ANUBIS- SUITE DE APLICACIONES DESTINADAS A LA ADMINISTRACION DE SERVICIOS DE REDES DE AREA LOCAL TIPO IP BAJO PLATAFORMA GNU/LINUX

JAVIER FERNANDO ARELLANO RUIZ
DICK ALEXANDER CUASQUER VIVEROS

UNIVERSIDAD DE NARIÑO
FACULTAD DE INGENIERÍA
PROGRAMA DE INGENIERÍA DE SISTEMAS
SAN JUAN DE PASTO
2007

ANUBIS- SUITE DE APLICACIONES DESTINADAS A LA ADMINISTRACION DE SERVICIOS DE REDES DE AREA LOCAL TIPO IP BAJO PLATAFORMA GNU/LINUX

JAVIER FERNANDO ARELLANO RUIZ
DICK ALEXANDER CUASQUER VIVEROS

Trabajo de Grado presentado como requisito
Para optar al título de Ingenieros de Sistemas

JUAN CARLOS CASTILLO ERASO
Ing. Esp.
Asesor

UNIVERSIDAD DE NARIÑO
FACULTAD DE INGENIERÍA
PROGRAMA DE INGENIERÍA DE SISTEMAS
SAN JUAN DE PASTO
2007

Nota de aceptación

_____
_____
_____
_____
_____
_____

_____
Firma del presidente del jurado

_____
Firma del jurado

_____
Firma del jurado

_____
Firma del asesor del proyecto

San Juan de Pasto, 12 de Marzo de 2007

RESUMEN

La suite de aplicaciones destinadas a la administración de servicios de redes de área local tipo IP bajo plataforma GNU/LINUX, nace de la necesidad de tener un mejor y optimo control de los recursos tecnológicos como lo son hoy por hoy las redes de datos de área local, la distribución y organización de la información, y todos los servicios que sobre este tipo de redes se puede brindar, en donde los mas usados son: Servicio de correo electrónico, servicio de publicaciones web, servicio proxy http, filtro web, y por supuesto el cortafuegos.

Así mismo en el trabajo se destaca la importancia de la utilización de software libre cubierto por la licencia publica general ò GPL y por la obra maestra que esta licencia cubre; el sistema operativo GNU/LINUX, con lo cual se pretende dar una solución a una necesidad gigantesca en todo tipo de empresas tanto en nuestra región como en nuestro país dado a que software de este tipo en el mercado actual bajo plataformas propietarias son extremadamente costosos, donde no todo el mundo puede tener acceso.

Este proyecto será implementado en la Universidad de Nariño con lo cual hará mas ágil y eficiente el control de usuarios a la red de la institución, brindar con mayor facilidad servicios de correo electrónico, internet, publicaciones Web, y otros servicios que aunque el usuario final no los podrá observar, será beneficiado de forma transparente como lo son los servicios de Firewall, y Filtro Web.

En el desarrollo del proyecto se utilizó la metodología Proceso Unificado de rational (RUP), haciendo uso del Modelo Orientado a Objetos con la notación de UML por sus ventajas sobre el Modelo Estructurado. El diseño orientado a objetos es más cercano a la realidad, el desarrollo realizado es más fácil de mantener y de reutilizar, además evita la redundancia en los procesos, luego los códigos son más entendibles y resumidos.

ABSTRACT

The suite of applications guided to the administration of local area network services class IP under a GNU/LINUX architecture, is born of the need to have a better an optimal control of technological resources like local area data networks are nowadays, distribution and organization of the information and all the services which can be offered by this mean, where the most used are: mail service and e-mails, web hosting service, proxy http service, web filter and off course, firewall.

In the same way, it is remarkable the importance of making use of free software covered by the general public license or GPL and by the masterwork this license covers; the operative system GNU/LINUX, so that it is pretended to give a solution to a huge need in all kind of enterprises not only in our region but in our country because these kind of software in the current market under copyright architectures are extremely expensive, where not everybody can access.

The present project will be implemented in Nariño's University, with the one net users control of the institution will be fast and efficient, it will be possible to provide mail service and e-mails, internet, web hosting service, and other services in an easier way, even when the final user won't see them, he will profit from it in a transparent way like Firewall and Web filter services are.

In the development of this project was used a methodology called Rational Unified Process (RUP), making use of Objects Oriented Model with the UML notation due to its advantages over the Structured Model. The design oriented toward objects is nearer to the reality, the development carried out is easier to maintain and to reuse.

CONTENIDO

Pág.

LISTA DE ESQUEMAS

LISTA DE FIGURAS

LISTA DE TABLAS

LISTA DE ANEXOS

INTRODUCCION

La Universidad de Nariño debe contar con procesos eficaces, dinámicos y seguros en todas las áreas, el área de administración de servicios de red es de vital importancia dentro de la organización necesitando así un sistema de administración competente, integral, seguro y capaz de llevar a cabo las actividades que conducen al óptimo aprovechamiento de una red de datos.

En este trabajo de grado se desarrollará lo que corresponde al análisis, diseño, e implementación de una suite de aplicaciones destinadas a la administración de servicios de red, correspondiente a correo electrónico, publicaciones Web, administración de nodos de red, control de un filtro Web, administración de un firewall o muro corta fuegos, y control de ancho de banda; aplicando el Lenguaje Unificado de Modelado (UML) y la metodología Proceso Unificado de Rational (RUP), junto con las robustas herramientas que solo un sistema GNU/LINUX basado en UNIX puede brindar.

1. DESCRIPCIÓN DEL PROBLEMA

1.1 PLANTEAMIENTO DEL PROBLEMA

La carencia de un sistema de Administración y control modular de servicios de red, impide la óptima administración de la misma, evitando brindar y utilizar al máximo los recursos que una red de datos ofrece.

Uno de los principales inconvenientes de la implementación de este tipo de sistemas, sobre plataformas propietarias, es su excesivo costo teniendo además opciones limitadas a las que el proveedor del software ofrece.

Por el contrario, sobre plataformas libres como en el caso de GNU/Linux, se encuentran robustas herramientas, que ofrecen soluciones propias a problemas específicos teniendo así que manipular varias aplicaciones o archivos del sistema de forma separada como son (APACHE, DHCP Server, SQUID, IPTABLES, entre otros). Cabe destacar que cada aplicación posee sus propios archivos de configuración, su propia forma de instalación, y su propia forma de inicialización y mantenimiento.

1.2 FORMULACIÓN DEL PROBLEMA

¿De que manera se puede optimizar todos los procesos de administración de servicios de una red de área local, utilizando herramientas de software libre de forma que se obtenga el mayor beneficio posible de dichos servicios y de la red de datos misma?

1.3 SISTEMATIZACIÓN DEL PROBLEMA

- ¿Cómo se pueden unificar los diferentes medios de administración de redes que ofrecen los sistemas UNIX?

- ¿Cómo se puede tener un control sobre un sistema de correo electrónico basado en el protocolo IMAP?

- ¿Cómo se puede conseguir un fácil acceso a una publicación Web por parte de determinados usuarios?

- ¿Cómo se puede tener un completo control de los nodos conectados a una red de datos, y de las personas o usuarios que los usan?

- ¿Cómo se puede dar a los usuarios una calidad de servicio teniendo en cuenta una estratificación de usuarios?

- ¿Cómo se puede tener un óptimo control de un servidor Proxy sobre SQUID, de manera que se pueda tener un rápido mantenimiento y fácil acceso a las diferentes funcionalidades que este provee?

- ¿Cómo se puede administrar de manera sencilla y rápida un muro corta fuegos o Firewall utilizando el kernel del sistema operativo GNU/LINUX?

- ¿Cómo puede controlar el acceso a las distintas páginas de Internet, teniendo en cuenta su contenido (sexual o violento) a través de la URLS, dominios, y palabras específicas?

1.4 ALCANCE

El proyecto se refiere al análisis, diseño, codificación e implementación del Sistema Integrado o suite de aplicaciones destinadas a la administración de servicios de redes de área local tipo IP, bajo la metodología RUP (Rational Unified Process) y el modelamiento Orientado a Objetos.

El análisis de requerimientos considera las etapas de presentación general del sistema, identificación de usuarios y metas, casos de uso, diagramación de casos de uso, y modelo conceptual.

El diseño comprenderá las etapas de elaboración diagramas de secuencia del sistema, diagramas de clases, diagramación de paquetes y realización del diseño de base de datos empleando el modelo entidad - relación.

Para llevar a buen término cada una de las actividades, el sistema se subdividirá en módulos, así:

- Administración de publicaciones WEB
- Administración y control de usuarios de correo electrónico.
- Administración y control de nodos conectados a la red.
- Administración de servidor Proxy.
- Administración de filtro Web.
- Administración y control de ancho de banda.
- Administración y control de un muro corta fuegos (Firewall).

La codificación del sistema será divida en varios lenguajes de programación dependiendo de la necesitad el sistema, es decir, si el sistema necesita de alguna forma realizar procesos o modificar archivos que necesiten privilegios de root o de súper usuario, se utilizara PERL, C++, y manejo de Shell para dicho fin, o bien se utilizará PHP como lenguaje de programación orientado a objetos desde su versión 5, HTML para la interfaz de usuario, y JavaScript para la validación de formularios.

1.5 JUSTIFICACION

Debido a la importancia y gran cantidad de información que se maneja en cualquier mediana o gran empresa, no solo en los procesos administrativos, sino también en los procesos financieros, contables, y operativos, se considera la necesidad de implementar un sistema de administración y control que permita gestionar e integrar de manera confiable, dinámica y segura los servicios que brinda una red de datos, además de disminuir el tiempo de ejecución de cada proceso.

Este sistema de administración de servicios de red ha de permitir gestionar grandes redes de computadores con múltiples propósitos y sistemas operativos de forma racional y sostenible, haciendo que el coste de mantenimiento disminuya con el número de computadores gestionados en lugar de crecer, tal y como viene siendo habitual con los sistemas de administración actuales.

Hoy en día, se pueden brindar muchos servicios a través de una red de datos, en especial cuando esta es Ethernet y utiliza IP como protocolo de red, entre estos servicios encontramos: Videoconferencias, correo electrónico, servidor de transferencia de archivos FTP, servicio de publicación Web, Messenger corporativo, e inclusive la reciente tecnología de voz sobre IP ó VoIP, entre otros.

Tener un rápido control de estos servicios facilitaría la completa administración de la red corporativa, y a la vez reduciría sustancialmente costos de mantenimiento de equipos clientes, y costos de acceso a Internet con el proveedor de servicio, ya que distribuiría un recurso de mejor forma, para todos los usuarios de la red, de allí su justificación.

2. OBJETIVOS

2.1 OBJETIVO GENERAL

Crear un sistema modular, totalmente integrado y seguro, que permita el control y administración de los servicios de red mas importantes a nivel de redes LAN.

2.2 OBJETIVOS ESPECÍFICOS

- Unificar medios de administración de Redes ofrecidos por los entorno UNIX.
- Obtener un sistema de Control y Administración de Servicios como el correo electrónico.
- Dar acceso de manera sencilla a las publicaciones Web, a los usuarios que lo requieran.
- Controlar de manera dinámica vía Web los diferentes nodos y usuarios registrados dentro de la red que se desee administrar.
- Brindar Calidad de Servicio a los usuarios en función de sus diferentes divisiones.
- Crear un sistema basado en Web, para la administración y mantenimiento de un servidor PROXY Squid.
- Establecer un sistema unificado, de sencillo manejo para la creación de reglas para la administración de un Firewall basado en los nuevos kernel del Sistema Operativo GNU/Linux.
- Controlar el acceso a páginas Web por parte de los usuarios de la red en función de su contenido categorizado.

3. MARCO TEORICO

3.1 UTILIDADES DE ADMINISTRACION DE RED DE GNU/LINUX

3.1.1 DHCP

3.1.1.1 Dynamic Host Configuration Protocol (DHCP) es un estándar IP para simplificar la administración de la configuración del IP del cliente. El estándar DHCP permite que se utilice los servidores de DHCP para manejar la asignación dinámica de las direcciones y la configuración de otros parámetros IP para clientes DHCP en la red.

3.1.1.2 ¿Por qué utilizar DHCP? En redes TCP/IP, DHCP reduce la complejidad y el trabajo administrativo de re-configurar las equipos de computo del cliente. Para entender por qué DHCP es útil para configurar clientes TCP/IP, es importante comparar la configuración manual de TCP/IP con la configuración automática que utiliza DHCP.

3.1.1.3 Configuración manual de TCP/IP Cuando se realiza la configuración IP para cada cliente, ingresando manualmente información como la dirección IP , máscara de subred o la puerta de enlace por defecto , pueden llegar a producirse errores de tipeo (errores humanos), que es probable deriven en problemas de comunicación o problemas asociados a la IP duplicada. Por otra parte, hay carga administrativa adicional en las redes donde las computadoras se mueven con frecuencia de una subred a otra y, en adición, cuando necesita cambiar un valor IP para varios clientes, tiene que actualizar la configuración IP de cada cliente.

3.1.1.4 Configuración automática TCP/IP Cuando se configura un servidor DHCP para dar soporte a clientes DHCP, éste provee automáticamente la información de la configuración a clientes DHCP y también se asegura que los clientes de la red utilicen la configuración correcta. Además, si se necesita realizar un cambio en la configuración IP de varios clientes, se podrá realizarlo una vez en el servidor DHCP, para que el DCHP actualice automáticamente la configuración del cliente reflejando el cambio.

