dada por los siguientes aspectos:

- Robustez, proyecto iniciado en 1999.
- Personalización al máximo.
- Visión clara y directa de carpetas y correos.
- Rapidez.
- Multitud de plugins para añadir funcionalidades.

3.3.2.7 Linux-HA: heartbeat y LVS.

El software de cluster de alta disponibilidad utilizado será heartbeat, integrado en Linux-HA, un proyecto de software libre con casi 10 años de experiencia, y con un alto grado de usabilidad entre la comunidad del software libre. Heartbeat proporciona fiabilidad y disponibilidad compitiendo con soluciones propietarias y siendo implantado en aplicaciones críticas alrededor del mundo, estimándose en 30000 el número de clústeres en producción actualmente.

LVS (Linux Virtual Server) es una herramienta completamente integrable dentro de Linux-HA, que proporciona balanceo de carga a través de una arquitectura transparente.