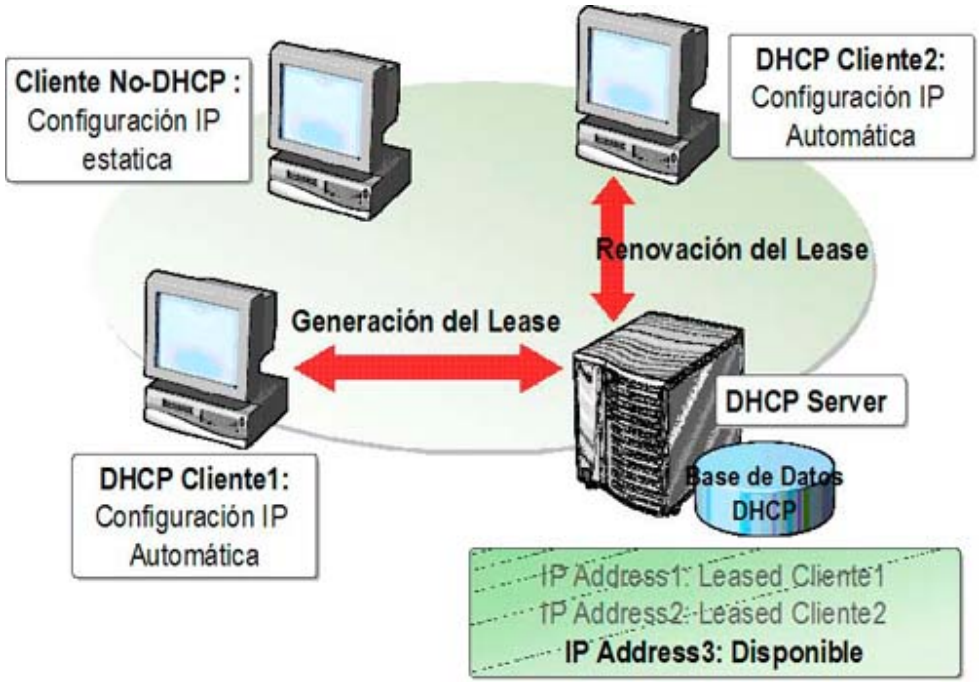


Figura. 1. ¿Cómo el DHCP asigna direcciones IP?

El **lease** es el espacio de tiempo en el cual un cliente DHCP puede utilizar una configuración dinámicamente asignada de IP. Antes de la expiración del tiempo de lease, el cliente debe renovarlo u obtener un nuevo lease del DHCP tal y como lo muestra la Figura 1.

3.1.1.5 DHCPD. El ***Dynamic Host Configuration Protocol Daemon*** es el corazón de todo sistema DHCP. Éste se encarga de "alquilar" direcciones y de vigilar su uso como está estipulado en el archivo de configuración /etc/dhcpd.conf. El administrador del sistema puede determinar el comportamiento del DHCP según sus preferencias mediante los parámetros y valores definidos en este archivo.

Un ejemplo para un archivo /etc/dhcpd.conf sencillo seria:

```
default-lease-time 600;          # 10 minutos
max-lease-time 7200;             # 2  horas
```

```
option domain-name "intranet.udenar.edu.co";
option domain-name-servers 192.168.1.1, 192.168.1.2;
option broadcast-address 192.168.1.255;
option routers 192.168.1.254;
option subnet-mask 255.255.255.0;

subnet 192.168.1.0 netmask 255.255.255.0
 {
  range 192.168.1.10 192.168.1.20;
  range 192.168.1.100 192.168.1.200;
 }
```

Como se puede observar, el anterior ejemplo puede dividirse en tres bloques. En la primera parte se define de forma estándar cuántos segundos se "alquilará" una dirección IP a un ordenador que lo solicite antes de que éste tenga que pedir una prórroga (default-lease-time). Aquí también se define el tiempo máximo durante el cual un ordenador puede conservar un número IP otorgado por el servidor DHCP sin tener que tramitar para ello una prórroga (max-lease-time).

En el segundo bloque se definen globalmente algunos parámetros de red básicos:

- Con ***option domain-nam***e se define el dominio por defecto de su red.
- En ***option domain-name***-servers se pueden introducir hasta tres servidores DNS que se encargarán de resolver direcciones IP en nombres de host (y viceversa).
- ***option broadcast-address*** define qué dirección broadcast debe usar el ordenador que efectúa la consulta.
- ***option routers*** define dónde deben ser enviados los paquetes de datos que no pueden ser entregados en la red local (a causa de la dirección del host de origen y el host de destino así como de la máscara de subred). Este enrutador suele actuar como la pasarela a Internet en pequeñas redes.
- ***option subnet-mask*** proporciona al cliente la máscara de red a entregar.

Por debajo de esta configuración general se define una red con su máscara de subred.

Por último, basta con seleccionar el rango de direcciones utilizado por el demonio DHCP para asignar direcciones IP a clientes que lo consulten. Para el ejemplo dado, son todas las direcciones entre 192.168.1.10 y 192.168.1.20 y también en el rango de 192.168.1.100 hasta 192.168.1.200.

El DHCPD consiste en 2 programas principales:

- dhcpd – el proceso ó demonio del servicio DHCP de GNU/Linux.

- dhcrelay – un transmisor DHCP (para transmitir peticiones a un servidor DHCP central, puesto que el DHCP está basado en broadcasts, las cuales por lo general no se extienden (o no deberían) a routers.

DHCPD requiere 2 librerías:
- /lib/ld-linux.so.2
- /lib/libc.so.6

Un fichero de configuración:

- /etc/dhcpd.conf – información de configuración, situación de los ficheros de arranque, etc. (Ver ejemplo anterior).

3.1.2 Servidor proxy caché squid.

3.1.2.1 Servidores Proxy Un Servidor Proxy permite a otros equipos conectarse a una red de forma indirecta a través de él. Cuando un equipo de la red desea acceder a una información o recurso, es realmente el Proxy quien realiza la comunicación y a continuación traslada el resultado al equipo inicial. En unos casos esto se hace así porque no es posible la comunicación directa y en otros casos porque el Proxy añade una funcionalidad adicional, como puede ser la de mantener los resultados obtenidos (ejemplo: una página Web) en un Caché que permita acelerar sucesivas consultas coincidentes.

El funcionamiento es de la siguiente forma:

1. El cliente realiza una petición (por ejemplo. mediante un navegador Web) de un recurso de Internet (una página Web o cualquier otro archivo) especificado por una URL.
2. Cuando el Proxy caché recibe la petición, busca la URL resultante en su caché local. Si la encuentra, devuelve el documento inmediatamente, si no es así, lo captura del servidor remoto, lo devuelve al que lo pidió y guarda una copia en su caché para futuras peticiones.
3. El caché utiliza normalmente un algoritmo para determinar cuándo un documento está obsoleto y debe ser eliminado de la caché, dependiendo de su antigüedad, tamaño e histórico de acceso. Dos de esos algoritmos básicos son el LRU (el usado menos recientemente, en inglés "Least Recently Used") y el LFU (el usado menos frecuentemente, "Least Frequently Used").

Squid es un programa que hace caché de datos obtenidos en Internet. Realiza este trabajo aceptando peticiones de los objetos que los usuarios quieren descargar y realizando estas

peticiones a la red en su nombre. Squid se conecta con el servidor correspondiente, pide el objeto.

El servidor ***Proxy Squid Caché,*** almacena en el disco duro del servidor las páginas más visitadas desde la estaciones de tal manera que se realiza un ahorro significativo del ancho de banda del enlace del centro de acceso cuando se solicita la página nuevamente desde la misma u otra estación. Squid verifica si la página ha cambiado, y de ser así, vuelve a almacenarla localmente. Es posible configurar Squid para definir cuanto tiempo pueden estar almacenadas las páginas en el servidor.

El fichero de configuración de SQUID se halla generalmente en `/etc/squid/squid.conf` o en la ruta que se haya escrito en la instalación. Se deberá editar este archivo para realizar los cambios adecuados y conseguir que cumpla su tarea con cierta seguridad para el sistema a implementar.

Este fichero de configuración consta de multitud de parámetros configurables que ajustan el servidor a cualquier necesidad. Aquí se trata de reflejar aquellos indispensables para un óptimo funcionamiento.

3.1.2.2 Puerto para SQUID Por defecto, SQUID utilizará el puerto 3128, y la sentencia en el archivo es: **http_`port 3128`.**

3.1.2.3 Tamaño de caché En esta instrucción se fija el espacio en disco que se usará para almacenar las páginas visitadas, es decir, se responde a la pregunta, ¿Cuánto deseo almacenar de Internet en nuestro disco duro?

Por defecto SQUID usará 100 MB, como límite para el tamaño del caché, pero si se quiere fijar, por ejemplo 500 MB, debemos fijar la entrada correspondiente de la siguiente forma:

```
cache_dir ufs /usr/local/squid/cache 500 16 256
```

En la línea anterior se selecciona el directorio de caché (/usr/local/squid/cache), indicando el tamaño máximo para éste (500), la cantidad de subdirectorios de primer nivel que puede contener (16, el valor por defecto) y, el número de subdirectorios de segundo nivel (256, también por defecto) que puede almacenar.

3.1.2.4 Vida en el caché Se puede configurar también el tiempo que pueden permanecer los objetos almacenados en el caché, dependiendo de las necesidades, lógicamente. De modo general, si se define un tiempo de permanencia demasiado bajo, se estará desaprovechando una de las principales ventajas del uso de servidor Proxy, mientras que si se establece un periodo demasiado alto, también se saturará innecesariamente la capacidad de almacenaje.

Parece una decisión razonable, en la mayoría de casos, fijar un mes de vida para los objetos del caché. Esto se logra con la instrucción:

```
reference_age 1 month.
```

3.1.3 Firewall (Iptables). Un firewall es un dispositivo que filtra el tráfico entre redes, como mínimo dos. El firewall puede ser un dispositivo físico o un software sobre un sistema operativo. En general, se debe verlo como una caja con 2 o más interfaces de red en la que se establecen unas reglas de filtrado con las que se decide si una conexión determinada puede establecerse o no. Incluso puede ir más allá y realizar modificaciones sobre las comunicaciones, como el NAT "Network Address Translation" ó (Traducción de direcciones de red).

Esa sería la definición genérica, hoy en día un firewall es un hardware específico con un sistema operativo o una IOS que filtra el tráfico TCP/UDP/ICMP/../IP y decide si un paquete pasa, se modifica, se convierte o se descarta. Para que un firewall entre redes funcione como tal debe tener al menos dos tarjetas de red. En la figura 2 se muestra la tipología clásica de un firewall:

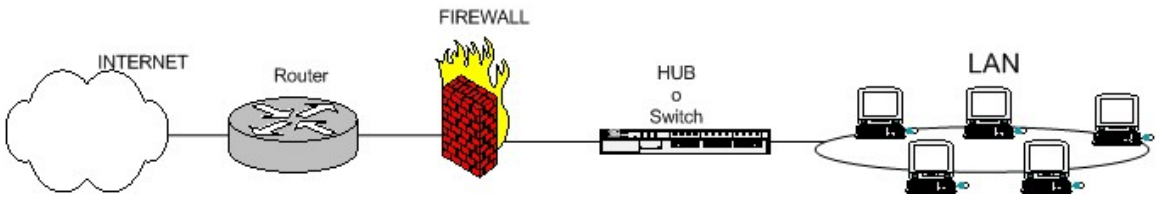


Figura 2: esquema de firewall típico entre red local e Internet

Sea el tipo de firewall que sea, generalmente no tendrá más que un conjunto de reglas en las que se examina el origen y destino de los paquetes del protocolo TCP/IP. En cuanto a protocolos es probable que sean capaces de filtrar muchos tipos de ellos, no solo los TCP, también los udp, los ICMP, y otros protocolos vinculados a VPNs. Este podría ser (un seudo-lenguaje). El conjunto de reglas del firewall del primer gráfico podría ser:

```
Politica por defecto ACEPTAR
```

```
Todo lo que venga de la red local al firewall ACEPTAR
Todo lo que venga da la IP de mi casa al puerto TCP22 ACEPTAR
Todo lo que venga de la IP de casa del jefe al puerto TCP 1723 ACEPTAR
Todo lo que venga de udenar.edu.co al puerto UDP 123 ACEPTAR
Todo lo que venga de la red local y vaya al exterior ENMASCARAR
Todo lo que venga del exterior al puerto TCP 1 a 1024 DENEGAR
Todo lo que venga del exterior al puerto TCP 3389 DENEGAR
Todo lo que venga del exterior al puerto UPD 1 al 1024 DENEGAR
```

En definitiva lo que se hace es:

1. Habilita él acceso a puertos de administración a determinadas IPs privilegiadas
2. Enmascara él tráfico de la red local hacia el exterior (NAT, una petición de un PC de la LAN sale al exterior con la IP pública), para poder salir a Internet
3. Denega él acceso desde el exterior a puertos de administración y a todo lo que este entre 1 y 1024.

Hay dos maneras de implementar un firewall:

- Política por defecto ACEPTAR: en principio todo lo que entra y sale por el firewall se acepta y solo se denegará lo que se diga explícitamente.
- Política por defecto DENEGAR: todo esta denegado, y solo se permitirá pasar por el firewall aquellos que se permita explícitamente.

Como es obvio imaginar, la primera política facilita mucho la gestión del firewall, ya que simplemente se preocupa de proteger aquellos puertos o direcciones que se sabe que no interesan; el resto no importa tanto y se deja pasar. Por ejemplo, si se quiere proteger solamente una máquina Linux, se puede hacer un netstat -ln (o netstat -an, o netstat -puta | grep LISTEN), saber que puertos están abiertos, poner reglas para proteger esos puertos.

En cambio, si la política por defecto es DENEGAR, a no ser que lo permita explícitamente, el firewall se convierte en un auténtico MURO infranqueable. El problema es que es mucho más difícil preparar un firewall así, y hay que tener muy claro como funciona el sistema (sea iptables o el que sea) y que es lo que se tiene que abrir sin caer en la tentación de empezar a introducir reglas súper-permisivas.

Cabe destacar que el orden en el que se ponen las reglas de firewall es determinante. Normalmente cuando hay que decidir que se hace con un paquete se va comparando con cada regla del firewall hasta que se encuentra una que afecta (match), y se hace lo que dicte esta regla (aceptar o denegar); después de eso ***no se mirarán más reglas*** para ese paquete. ¿Cuál es el peligro? Si se ponen reglas muy permisivas entre las primeras del firewall, puede que las siguientes no se apliquen y no sirvan de nada.

3.1.3.1 ¿Que es IPTABLES? IPTABLES es un sistema de firewall vinculado al kernel de Linux que se ha extendido enormemente a partir del kernel 2.4 de este sistema operativo. Al igual que el anterior sistema IPCHAINS (Utilizado en antiguos Kernels), un firewall de IPTABLES no es como un servidor que lo inicia o detiene o que se pueda caer por un error de programación, nunca tendrá tanto peligro como las aplicaciones que escuchan en determinado puerto TCP. Es así como IPTABLES esta integrado con el kernel, es parte del sistema operativo.

¿Cómo se pone en marcha? Realmente lo que se hace es aplicar reglas. Para ello se ejecuta el comando IPTABLES, con el que se añade, borra, o crea reglas. Un firewall de IPTABLES no es más que un script de shell en el que se van ejecutando las reglas de firewall. Un sencillo ejemplo sería:

```
## Administración de Servicios de red Universidad de Nariño
## www.udenar.edu.co

echo -n Aplicando Reglas de Firewall...

## FLUSH de reglas
iptables -F
iptables -X
iptables -Z
iptables -t nat -F

## Establecemos politica por defecto
iptables -P INPUT ACCEPT
iptables -P OUTPUT ACCEPT
iptables -P FORWARD ACCEPT
iptables -t nat -P PREROUTING ACCEPT
iptables -t nat -P POSTROUTING ACCEPT

## Empezamos a filtrar
## Nota: eth0 es el interfaz conectado al router y eth1 a la LAN
# El localhost se deja (por ejemplo conexiones locales a mysql)
/sbin/iptables -A INPUT -i lo -j ACCEPT

# Al firewall tenemos acceso desde la red local
iptables -A INPUT -s 192.168.10.0/24 -i eth1 -j ACCEPT

# Ahora hacemos enmascaramiento de la red local
# y activamos el BIT DE FORWARDING (imprescindible.)
iptables -t nat -A POSTROUTING -s 192.168.10.0/24 -o eth0 -j MASQUERADE

# Con esto permitimos hacer forward de paquetes en el firewall, o sea
# que otras máquinas puedan salir a traves del firewall.
echo 1 > /proc/sys/net/ipv4/ip_forward

## Y ahora cerramos los accesos indeseados del exterior:
# Nota: 0.0.0.0/0 significa: cualquier red
```

```
# Cerramos el rango de puerto bien conocido
iptables -A INPUT -s 0.0.0.0/0 -p tcp -dport 1:1024 -j DROP
iptables -A INPUT -s 0.0.0.0/0 -p udp -dport 1:1024 -j DROP

# Cerramos un puerto de gestión: webmin
iptables -A INPUT -s 0.0.0.0/0 -p tcp -dport 10000 -j DROP

echo " OK . Verifique que lo que se aplica con: iptables -L -n"

# Fin del script
```

En IPTABLES, se tienen varios tipos de reglas: reglas de filtrado, reglas de NAT, reglas de mangle (para manipular paquetes). El sistema se centrará principalmente en las reglas de filtrado, para poder filtrar tráfico e implementar buen firewall o cortafuegos.

Estas reglas se definen en la tabla filter (que es la tabla por defecto de iptables). Esta tabla tiene 3 cadenas:

- **INPUT:** es para filtrar paquetes que vienen hacia nuestra máquina.
- **OUTPUT:** es para filtrar paquetes generados por nuestra máquina.
- **FORWARD:** es para filtrar aquellos paquetes que llegan a nuestra máquina pero son para terceros, es decir, que llegan para que la máquina los vuelva a encaminar.

3.1.3.2 Sintaxis básica de IPTABLES La sintaxis que seguiremos para añadir reglas a cada una de las cadenas anteriores será del estilo:

```
iptables –t filter –A INPUT <opciones>
iptables –A INPUT <opciones>
```

Se puede usar cualquiera de las dos, ya que la tabla filter es la tabla por defecto. El parámetro -A se utiliza para ***añadir*** una regla a la cadena especificada justo después.

Los parámetros que se utilizan para filtrar son los siguientes:

- **-t <tabla>** Para especificar la tabla sobre la que trabajamos. Por ejemplo: ***-t nat***

- **-i <interfaz>** Para especificar la interfaz de red por la que entra el paquete. Por ejemplo: ***-i eth0***

- **-o <interfaz>** Para especificar la interfaz de red por la que sale el paquete. Por ejemplo: ***-o eth0***

- **-p <protocolo>** Para especificar el protocolo del paquete. Por ejemplo: ***-p tcp***

- **-s <ip>** Para especificar la ip de origen (o red de la que procede) del paquete. Por ejemplo: ***-s 192.168.0.2*** para especificar una ip, o bien ***-s 192.168.0.0/24*** para especificar una red de origen.

- **-d <ip>** Igual que en el caso anterior pero para la ip destinataria del paquete.

- **--dport <puerto>** Para especificar el puerto al que va dirigido el paquete. Por ejemplo: ***--dport 22***, o bien ***--dport 1:1024*** (para especificar un rango de puertos).

- **-j <accion>** Para especificar la acción que se realiza con el paquete si la regla se acepta. Por ejemplo ***-j ACCEPT*** para aceptar el paquete.

Con esto, y después de haber entendido el script se pueden resumir los pasos que deberían seguirse a la hora de configurar un cortafuego básico como este. Evidentemente, cualquier variación para adaptarlo a las necesidades de cada quien es perfectamente válida.

1. Borrar las reglas y las cadenas que hubiera, para asegurarse de que sólo estén cargadas las nuevas reglas.

2. Establecer las políticas por defecto para saber qué hacer si un paquete no coincide con ninguna regla.

3. Empezar el filtrado de paquetes con las reglas que se deseen, hay que tener cuidando con el orden: se pondrán las reglas más específicas ante las más generales.

3.1.4 Control de ancho de banda CBQ (Class-Based Queuing ó "Encolamiento Basado en Clases). En principio CBQ presenta la capacidad de otorgar el ancho de banda requerido por cada clase en un intervalo de tiempo especificado, si hubiera demanda del mismo. Esto se logra mediante un mecanismo similar al utilizado por los delay_pools de Squid para limitación de ancho de banda de Proxy HTTP, aplicando "esperas" entre las transferencias de paquetes.

En segunda instancia CBQ permite que las clases "tomen prestado" ancho de banda no utilizado por otras clases.

El Ancho de Banda en sí mismo es una función del tamaño y el tiempo: por ejemplo, la velocidad se la mide en metros por segundo. En el mundo de las comunicaciones, se

miden bits, bytes o algún múltiplo por segundo. De esta forma, se tiene que en un vínculo de 512kbit/s se logra una velocidad o tasa de transferencia de 64 kilobytes por segundo, ya que 8 bits = 1 byte y por lo tanto 512 / 8 = 64. (Hay que tener en cuenta que en ADSL o Cable módem tenemos diferentes anchos de banda dependiendo de si estamos enviando o recibiendo datos). De aquí que las limitaciones de ancho de banda se realicen intercalando esperas en la transmisión / recepción de datos.

3.1.4.1 ¿Qué son las colas? Las colas determinan el orden en que se mandan los paquetes. ¿Qué tiene que ver con el ancho de banda?

Imagínese una caja de supermercado donde la gente hace cola para pagar sus compras. La última persona llegada se pone al final de la cola y espera su turno: es una cola FIFO (First In, First Out). Ahora si dejamos ciertas personas siempre ponerse en medio de la cola, serán atendidas antes y podrán comprar más rápidamente.

Internet esta basado principalmente en TCP/IP y TCP/IP "no sabe nada" de ancho de banda. Lo que hace una máquina es mandar datos cada vez más rápido hasta que se detecte que algunos paquetes se están perdiendo, luego ralentiza el proceso.

Es el equivalente de no leer la mitad de los emails recibidos, esperando que la gente deje de mandar correo. La diferencia es que con Internet sí funciona.

3.1.4.2 Colas Basadas en Clases CBQ (***Class Based Queueing***) es un algoritmo de formación de colas que divide el ancho de banda de una conexión de red entre varias colas o clases. A cada cola se le asigna un tráfico basándose en la dirección de origen o de destino, el número de puerto, protocolo, etcétera. De forma opcional, se puede configurar una cola para que tome prestado ancho de banda de la cola matriz de la cual origina, si ésta está siendo infrautilizada. A las colas también se les da una prioridad de modo que aquellas que contengan tráfico interactivo, como SSH, puedan tener sus paquetes procesados antes que las colas que contengan tráfico masivo, como FTP.

Las colas CBQ se ordenan de un modo jerárquico. En la parte superior de la jerarquía se encuentra la cola matriz, que define la cantidad total de ancho de banda disponible. Las colas derivadas de ésta se crean bajo la cola matriz, y a cada una de ellas se les puede asignar alguna porción del ancho de banda de la cola matriz. Por ejemplo, se pueden definir las colas como sigue: 6

Cola Matriz (2Mbps)
Cola A (1Mbps)
Cola B (500Kbps)
Cola C (500Kbps)

En este caso, el ancho de banda total disponible se ha configurado a 2 mega bits por segundo (Mbps), que luego se divide entre las tres colas derivadas.

La jerarquía se puede expandir aún más definiendo colas dentro de otras colas. Para dividir el ancho de banda en partes iguales entre varios usuarios y clasificar también el tráfico de éstas con el fin de evitar que ciertos protocolos agoten el ancho de banda de otros, se puede definir una estructura de formación de colas como la siguiente:

Cola Matriz (2Mbps)
UsuarioA (1Mbps)
SSH (50Kbps)
Tráfico masivo (950Kbps)
UsuarioB (1Mbps)
Audio (250Kbps)
Tráfico masivo (750Kbps)
Http (100Kbps)
Otro tráfico (650Kbps)

Nótese que, en cada nivel, la suma del ancho de banda asignado a cada una de las colas no es superior al ancho de banda asignado a la cola matriz.

Se puede configurar una cola para que tome prestado ancho de banda de la cola de la que origina, si le sobra ancho de banda debido a que no está siendo utilizado por otras colas derivadas. Mírese como ejemplo una configuración de formación de colas como la siguiente:

Cola Matriz (2Mbps)
Usuario A (1Mbps)
SSH (100Kbps)
FTP (900Kbps, préstamo)
Usuario B (1Mbps)

Si el tráfico en la cola de ftp excede los 900Kbps y el tráfico en la cola del UsuarioA es menor de de 1Mbps (debido a que la cola de SSH está usando menos tráfico que los 100Kbps asignados), la cola de ftp tomará prestado el ancho de banda sobrante del UsuarioA. De este modo, la cola de ftp podrá usar más ancho de banda del que tiene asignado cuando sufra una sobrecarga. Cuando la cola de SSH incremente su carga, se devolverá el ancho de banda que se ha tomado prestado.

CBQ asigna a cada cola un nivel de prioridad. Las colas con una prioridad más alta tendrán preferencia sobre las colas de prioridad más baja durante una congestión, ya que ambas colas comparten la misma matriz de origen (o sea, siempre que ambas colas se encuentren

en la misma rama dentro de la jerarquía). Las colas con una misma prioridad se procesan del modo ***round-robin***. Por ejemplo:

Cola Matriz (2Mbps)
Usuario A (1Mbps, prioridad 1)
SSH (100Kbps, prioridad 3)
FTP (900Kbps, prioridad 5)
Usuario B (1Mbps, prioridad 1)

CBQ procesará las colas del UsuarioA y del UsuarioB del modo ***round-robin***; ninguna de las dos colas tendrá preferencia sobre la otra. Al mismo tiempo que esté procesando la cola del UsuarioA, CBQ también procesará las colas que deriven de ésta. En este caso, la cola de SSH tiene una prioridad más alta y obtendrá un trato preferente sobre la cola de ftp si hay congestión en la red. Nótese que no se comparan las prioridades de las colas de ssh y ftp con las colas del UsuarioA y UsuarioB, ya que no están en la misma rama dentro de la jerarquía.

3.1.4.3 ¿Qué es CBQ-INIT Script? Cbq-init script es un pequeño script es capaz de limitar el ancho de banda basándose en reglas como IP origen, IP destino, puerto origen, puerto destino y todas sus posibles combinaciones.

Dependencias: soporte QoS en el kernel (como módulo o en el propio kernel) para CBQ como mínimo.

En este caso los archivos de configuración están en un directorio indicado en la variable CBQ_PATH del propio script.

Los archivos de configuración se tienen que llamar cbq-X.nombre donde x es un número en hexadecimal de 4 cifras e indica el orden de arranque respecto a los demás archivos de configuración (hay uno por servicio normalmente). Los archivos tienen la siguiente apariencia: /etc/sysconfig/cbq/cbq-0001.http

Este es un ejemplo de archivo de configuración de cbq_init script.

```
DEVICE=eth0, 10Mbit, 1Mbit
        RATE=80Kbit
        WEIGHT=8Kbit
        PRIO=5
        RULE=:80,

DEVICE: nos indica el dispositivo de red, el ancho de banda del físico
del dispositivo (10/100Mbps) y un parámetro de afinamiento que suele ser
ancho de banda / 10.
```

```
RATE: es el máximo ancho de banda permitido
WEIGHT: es un parámetro de afinamiento que suele ser RATE/10
PRIO: es la prioridad entre 1 y 8. Cuanto más grande menos prioridad
5 es un valor estándar.

RULE: lo mejor es verlo con varios ejemplos:


RULE=10.1.1.0/24:80
Selecciona el tráfico que va al puerto 80 de la red 10.1.1.0

 RULE=10.2.2.5
 Selecciona todo el tráfico del host 10.2.2.5

 RULE=10.2.2.5:20/0xfffe
 Selecciona el tráfico que va a los puertos 20 y 21 en el host 10.2.2.5

 RULE=:25,10.2.2.128/26:5000
 Selecciona el tráfico que viene desde cualquier IP en el puerto 25 al
 Puerto 5000 de la red 10.2.2.128.

 RULE=10.5.5.5:80,
 Selecciona el tráfico que viene del puerto 80 del host 10.5.5.5
```

3.1.5 Funcionamiento de correo electrónico El servidor de correo electrónico, es una aplicación que permite enviar mensajes o correos de unos usuarios a otros, con independencia de la red que dichos usuarios estén utilizando.

Para lograrlo se definen una serie de protocolos, cada uno con una finalidad concreta, con los cuales se busca la interoperabilidad entre los diferentes servidores.

3.1.5.1 Protocolo SMTP Simple Mail Transfer Protocol: Es el protocolo que se utiliza para que dos servidores de correo intercambien mensajes. Este se basa en el modelo cliente-servidor, donde un cliente envía un mensaje a uno o varios receptores.

En el conjunto de protocolos TCP/IP, el SMTP va por encima del TCP, usando normalmente el puerto 25 en el servidor para establecer la conexión. En el protocolo SMTP todas las órdenes, réplicas o datos son líneas de texto, delimitadas por el carácter <CRLF>. Todas las réplicas tienen un código numérico al comienzo de la línea.

- Cuando un cliente establece una conexión con el servidor SMTP, espera a que éste envíe un mensaje ***"220 Service ready"*** o ***"421 Service non available"***.

- Se envía un ***HELO*** desde el cliente. Con ello el servidor se identifica. Esto puede usarse para comprobar si se conectó con el servidor SMTP correcto.

- El cliente comienza la transacción del correo con la orden ***MAIL***. Como argumento de esta orden se puede pasar la dirección de correo al que el servidor notificará cualquier fallo en el envío del correo. El servidor responde ***"250 OK"***.

- Ya se le ha dicho al servidor que se quiere mandar un correo, ahora hay que comunicarle a quien. La orden para esto es "***RCPT TO:<destino@host>".*** Se pueden mandar tantas órdenes RCPT como destinatarios del correo queramos. Por cada destinatario, el servidor contestará ***"250 OK"*** o bien ***"550 No such user here"***, si no encuentra al destinatario.

- Una vez enviados todos los RCPT, el cliente envía una orden ***DATA*** para indicar que a continuación se envían los contenidos del mensaje. El servidor responde ***"354 Start mail input, end with <CLRF>.<CLRF>"*** Esto indica al cliente como ha de notificar el fin del mensaje.

- Ahora el cliente envía el cuerpo del mensaje, línea a línea. Una vez finalizado, se termina con un <CLRF>.<CLRF> (la última línea será un punto), a lo que el servidor contestará ***"250 OK"***, o un mensaje de error apropiado.

- Tras el envío, el cliente, si no tiene que enviar más correos, con la orden ***QUIT*** corta la conexión. También puede usar la orden ***TURN***, con lo que el cliente pasa a ser el servidor, y el servidor se convierte en cliente. Finalmente, si tiene más menajes que enviar, repite el proceso hasta completarlos.

3.1.5.2 Protocolo IMAP Internet Message Access Protocol: Se utiliza para obtener los mensajes guardados en el servidor y pasárselos al usuario. Mediante IMAP se puede tener acceso al correo electrónico desde cualquier equipo que tenga una conexión a Internet. Una vez configurada la cuenta IMAP es posible especificar las carpetas que se desea mostrar y las que desean ocultar.

Así pues, un servidor de correo consta en realidad de dos servidores: un servidor SMTP que será el encargado de enviar y recibir mensajes, y un servidor IMAP que será el que permita a los usuarios obtener sus mensajes.

Para obtener los mensajes del servidor, los usuarios se sirven de clientes, es decir, programas que implementan un protocolo IMAP. En algunas ocasiones el cliente se ejecuta en la máquina del usuario (como el caso de Mozilla Mail, Evolution, Microsoft Outlook). Sin embargo existe otra posibilidad: que el cliente de correo no se ejecute en la máquina del

usuario; es el caso de los clientes vía web, como Horde, SquirrelMail, OpenWebmail. En ellos la arquitectura del servicio es más compleja.

3.1.5.3 IMAP y POP3 (Post Office Protocol versión 3) son los dos protocolos más prevalecientes para la obtención de correo electrónico. Todos los servidores y clientes de email están virtualmente soportados por ambos, aunque en algunos casos hay algunas interfaces específicas del fabricante típicamente propietarias. Por ejemplo, mientras que los protocolos propietarios utilizados entre el cliente Microsoft Outlook y su servidor Microsoft Exchange Server o el cliente Lotus Notes de IBM y el servidor Domino, estos productos también soportan interoperabilidad con IMAP y POP3 con otros clientes y servidores. La versión actual de IMAP, IMAP versión 4 revisión 1 (IMAP4ver1), está definida por el RFC 3501.

IMAP fue diseñado como una moderna alternativa a POP por Mark Crispin en el año 1986 [1]. Fundamentalmente, los dos protocolos les permiten a los clientes de correo acceder a los mensajes almacenados en un servidor de correo.

Algunas de las características importantes que diferencian a IMAP y POP3 son:

- Soporte para los modos de operación connected y disconnected
  Al utilizar POP3, los clientes se conectan al servidor de correo brevemente, solamente lo que tome descargar los nuevos mensajes. Al utilizar IMAP4, los clientes permanecen conectados el tiempo que su interfaz permanezca activa y descargan los mensajes bajo demanda. El patrón de IMAP4 puede dar tiempos de respuesta más rápidos para usuarios que tienen una gran cantidad de mensajes.

- Soporte para la conexión de múltiples clientes simultáneos a un mismo destinatario
  El protocolo POP3 asume que el cliente conectado es el único dueño de una cuenta de correo. En contraste, el protocolo IMAP4 permite accesos simultáneos a múltiples clientes y proporciona ciertos mecanismos a los clientes para que se detecten los cambios hechos a un mailbox por otro cliente concurrentemente conectado.

- Soporte para acceso a partes MIME de los mensajes y obtención parcial. Casi todo el correo electrónico de Internet es transmitido en formato MIME. El protocolo IMAP4 les permite a los clientes obtener separadamente cualquier parte MIME individual, así como obtener porciones de las partes individuales o los mensajes completos.

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

A través de la utilización de banderas definidas en el protocolo IMAP4 de los clientes, se puede vigilar el estado del mensaje, por ejemplo, si el mensaje ha sido o no leído, respondido o eliminado. Estas banderas se almacenan en el servidor, de manera que varios clientes conectados al mismo correo en diferente tiempo pueden detectar los cambios hechos por otros clientes.

- Soporte para accesos múltiples a los buzones de correo en el servidor. Los clientes de IMAP4 pueden crear, renombrar o eliminar correo (por lo general presentado como carpetas al usuario) del servidor, y mover mensajes entre cuentas de correo. El soporte para múltiples buzones de correo también le permite al servidor proporcionar acceso a los directorios públicos y compartidos.

- Soporte para búsquedas de parte del servidor IMAP4 proporciona un mecanismo para que los clientes pidan al servidor que busque mensajes de acuerdo a una cierta variedad de criterios. Este mecanismo evita que los clientes descarguen todos los mensajes de su buzón de correo con el fin de agilizar las búsquedas.

- Soporte para un mecanismo de extensión definido como reflejo de la experiencia en versiones anteriores de los protocolos de Internet, IMAP define un mecanismo explícito mediante el cual puede ser extendido. Se han propuesto muchas extensiones de IMAP4 y son de uso común. Un ejemplo de extensión es el IMAP IDLE, que sirve para que el servidor avise al cliente cuando ha llegado un nuevo mensaje de correo y éstos se sincronicen. Sin esta extensión, para realizar la misma tarea, el cliente debería contactar periódicamente al servidor para ver si hay mensajes nuevos.

3.1.5.4 Funcionamiento general de correo En una máquina (A) tenemos el servidor SMTP y el servidor POP/IMAP. En otra (B) tenemos un servidor Web con una aplicación cliente POP/IMAP. El usuario conecta vía WEB con (B) y entonces el cliente POP/IMAP establece una conexión POP/IMAP con el servidor de la máquina A; éste servidor le devuelve a B los mensajes del usuario, y una vez recibidos, el cliente genera una página Web con los mensajes recibidos. La página Web se pasa al servidor Web que será el que la envíe al explorador Web del usuario.

La transferencia de datos, entre cliente y servidor, se hace de manera encriptada mediante SSL Secure Sockets Layer para proteger la información del usuario.

3.1.5.5 SSL proporciona autentificación y privacidad de la información entre extremos sobre Internet mediante el uso de criptografía. Habitualmente, sólo el servidor es autentificado (es decir, se garantiza su identidad) mientras que el cliente se mantiene sin autentificar; la autentificación mutua requiere un despliegue de infraestructura de claves públicas (o PKI) para los clientes. Los protocolos permiten a las aplicaciones cliente-

servidor comunicarse de una forma diseñada para prevenir escuchas, la falsificación de la identidad del remitente y mantener la integridad del mensaje.

SSL implica una serie de fases básicas:

- Negociar entre las partes el algoritmo que se usará en la comunicación
- Intercambio de claves públicas y autenticación basada en certificados digitales
- Encriptación del tráfico basado en cifrado simétrico

Durante la primera fase, el cliente y el servidor negocian qué algoritmos criptográficos se van a usar. Las implementaciones actuales proporcionan las siguientes opciones:

Para criptografía de clave pública: RSA, Diffie-Hellman, DSA (Digital Signature Algorithm) o Fortezza; Para cifrado simétrico: RC2, RC4, IDEA (International Data Encryption Algorithm), DES (Data Encryption Standard), Triple DES o AES (Advanced Encryption Standard); Con funciones hash: MD5 o de la familia SHA.

El protocolo SSL intercambia registros; opcionalmente, cada registro puede ser comprimido, encriptado y empaquetado con un código de autentificación del mensaje (MAC). Cada registro tiene un campo de ***content_type*** que especifica el protocolo de nivel superior que se está usando.
Cuando se inicia la conexión, el nivel de registro encapsula otro protocolo, el protocolo ***handshake***, que tiene el ***content_type 22***.

El cliente envía y recibe varias estructuras ***handshake***:

- Envía un mensaje ***ClientHello*** especificando una lista de conjunto de cifrados, métodos de compresión y la versión del protocolo SSL más alta permitida. Éste también envía bytes aleatorios que serán usados más tarde (llamados ***Challenge*** de Cliente o Reto). Además puede incluir el identificador de la sesión.
- Después, recibe un registro ***ServerHello***, en el que el servidor elige los parámetros de conexión a partir de las opciones ofertadas con anterioridad por el cliente.
- Cuando los parámetros de la conexión son conocidos, cliente y servidor intercambian certificados (dependiendo de las claves públicas de cifrado seleccionadas). Estos certificados son actualmente X.509, pero hay también un borrador especificando el uso de certificados basados en OpenPGP.

- El servidor puede requerir un certificado del cliente, para que la conexión sea mutuamente autenticada.

- Cliente y servidor negocian una clave secreta común llamada ***master secret***, posiblemente usando el resultado de un intercambio ***Diffie-Hellman***, o simplemente encriptando una clave secreta con una clave pública que es desencriptada con la clave privada de cada uno. Todos los datos de claves restantes son derivados a partir de este ***master secret*** (y los valores aleatorios generados en el cliente y el servidor), que son pasados a través una función pseudo aleatoria cuidadosamente elegida.

TLS/SSL poseen una variedad de medidas de seguridad:

- Numerando todos los registros y usando el número de secuencia en el MAC.
- Usando un resumen de mensaje mejorado con una clave (de forma que solo con dicha clave se pueda comprobar el MAC). Esto se especifica en el RFC 2104).

- Protección contra varios ataques conocidos (incluidos ataques man in the middle attack), como los que implican un degradado del protocolo a versiones previas (por tanto, menos seguras), o conjuntos de cifrados más débiles.

- El mensaje que finaliza el protocolo handshake (Finished) envía un hash de todos los datos intercambiados y vistos por ambas partes.

- La función seudo aleatoria divide los datos de entrada en 2 mitades y las procesa con algoritmos hash diferentes (MD5 y SHA), después realiza sobre ellos una operación XOR. De esta forma, se protege a sí mismo de la eventualidad de que alguno de estos algoritmos se revelen vulnerables en el futuro.

4. ANALISIS ORIENTADO A OBJETOS DEL SISTEMA ANUBIS - SUITE DE APLICACIONES DESTINADAS A LA ADMINISTRACION DE SERVICIOS DE REDES DE AREA LOCAL TIPO IP BAJO PLATAFORMA GNU/LINUX

4.1 DESCRIPCION DEL SISTEMA ACTUAL DE LA RED DE DATOS DE LA UNIVERSIDAD DE NARIÑO

El Sistema de Administración de red de la Universidad de Nariño, se divide en las siguientes secciones: Publicaciones WEB, Control de usuarios de correo electrónico, Administración de nodos conectados a la red de cable e inalámbrica (WIFI), Administración del servidor Proxy, Control y Mantenimiento del filtro Web, Control de ancho de banda, Administración y control de un muro corta fuegos (Firewall).

4.1.1 Publicaciones web Actualmente en la Universidad, no existe un sistema de publicaciones Web como tal, los estudiantes, docentes, y demás personal administrativo, están en la incapacidad de publicar ellos mismos su contenido en línea, dado que cualquier tipo de publicación que se realiza sobre el portal de la Universidad, se realiza de forma manual y directamente en el servidor correspondiente, con previa autorización de la dependencia encargada, lo que crea dificultades en tener la información actualizada.

Los contenidos deben ser previamente revisados, que contemplen contenidos con fines académicos, y/o administrativos a la institución, deben llegar en formato digital para facilidad y eficiencia de la publicación al servidor correspondiente.

4.1.2 Correo electrónico Hoy en día la Universidad de Nariño, posee un sistema de correo electrónico, que trabaja sobre el protocolo IMAP, cuya interfaz está desarrollada en PHP, implementada sobre el servidor Web Apache, llamada Horde (Interfaz de correo libre bajo licencia GNU), pero que debido a su complejidad no ha permitido que el servicio como tal sea eficiente y rápido.

El servicio actual no es rápido, ágil, ó versátil para los usuarios, no se adapta a las necesidades de la Universidad, de su organización, así mismo no permite un control en el envío y recepción de correo electrónico. No es posible la creación de listas y grupos de usuarios lo cual es uno de los aspectos más importantes a tener en cuenta en esta sección dado que brindan la posibilidad de enviar correos específicos a grupos específicos, por ejemplo, un correo sobre la promoción de un seminario de ingeniería, sólo debería llegar aquellas personas que tengan que ver con el tema, como: ingeniería de sistemas, ingeniería electrónica, o ingeniería civil.

4.1.3 Administración de nodos de red Con respecto la administración de nodos de red de la Universidad, se tiene que hace algunos años existía un sistema que administraba los usuarios y los equipos asignados a dichos usuarios, y sus respectivos permisos, pero poco a poco se fue volviendo obsoleto con las nuevas distribuciones de sistemas operativos que aparecían, lo que se está haciendo es modificar y administrar manualmente los archivos de configuración, escribiendo directamente el archivo dhcpd.conf (Archivo de configuración del sistema para clientes DHCP), para la creación de nuevos nodos, sin la posibilidad de registrar datos completos de los dueños o usuarios de esos nodos, como sus nombre completos, ubicación, teléfonos de o cualquier otro tipo de información adicional vital e importante para la prestación de un correcto servicio.

Esto también perjudica en gran medida el control o administración de los demás servicios (ancho de banda, servicios temporizados, puertos, etc.), ya que es este archivo, la clave fundamental del orden y la jerarquía que tiene el nodo dentro de la red.
La forma en que se gestionan los permisos del equipo de red, así como la creación del mismo dentro del sistema, se vuelve con el tiempo, inoperable e insegura y propenso a que existan cada vez más errores humanos que sean difíciles de encontrar dado a la carencia de un sistema que controle la edición de estos archivos.

Para la creación de un nodo de red se necesita lo siguiente:

- La ubicación del equipo de cómputo a conectar.
- El equipo debe estar conectado físicamente, es decir cuenta con un punto de red conectado a su interfaz de red Ethernet ó Fast Ethernet.
- Se obtiene la dirección MAC de la interfaz de red del equipo.
- La dirección MAC es registrada manualmente en el archivo de configuración dhcpd.conf en el servidor Proxy encargado del servicio DHCP.

Para eliminar el equipo de la red, se edita el archivo de configuración dhcpd.conf para que el nodo ya no figure dentro de la lista de clientes del servidor DHCP.

Para mover a un equipo de subred, se debe editar en archivo dhcpd.conf para que el nodo figure dentro de otra subred, dependiendo de las necesidades que este tenga.

Actualmente, según la ubicación del equipo conectado a la red se puede conocer la subred a la que pertenece. Se tiene el siguiente orden:

- 192.168.1.0 máscara 255.255.255.0 → Bloque Biblioteca
- 192.168.1.20 máscara 255.255.255.0 → Bloque 2
- 192.168.1.3 máscara 255.255.255.0 → Bloque 3
- 192.168.1.4 máscara 255.255.255.0 → Antenas y red inalámbrica.
- 192.168.1.5 máscara 255.255.255.0 → Bloque Administrativo.
- 192.168.1.6 máscara 255.255.255.0 → Bloque Ingeniería.
- 192.168.1.7 máscara 255.255.255.0 → Bloque Medicina.
- 192.168.1.8 máscara 255.255.255.0 → Equipos Móviles WIFI.
- 192.168.1.10 máscara 255.255.255.0 → Bloque 1
- 192.168.1.11 máscara 255.255.255.0 → Bloque Medicina Veterinaria
- 192.168.1.12 máscara 255.255.255.0 → Bloque de Artes
- 192.168.1.13 máscara 255.255.255.0 → Bloque de Derecho

De acuerdo con esto cabe destacarse que existe una gran limitante en la creación de nuevos nodos de red, ya que impiden la creación de más de 253 nodos por cada subred, esto debido a que el direccionamiento está hecho en direcciones clase C con máscara clase C lo cual indica que solo se dispone de el ultimo octeto para utilización de hosts, y los tres primeros octetos para la subred, para mayor información sobre manejo de subredes ***leer anexo subredes***.

4.1.4 Administración de servidor proxy. Al igual que los demás servicios, la configuración del servidor Proxy se realiza por medio de la edición de archivos secuenciales propios de la aplicación instalada en Linux, como lo es en este caso SQUID.

La configuración que se realiza en SQUID por lo general, se hace una sola vez al momento de instalar la aplicación, de implementarla, y adaptarla a las necesidades que se tenga en la red como tal.

Así mismo, se trata de poder controlar y administrar las opciones más utilizadas, y/o algunas que se puedan utilizar en un futuro, que expandan la capacidad del caché como tal, y que se ajuste a las necesidades de la institución.

Cabe destacar que de la Administración del servidor Proxy, se deriva directamente la parte del filtro Web ya que es una de tantas opciones que SQUID es capaz de soportar.

4.1.5 Filtro web. Solo desde el inicio del semestre A-2006 en la Universidad, se ha venido implementando un filtro Web que ha ayudado en gran parte a brindar un mejor servicio de Internet y una mejor velocidad a todos los usuarios. Cabe destacar que no solo beneficia a la velocidad del servicio y al desempeño del servidor, sino también a todos los equipos clientes integrados a la red ya que al bloquear ciertas páginas mal intencionadas de la red Internet (aplicaciones espías, páginas con contenido pornográfico, screensavers malintencionados o programas de ocio), se crean dos fenómenos:

Uno de ellos es en el aspecto social-cultural, y el otro en el aspecto lógico-físico de la máquina cliente. Es muy importante hacer caer en cuenta a la comunidad Universitaria que los recursos que posee la institución son limitados, que existen para propósitos meramente académico-administrativos, que es Academia lo que se encuentra a través de todo el campus y que debe respetarse como tal, los resultados han sido sorprendentes, los equipos infectados han disminuido alrededor del 70% y los problemas de conexión a la red debido al daño del sistema en cada cliente son ínfimos, de allí su gran importancia.

Actualmente, el filtro Web se realiza actualizando archivos secuenciales que son llamados a través del archivo de configuración inicial de SQUID “squid.conf”, siguiendo las siguientes listas de acceso.

```
#Bloqueo paginas

acl paginas url_regex -i "/export/squidconf/paginas.deg"
deny_info http://www.udenar.edu.co/general/denied/ paginas
http_access deny paginas
```

La anterior lista de acceso brinda la posibilidad de agregar nuevas URLS corruptas, y/o palabras inadecuadas para la comunidad universitaria, dado a que hace referencia al archivo paginas.deg ubicado en la ruta "/export/squidconf" la cual representa un directorio cualquiera hecho por el usuario administrador, el archivo se representa de la siguiente forma:

```
#Bloqueo paginas
gator
bananasexy
hentai
sexyono
yadio
casino
^http://www.pasto.com
^http://www.amigos.com
^http://www.pasto.com/index.php
^http://www.depasto.com
^http://www.caliescali.com
^http://webmessenger.msn.com
^http://webmessenger.msn.es
^http://www.latinchat.com
^http://habla.chat-co.terra.co
e-messenger.net
^http://www.pastorumba.com
^http://www.chicas.com
^http://www.juegos.com
^http://pastorumba.com
^http://www.batanga.com
^http://www.e-messenger.cl
^http://www.supertangas.com
```

En este archivo se puede insertar cualquier palabra que se quiere sea filtrada de alguna URL como "casino", aquí todas las URLS que contengan la palabra casino serán bloqueadas, ó en donde se sea explicito con una URL completa como por ejemplo ^http://www.batanga.com.

Luego en la segunda línea se encuentra la URL que SQUID presentará por defecto para todas y cada una de la URLS que sean detectadas en los navegadores de los usuarios, por ejemplo si se tiene reportada la URL `http://www.playboy.com` dentro del archivo "paginas.deg", entonces a la hora de introducir `http://www.playboy.com` en la barra de direcciones del navegador , SQUID impedirá su acceso y mostrará el contenido de `http://www.udenar.edu.co/general/denied/` la cual es una URL que informa que la solicitud hecha por el cliente ó usuario ha sido bloqueada debido a que incumple con los objetivos de la institución.

La tercera y última línea es la habilitación o deshabilitación de esa lista de acceso, en otras palabras "deny", deniega el servicio, y "allow" lo brinda o permite.

El principal problema es agregar nuevas URLS indebidas al archivo en cuestión debido a la gran cantidad de pornografía y paginas sin valor educativo, artístico y/o científico.

Entre más URLS tenga determinado archivo "paginas.deg", más confiable será el filtro. Su crecimiento es siempre constante.

4.1.6 Control de ancho de banda. Actualmente no se tiene implementado ningún tipo de control de ancho de banda en la institución, el recurso se limita bloqueando puertos especiales para evitar descargas desbordantes por parte de los clientes pero inclusive así, la situación algunas veces o en los conocidos horarios pico, se vuelve inquietante.

La adaptación del tráfico da al administrador de la red la posibilidad de controlar la utilización del ancho de banda de un enlace físico individual compartido basado en ciertos criterios del tráfico de la misma manera que lo hace el filtrado. Es necesario ya que TCP/IP no fue diseñado originalmente para soportar la gestión y las peticiones del ancho de banda con el propio protocolo, como por ejemplo, SNA (***Systems Network Architecture*** el cual es un modelo que presenta similitudes con el modelo de referencia OSI).

Sin estar controlado, los clientes TCP/IP usarán el ancho de banda hasta que estén saciados, o no haya más disponible. De esta manera, las redes basadas en TCP/IP ofrecen el servicio ***del mejor esfuerzo. QoS,*** o Calidad del servicio (***Quality of Service***), está muy relacionado con la adaptación del tráfico; ofrece a los clientes de una red un mecanismo por el cual piden una reserva de ancho de banda para su sesión. Esta petición la realiza el router de la red, el cual intentará garantizar que el ancho de banda es disponible través de la red, o al menos de la extensión en la que el router tiene influencia.

CBQ (***Class – Based Queue***, Cola basada en clases). Esta disciplina implementa un algoritmo basado en prioridades relativas de las clases de componentes. Por esta razón, se utiliza como un conector para enviar paquetes a clases hijas que pueden contener

disciplinas de colas (o simples FIFO). Se necesita saber cuanto ancho de banda hay disponible para ello (bandwidth pbs), cuál es el tamaño medio del paquete (avpkt bytes), y la tasa a la cual deberían pasar los datos (rate bps). También requiere un ***weigth bps***, el cual es un parámetro notable que se debería establecer sobre la tasa de 1 a 10. Si se profundiza el código, el algoritmo necesita de esas figuras para ser capaz de funcionar en intervalos apropiados con el objeto de servir clases y colas.

Igualmente, existe la necesidad de poder modificar las clases existentes de control de ancho de banda y crear nuevas, dependiendo de las necesidades que se tengan en un momento dado, obviamente administrándolo desde la misma interfaz Web, sin tener que modificar los archivos del sistema operativo como tal directamente, eso simplificaría la tediosa tarea de controlar este preciado recurso como lo es el ancho de banda.

4.1.7 Firewall o corta fuegos La adopción de la tecnología de IPTABLES como cortafuegos en la Universidad se ha venido adoptando por los últimos 2 años, tal es su importancia que ha permitido enlazar por primera vez en la historia a todas sus sedes, al menos tecnológicamente hablando, cuando se trata de realizar video conferencias entre sedes como por ejemplo (Pasto - Ipiales), así como también brindar la posibilidad crear servicios especiales como un NAT o un DNAT para que un equipo de la red local interna y privada, pueda ser visto a través de Internet.

La importancia de IPTABLES, o la adopción de algún tipo de firewall son una pieza fundamental en cualquier red de área local, y mucho más cuando se trata de una Institución tan grande como lo es la Universidad como tal. Se debe tener mucho cuidado a la hora de brindar permisos, de filtrar paquetes, ó de crear servicios avanzados de red, por que de la estructura de un buen firewall ó corta fuegos depende en gran parte la optimización, y el rendimiento de la red.

Es aquí en donde se abren o se cierran determinados puertos de red para asignar los distintos servicios de red antes vistos. **Véase sección de iptables capitulo 3.**

Ahora bien, hoy por hoy se tiene implementado un firewall bajo IPTABLES que corre bajo RedHat Enterprise Linux 3, cuya estructura funciona en cualquier distribución de Linux actual ya sea propietaria o GNU/Linux, la diferencia es nula.

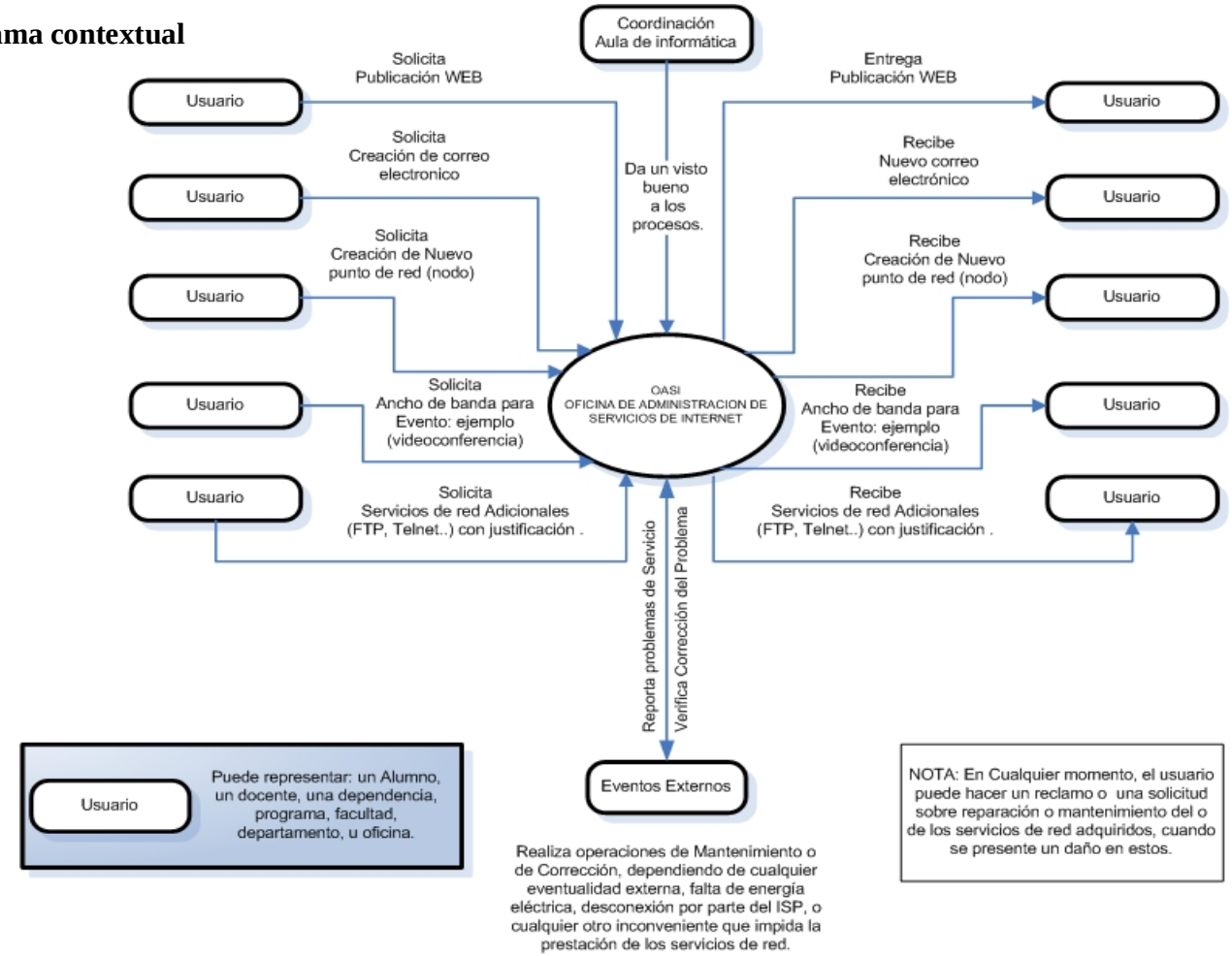
El proceso para llevar a cabo cualquier permiso de red antes visto, se realiza de forma manual, escribiendo directamente en un Script antes elaborado, las nuevas reglas a adicionar. Para esto es necesario tener el conocimiento de la sintaxis de las reglas, y de la semántica de cada una de ellas, así como la estructura lógica de cómo esta escrito el Script como tal.

Para que el usuario adquiera este conocimiento es necesario que el usuario sea capaz de administrar a un buen nivel un sistema operativo Linux, así como también de conocer el funcionamiento interno de la máquina, como Linux maneja los puertos, ser capaz de gestionar manualmente servicios de red (DHCP, FTP, SSH,…), así como también tener un claro conocimiento de enrutamiento bajo Linux.

Tal es que se hace vital, la creación de este módulo que facilitaría en gran medida la administración de la mayor parte de los servicios de red, así como también haría mucho más sencilla cualquier capacitación al respecto.

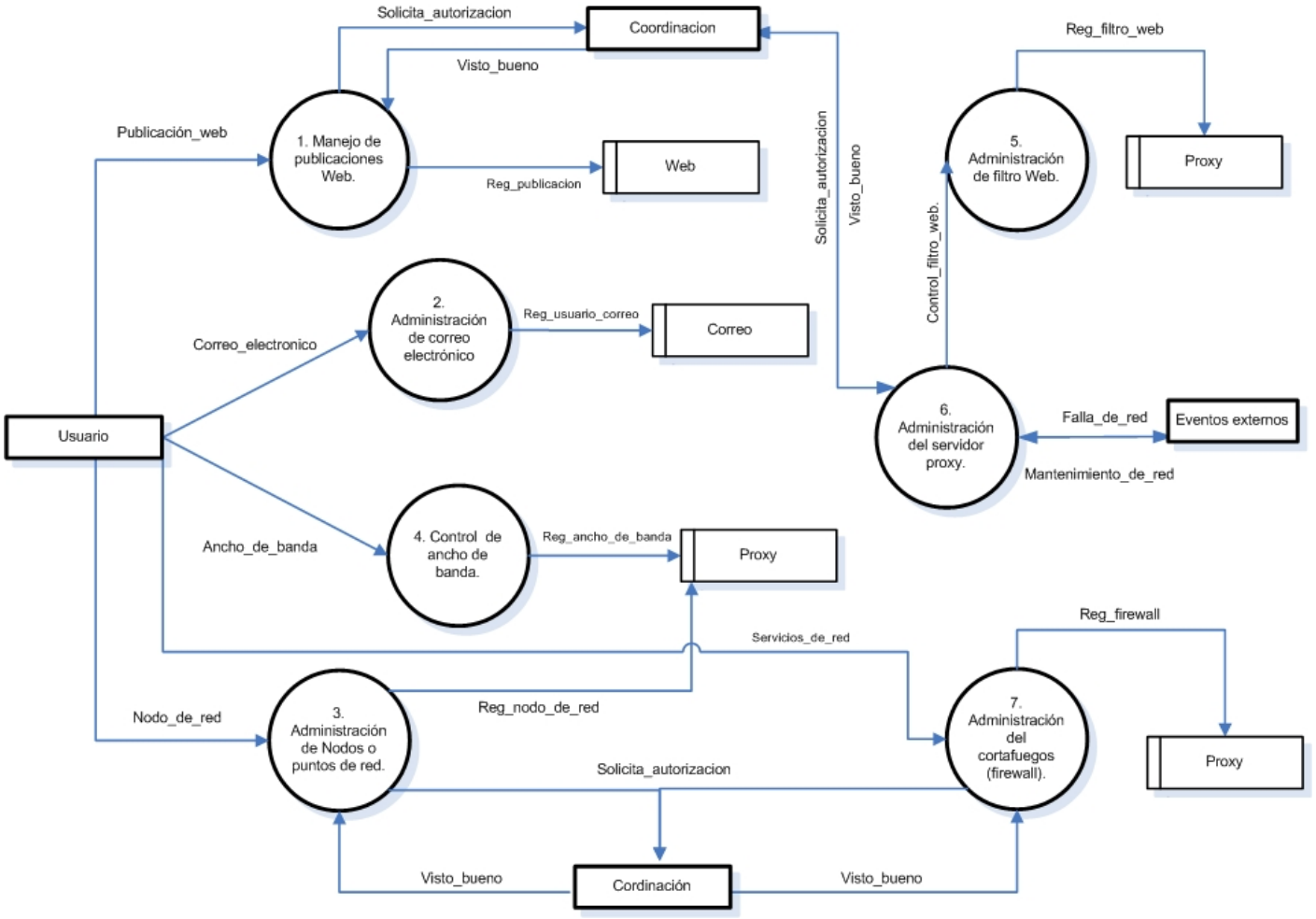
4.2 MODELO ESTRUCTURADO DEL SISTEMA ACTUAL

4.2.1 Diagrama contextual



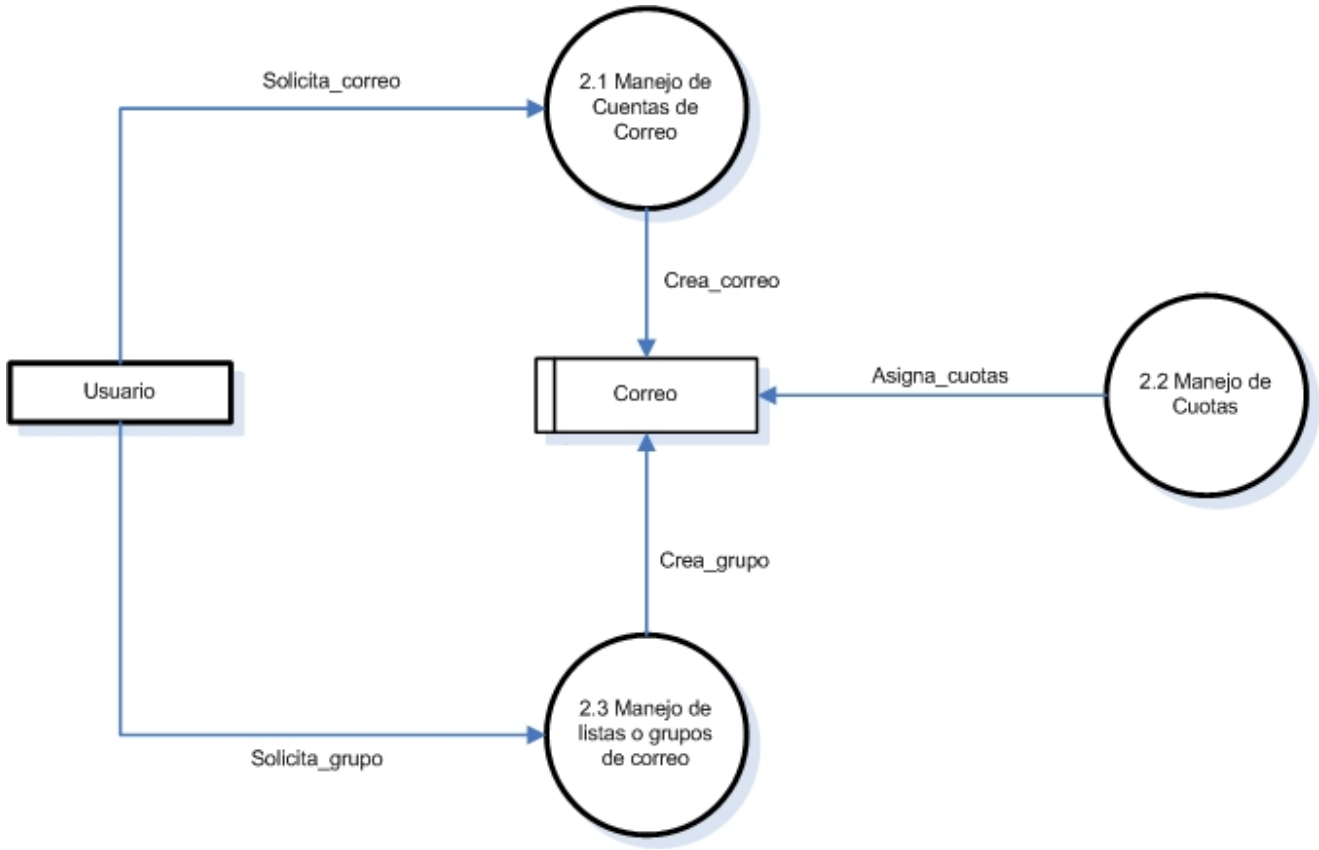
Esquema. 1 Diagrama Contextual

4.2.2 Nivel 1. OASI (Oficina de Administración de Servicios de Internet)



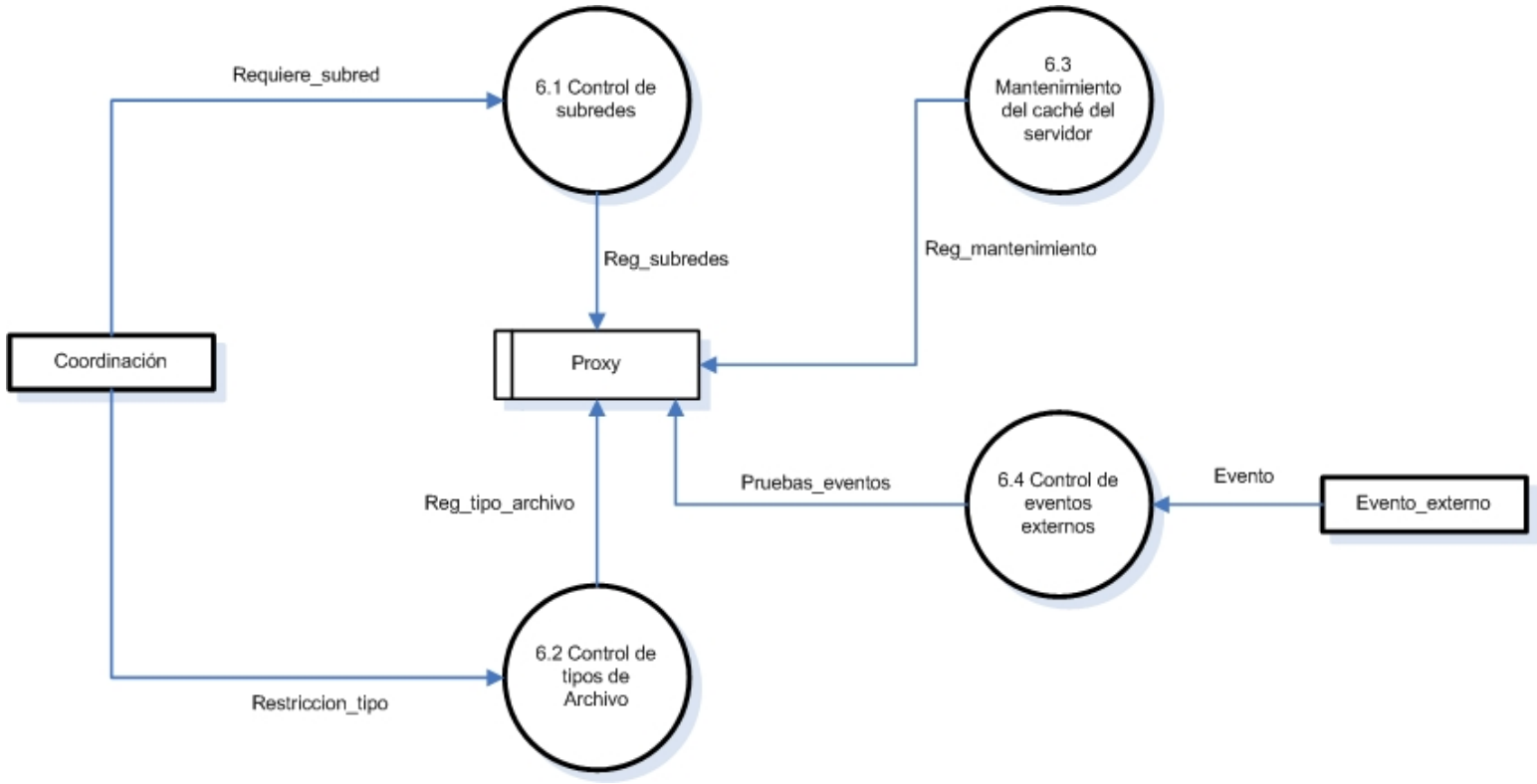
Esquema 2. Diagrama contextual nivel 1 (Oficina de administración de servicios de Internet).

4.2.3 Nivel 2 proceso 2: administración de correo electrónico



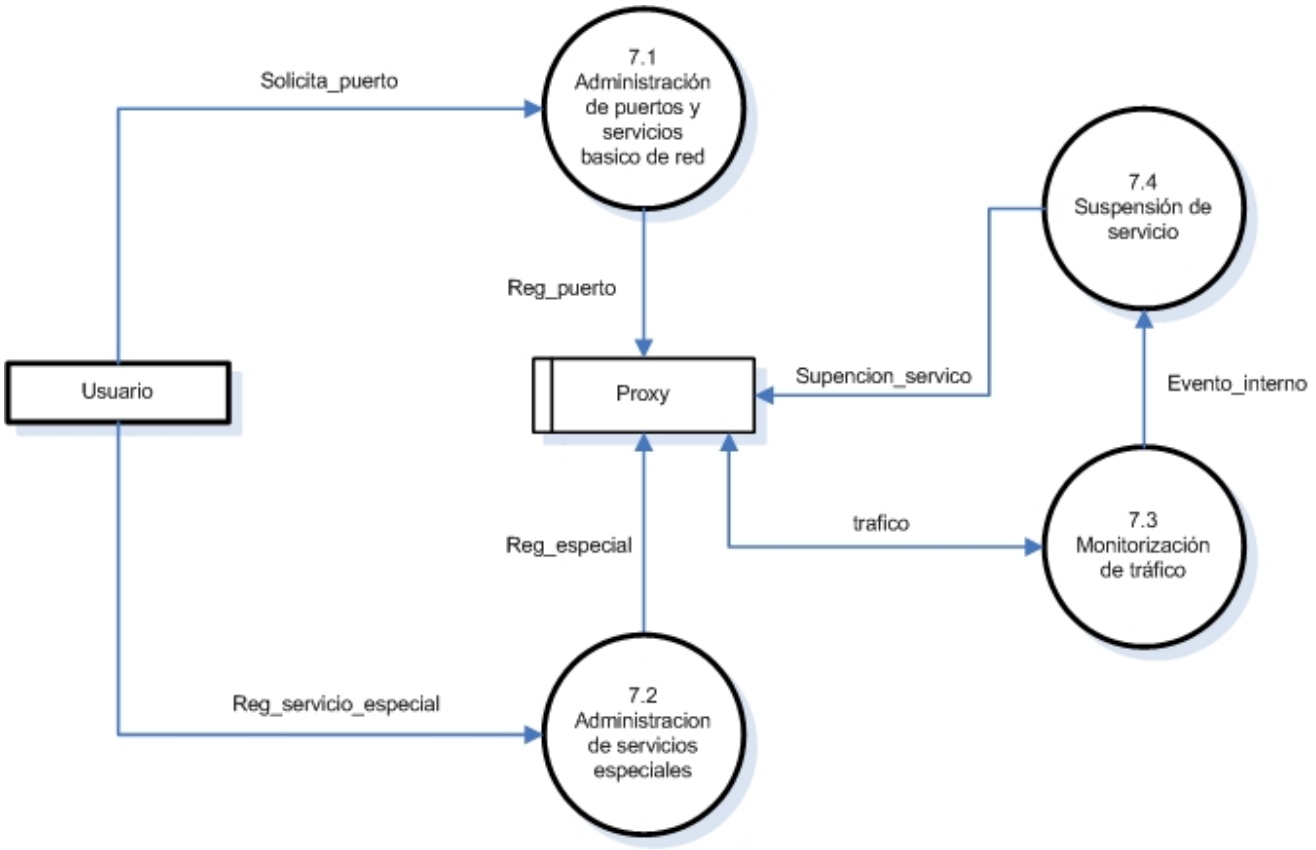
Esquema 3. Diagrama contextual nivel 2 proceso 2 (Administración de correo electrónico).

4.2.4 Nivel 2 proceso 6: administración de servidor proxy



Esquema 4. Diagrama Contextual nivel 2 proceso 6 (Administración de servidor Proxy).

4.2.5 Nivel 2 proceso 7: administración de firewall o corta fuegos



Esquema 5. Diagrama contextual nivel 2 proceso 7 (Administración de firewall o cortafuegos).

4.3 DICCIONARIO DE DATOS (OASI)

4.3.1 Descripción de procesos

Número / Id:	1
Nombre:	Manejo de Publicaciones Web
Descripción:	Se encarga de manejar y publicar la información en línea en el portal de la Universidad del personal académico y/o administrativo con previa solicitud por escrito a la coordinación del aula de informática.

Número / Id:	2
Nombre:	Administración de Correo electrónico
Descripción:	Se encarga de Crear, manejar y/o eliminar las cuentas de correo electrónico de los docentes y estudiantes de la Universidad, a través del registro directo en el servidor de correo.

Número / Id:	3
Nombre:	Administración de nodos o puntos de Red
Descripción:	Registra, Modifica, o elimina nodos o puntos de red a través de archivos de configuración del DHCP Server en el servidor, utilizando la dirección física o (MAC Address) de cada equipo cliente.

Número / Id:	4
Nombre:	Control de Ancho de Banda
Descripción:	Este proceso se encarga de brindar, o restringir el ancho de banda a un equipo o subred, dentro de la LAN privada de la institución, utilizando archivos de configuración específicos para la utilización de un script que trabaja sobre CBQ (Class – Based Queue, Cola basada en clases).

Número / Id:	5
Nombre:	Administración de filtro Web
Descripción:	Proceso que controla el acceso a Internet a ciertas páginas, URLS, direcciones físicas (IP), e inclusive de ciertas palabras que estén dentro del ámbito de lo vulgar u obsceno, que impidan la construcción o la formación académica dentro de la Universidad.

Número / Id:	6
Nombre:	Administración de Servidor Proxy
Descripción:	Trata de la administración, y el mantenimiento que se le da al servidor Proxy y caché (SQUID), en el cual se puede realizar otro tipo de restricciones como la descarga de ciertos tipos de archivos, (MP3, MPEG, ISO, etc...), controlar el tamaño de los archivos a descargar, agregar nuevas subredes con servicio de Internet, o para analizar los archivos logs de acceso, de los usuarios conectados, con fines de control y vigilancia. En la administración también se tiene en cuenta, el tamaño del caché que se crea durante un determinado tiempo de uso por parte de los usuarios, el tamaño del caché no debe sobrepasar el 60% de la partición física asignada para tal fin.

Número / Id:	7
Nombre:	Administración de Contrafuegos o (Firewall)
Descripción:	Este proceso es uno de los más importantes, ya que brinda o deniega acceso a los recursos del sistema y de la red de datos, controla la asignación de puertos, genera la posibilidad de crear Proxy transparente a los usuarios, protege al servidor y a los usuarios de posibles ataques, gracias a su metodología de "abrir solo lo que se necesite y cerrar todo lo demás", y brinda la posibilidad de crear NAT (Network Address Translation o traducción de dirección de red), para que un equipo de la red interna realice algún proceso como servidor y pueda ser visto a través de Internet. Realizado mediante la creación de un Script ordenadamente escrito para generar las reglas deseadas, mediante el uso de IPTABLES.

Número / Id:	2.1
Nombre:	Manejo de Cuentas de correo
Descripción:	Proceso que crea, edita o elimina las cuentas de correo electrónico de la institución, teniendo en cuenta la vinculación del usuario a esta.

Número / Id:	2.2
Nombre:	Manejo de Cuotas

Descripción:	Proceso que limita el espacio físico de las cuentas de correo cuando los usuarios abusan de este, es un proceso de mantenimiento y control.

Número / Id:	2.3
Nombre:	Manejo de Listas o grupos de correo
Descripción:	Proceso que permite al usuario solicitar el envió de un correo electrónico determinado, a más de un destinatario ya sea una lista especificada ó un grupo determinado (todos los decanos, todos los estudiantes de ingeniería, etc.)

Número / Id:	6.1
Nombre:	Control de subredes
Descripción:	Proceso que permite crear nuevas subredes o eliminar las existentes dentro del Proxy, con el fin de expandir la capacidad de la red como tal y/o para tener un mejor orden en la distribución de esta.

Número / Id:	6.2
Nombre:	Control de tipos de archivo
Descripción:	Proceso encargado de controlar los tipos de archivos que no pueden estar al acceso de los usuarios de la red LAN desde Internet. Es decir se encarga de restringir ciertos tipos de archivos (MPEG, MP3, etc.), que perjudicarían la velocidad de la LAN debido a su gran tamaño, y/o exigencias de recursos.

Número / Id:	6.3
Nombre:	Mantenimiento del caché del servidor
Descripción:	Proceso encargado de realizar operaciones de mantenimiento al espacio físico que ocupa el caché del servidor Proxy, así como también tener la posibilidad de ampliar o disminuir el caché en la configuración lógica del servidor Proxy.

Número / Id:	6.4
Nombre:	Control de Eventos externos

Descripción:	Proceso que realiza operaciones de mantenimiento, verificación de archivos de configuración, verificación de procesos, y verificación de logs que indiquen de alguna forma alguna inconsistencia o falencia en el sistema.

Número / Id:	7.1
Nombre:	Administración de puertos de red
Descripción:	Proceso que asigna o deniega acceso a ciertos puertos de red ya sea para un solo equipo o para toda una red. Los puertos de red están íntimamente ligados a un servicio de red y/o aplicación que pueden ser requeridos por el usuario justificando su necesidad.

Número / Id:	7.2
Nombre:	Administración de servicios especiales
Descripción:	Proceso que brinda servicio y/o acceso a aplicaciones especiales, como son las aplicaciones peer to peer, mensajería instantánea, así como también servicios avanzados de NAT, Enmascaramiento, o DNAT.
Número / Id:	7.3
Nombre:	Monitorización de tráfico
Descripción:	Proceso que brinda información al administrador sobre el estado del tráfico en la red, lo cual sirve para reconocer un evento interno como abuso de servicio por parte de un equipo o host, así como también para observar los cambios realizados por otros módulos como control de ancho de banda.

Número / Id:	7.4
Nombre:	Suspensión de servicio
Descripción:	Proceso que inhabilita a un equipo o serie de equipos dado el caso en que este o estos abusen del servicio, violen las normativas de seguridad de la red o este desaprovechando el recurso. La suspensión se lleva a cabo mediante monitorización de tráfico y de logs del servidor Proxy.

4.3.2 Descripción de flujo de datos

Nombre:	Publicación_web

Descripción:	Envía toda la información que desea ser publicada, en medio digital, con su correspondiente visto bueno de la coordinación del aula de informática.		
Tipo de Flujo de Datos:	Externa		
Datos:	Información a publicar en medio completamente digital, junto con la firma de visto bueno de la coordinación del aula de informática.		
Origen:	Usuario	**Destino:**	Proceso 1
Comentario:	En caso de que la petición no esté firmada o no tenga el visto bueno, la información, no podrá ser publicada.		

Nombre:	Reg_publicacion		
Descripción:	Envía toda la información entregada por el usuario solicitante, y formateada para su publicación, hacia el servidor Web que albergará dicha información.		
Tipo de Flujo de Datos:	Externa		
Datos:	Archivos digitalizados en formato Web para su publicación.		
Origen:	Proceso 1	**Destino:**	Servidor Web
Comentario:	En el caso de que la información tenga un vencimiento o no se tenga una actualización periódica al menos 1 vez al semestre, dicha información es desplazada del portal de la institución.		

Nombre:	Correo_electronico		
Descripción:	Envía una solicitud de creación de cuenta de correo electrónico de la Institución.		
Tipo de Flujo de Datos:	Externa		
Datos:	Oficio de la persona, grupo, u oficina, demostrando su vinculación a la Universidad, con el nombre de usuario que desea usar en la cuenta de correo.		
Origen:	Usuario	**Destino:**	Proceso 2
Comentario:	En el caso de que la información no sea autentica se deniega la cuenta de correo, o por el contrario, se le pide al representante de la cuenta que se dirija a la Oficina de Administración de servicios de Internet para que ingrese su nueva clave de usuario.		
Nombre:	Reg_usuario_correo		
Descripción:	Envía toda la información entregada por el usuario solicitante, hacia el servidor de Correo en el cual se crea un		

	usuario del sistema junto con el nombre completo del solicitante, y sus respectivos directorios para el manejo del correo.		
Tipo de Flujo de Datos:	Externa		
Datos:	Nombre completo de Solicitante, dependencia de trabajo, y nombre de usuario para la creación de cuenta.		
Origen:	Proceso 1	**Destino:**	Servidor de Correo
Comentario:	En el caso de que la cuenta creada no sea utilizada, en un semestre, la cuenta se elimina, o por el contrario si esta ocupa mucho espacio en disco, se envía un correo pidiendo mantenimiento de los mensajes guardados al usuario.		

Nombre:	Servicios_de_red		
Descripción:	Envía un oficio por escrito, con su correspondiente visto bueno de la coordinación del aula de informática, y con los servicios que necesita y/o los puertos requeridos.		
Tipo de Flujo de Datos:	Externa		
Datos:	Nombre del responsable, dependencia, servicios requeridos, o los números de puertos requeridos.		
Origen:	Usuario	**Destino:**	Proceso 7
Comentario:	En el caso de que la utilización del servicio sea utilizada de manera inadecuada, se suspende temporal o definitivamente dependiendo de la severidad del caso.		

Nombre:	Control_filtro_web.		
Descripción:	Revisión de archivos del sistema, en busca de fallos presentes ante un evento externo ó en busca de brindar algún permiso a un determinado usuario que solicite una URL bloqueada por el filtro.		
Tipo de Flujo de Datos:	Externa		
Datos:	Solicitud del permiso junto con la URL o problema presente.		
Origen:	Proceso 6	**Destino:**	Proceso 5
Comentario:	La mayoría de los problemas que se presentan en el correcto funcionamiento de la red son reportados por los usuarios. Así que la solicitud puede ser para reportar un inconveniente o pedir un permiso de URL.		

Nombre:	Reg_filtro_web

Descripción:	Edición manual de archivos del sistema, para corregir fallos presentes ante un evento externo ó para brindar algún permiso a un determinado usuario que solicitó una URL bloqueada por el filtro.		
Tipo de Flujo de Datos:	Externa		
Datos:	URL en conflicto.		
Origen:	Proceso 5	**Destino:**	Servidor Proxy
Comentario:	Cualquier modificación de los archivos del filtro, requiere el reinicio de dicho servicio.		

Nombre:	Falla_de_red		
Descripción:	Evento externo e inesperado que genera una falla en el servicio de red ya sea en un solo equipo en el menor de los casos, hasta la desconexión total de toda la universidad y/o alguna de sus sedes		
Tipo de Flujo de Datos:	Externa		
Datos:	Reporte o divulgación del problema presente.		
Origen:	Eventos Externos	**Destino:**	Proceso 6
Comentario:	Los fallos son reportados por los usuarios, o por operaciones de mantenimiento rutinarias como revisión general de todo el nodo de red (router, Proxy, DNS, Web Server, etc…).		

Nombre:	Mantenimiento_de_red		
Descripción:	Tareas de mantenimiento constante o respuesta a un Evento externo e inesperado que genera una falla en el servicio de red, es solucionado, y se procede a realizar las respectivas pruebas, verificar que lo afectado está en correcto funcionamiento y que no se hayan generado nuevos problemas		
Tipo de Flujo de Datos:	Externa		
Datos:			
Origen:	Proceso 6	**Destino:**	Eventos Externos
Comentario:	La reparación o corrección del problema también se puede comprobar preguntándole a la persona, ó personas afectadas sobre el estado de su servicio.		

Nombre:	Reg_firewall		
Descripción:	Crea o modifica las reglas de firewall necesarias para brindar el requerimiento deseado.		
Tipo de Flujo de Datos:	Externa		
Datos:	Dirección IP de la máquina, y número de puerto ó protocolo afectado.		
Origen:	Proceso 7	**Destino:**	Proxy
Comentario:			

Nombre:	Ancho_de_banda.		
Descripción:	Solicita de forma verbal o escrita la ampliación de ancho de banda de algún determinado equipo conectado a la red interna de la institución, por lo general debido a algún evento especial (Videoconferencia).		
Tipo de Flujo de Datos:	Externa		
Datos:	Justificación, nombre del responsable, dependencia, tiempo que necesita la ampliación de ancho de banda, y el ancho de banda estimado.		
Origen:	Usuario	**Destino:**	Proceso 4
Comentario:	En el caso de que la utilización del servicio sea utilizada de manera inadecuada, se suspende temporal o definitivamente dependiendo de la severidad del caso.		

Nombre:	Reg_ancho_de_banda		
Descripción:	Crea y Modifica los archivos necesarios para el requerimiento antes hecho por el usuario, de forma que se registran directamente al servidor Proxy, para su ejecución e implementación.		
Tipo de Flujo de Datos:	Externa		
Datos:	IP de la máquina cliente, ancho de banda requerido, tiempo del servicio.		
Origen:	Proceso 4	**Destino:**	Servidor Proxy
Comentario:	Este servicio se brinda siempre y cuando se justifique claramente, y no interfiera con el desempeño de las demás actividades académico administrativas.		

Nombre:	Nodo_de_red		
Descripción:	Envía un oficio por escrito, con su correspondiente visto bueno de la coordinación del aula de informática la solicitud de la implementación de un nuevo punto de red.		
Tipo de Flujo de Datos:	Externa		
Datos:	Nombre del responsable, dependencia, información física-lógica del equipo, y la futura ubicación del equipo.		
Origen:	Usuario	**Destino:**	Proceso 3
Comentario:	Dado el caso en que la ubicación carezca de cableado de red, se debe realizar un estudio técnico previo para la factibilidad de dicha instalación.		

Nombre:	Reg_nodo_de_red		
Descripción:	Crea y Modifica los archivos necesarios del servidor DHCP, de forma que se registran directamente al servidor Proxy, para su ejecución e implementación, según la petición antes hecha por el usuario.		
Tipo de Flujo de Datos:	Externa		
Datos:	Nombre del responsable, dependencia, información física del equipo (MAC address), y la futura ubicación del equipo.		
Origen:	Proceso 3	**Destino:**	Proxy
Comentario:	Dado el caso en que el equipo no forme parte de las subredes ya creadas, se debe crear una nueva subred para tal fin por ejemplo: un nuevo bloque de oficinas, amerita una nueva subred para mayor control.		

Nombre:	Solicita_autorizacion		
Descripción:	Solicitud escrita o verbal hecha por el usuario para obtener la aprobación de un nuevo servicio ó permiso de red.		
Tipo de Flujo de Datos:	Externa		
Datos:	Nombre de Usuario, dependencia, Servicio a establecer.		
Origen:	Proceso 1,3,7	**Destino:**	Coordinación de oficina
Comentario:			

Nombre:	Visto_bueno.
Descripción:	Si la respuesta a la solicitud es positiva, es enviada al

	proceso concerniente, para tal fin		
Tipo de Flujo de Datos:	Externa		
Datos:	Nombre de Usuario, dependencia, Servicio a establecer, y si el equipo ya esta registrado IP del equipo.		
Origen:	Coordinación Aula de informática	**Destino:**	Proceso 1,3,7
Comentario:			

Nombre:	Solicita_correo		
Descripción:	Comunicación escrita entre el usuario y el administrador en el cual realiza la petición de creación de una nueva cuenta de correo.		
Tipo de Flujo de Datos:	Externa		
Datos:	Nombre del responsable, dependencia, visto bueno de coordinación.		
Origen:	Usuario	**Destino:**	Proceso 2.1
Comentario:	Dado el caso en que el usuario ya tenga registrada una cuenta de correo a su nombre, se debe exigir una justificación para la creación de otra cuenta hacia el mismo usuario.		

Nombre:	Crea_correo		
Descripción:	Creación y/o modificación de archivos del sistema operativo por parte del sistema para la creación de una nueva cuenta de correo.		
Tipo de Flujo de Datos:	Externa		
Datos:	Nombre del usuario, login de usuario, visto bueno de coordinación.		
Origen:	Proceso 2.1	**Destino:**	Correo
Comentario:	Dado el caso en que el usuario ya tenga registrada una cuenta de correo a su nombre, se debe exigir una justificación para la creación de otra cuenta hacia el mismo usuario.		

Nombre:	Solicita_grupo
Descripción:	Comunicación escrita entre el usuario y el administrador en el cual realiza la petición de enviar un mismo correo a

	varios destinatarios, muchas veces específicos dentro y/o fuera de la institución.		
Tipo de Flujo de Datos:	Externa		
Datos:	Nombre de Usuario, lista de direcciones, motivo		
Origen:	Usuario	**Destino:**	Proceso 2.3
Comentario:	Se debe dar de alguna forma una justificación para lo cual es necesario la creación de una lista o grupo de direcciones, todo esto con el fin de evitar al máximo el spam o correo indeseado.		

Nombre:	Crea_grupo		
Descripción:	Crea un grupo de correo directamente al sistema que esta referenciado hacia un grupo de direcciones de correo electrónico.		
Tipo de Flujo de Datos:	Externa		
Datos:	Nombre del usuario, lista de correo, motivo y/o justificación.		
Origen:	Proceso 2.3	**Destino:**	Correo
Comentario:	Las listas deben ser claramente especificadas por el usuario		

Nombre:	Asigna_cuotas		
Descripción:	Modifica la configuración de determinado usuario para que tenga un buzón de entrada con espacio limitado debido al uso indebido o exagerado del correo electrónico por parte del usuario.		
Tipo de Flujo de Datos:	Externa		
Datos:	Nombre del usuario, login de usuario, espacio máximo de almacenamiento.		
Origen:	Proceso 2.2	**Destino:**	Correo
Comentario:	Las cuotas pueden ser estandarizadas para todos los usuarios y/o especificas para uno en particular.		
Nombre:	Requiere_subred		
Descripción:	Comunicación escrita entre la coordinación y el administrador en la cual se realiza la petición de creación de una nueva subred, o se presenta la necesidad de expandir la red de datos a una nueva sede o bloque de la institución.		
Tipo de Flujo de Datos:	Externa		
Datos:	Ubicación de la nueva subred.		

Origen:	Coordinación	**Destino:**	Control Subredes
Comentario:	La determinación del rango de direcciones es exclusiva del criterio del administrador del sistema		

Nombre:	Reg_subredes		
Descripción:	Creación y/o modificación de archivos del sistema operativo para la creación de una nueva subred en el servidor.		
Tipo de Flujo de Datos:	Externa		
Datos:	Ubicación de la nueva subred, direccionamiento IP.		
Origen:	Control Subredes	**Destino:**	Proxy
Comentario:	La determinación del rango de direcciones es criterio del administrador del sistema		

Nombre:	Restricción_tipo		
Descripción:	Comunicación escrita entre la coordinación y el administrador en la cual se realiza la creación o eliminación de una restricción de tipo de archivo son el fin de evitar abuso de servicio por parte de los usuarios.		
Tipo de Flujo de Datos:	Externa		
Datos:	Tipo de archivo a restringir o habilitar		
Origen:	Coordinación	**Destino:**	Control de tipos de archivo
Comentario:	La determinación de los tipos de archivo son responsabilidades del administrador apoyadas bajo la aprobación de coordinación.		

Nombre:	Reg_tipo_archivo		
Descripción:	Creación y/o modificación de archivos del sistema operativo para la creación de una nueva restricción de tipo de archivo en el servidor Proxy.		
Tipo de Flujo de Datos:	Externa		
Datos:	Tipo de archivo a restringir o habilitar		
Origen:	Control de tipos de archivo	**Destino:**	Proxy
Comentario:	La determinación de los tipos de archivo son responsabilidades del administrador apoyadas bajo la aprobación de coordinación.		

Nombre:	Reg_mantenimiento		
Descripción:	Operaciones de mantenimiento del caché del Proxy, expansión de tamaño, limpieza de caché.		
Tipo de Flujo de Datos:	Externa		
Datos:	Tamaño nuevo deseado.		
Origen:	Mantenimiento del caché del servidor.	**Destino:**	Proxy
Comentario:	El momento de realizar mantenimiento del caché del Proxy se da cuando el caché ocupa el 70 u 80% del máximo del espacio físico designado para este.		

Nombre:	Pruebas_eventos		
Descripción:	Operaciones manuales de mantenimiento de permiten comprobar la corrección de un problema antes dado o corregirlo.		
Tipo de Flujo de Datos:	Externa		
Datos:	Descripción del problema.		
Origen:	Control de eventos externos.	**Destino:**	Proxy
Comentario:	La operaciones van desde corroborar la conexión física de los enlace, hasta la configuración lógica de la LAN y sus respectivos servicios.		

Nombre:	Evento		
Descripción:	Suceso o acontecimiento inesperado influye en el comportamiento normal de la red.		
Tipo de Flujo de Datos:	Externa		
Datos:	Tamaño nuevo deseado.		
Origen:	Evento externo	**Destino:**	Control de eventos externos
Comentario:	Los eventos son inesperados.		

Nombre:	Solicita_puerto
Descripción:	Petición por parte del usuario para la apertura de un puerto determinado
Tipo de Flujo de	Externa

Datos:			
Datos:	Puerto requerido, motivo y justificación		
Origen:	Usuario	**Destino:**	Administración de puertos de red
Comentario:	El puerto se puede abrir a toda la LAN, a una subred, ó a un equipo específico.		

Nombre:	Reg_puerto		
Descripción:	Modificación del las reglas del firewall, que habilitan el puerto o servicio requerido.		
Tipo de Flujo de Datos:	Externa		
Datos:	Puerto requerido, subred, máscara de subred ó IP del equipo específico dado el caso, usuario.		
Origen:	Administración de puertos de red	**Destino:**	Proxy
Comentario:	Una vez aplicada la regla es necesario reiniciar todo el firewall		

Nombre:	Reg_servicio_especial		
Descripción:	Servicios especiales de firewall como es (NAT, DNAT) que se les brinda a ciertos usuarios medianamente avanzados, teniendo en cuenta su necesidad.		
Tipo de Flujo de Datos:	Externa		
Datos:	IP del equipo, usuario		
Origen:	Usuario	**Destino:**	Administración de servicios especiales.
Comentario:			

Nombre:	Reg_especial		
Descripción:	Modificación del las reglas del firewall, que habilitan el servicio requerido		
Tipo de Flujo de Datos:	Externa		
Datos:	IP del equipo, servicio específico, usuario		
Origen:	Administración de puertos de red	**Destino:**	Proxy
Comentario:	Una vez aplicada la regla es necesario reiniciar todo el firewall		

Nombre:	Suspensión_servicio		
Descripción:	Modificación de las reglas de firewall, que inhabilitan el acceso a la red a un usuario ó usuarios determinados.		
Tipo de Flujo de Datos:	Externa		
Datos:	IP del equipo o de los equipos		
Origen:	Suspensión del servicio	**Destino:**	Proxy.
Comentario:	La inhabilitación del sistema se hace debido a abuso drástico de ancho banda por uno o más equipo, de inhabilita hasta que haya una claridad en lo sucedido y se haga una advertencia.		

Nombre:	tráfico		
Descripción:	Informe de tráfico de red a través de herramientas propias del sistema operativo		
Tipo de Flujo de Datos:	Externa		
Datos:			
Origen:	Proxy	**Destino:**	Monitorización de tráfico
Comentario:	La monitorización permite detectar problemas o eventos internos que podrían requerir inhabilitar a algún equipo.		

Nombre:	Evento_interno		
Descripción:	Acontecimiento que muestra un abuso de recursos, y reporta la dirección del equipo para suspención		
Tipo de Flujo de Datos:	Externa		
Datos:	IP del equipo		
Origen:	Monitorización de tráfico	**Destino:**	Suspensión de servicio
Comentario:			

4.4 REQUERIMIENTOS DEL SISTEMA

La metodología de Proceso Unificado UP fomenta un conjunto de buenas prácticas una de las cuales es la gestión de requisitos, además el UP acepta el cambio en los requisitos como un motor fundamental del proyecto.

En el UP los requisitos se clasifican de acuerdo con el modelo FURPS+ un útil nemotécnico que significa los siguientes cinco tipos de requisitos.

- **Functional** (Funcional)
  Aquí se describirán las características principales del sistema, las capacidades que este pueda tener y la seguridad que debe infundir.

- **Usability** (Facilidad de uso)
  Descripción de factores humanos, ayuda y documentación.

- **Reliability** (Fiabilidad)
  Frecuencia de fallos, capacidad de recuperación de un fallo y grado de previsión.

- **Performance** (Rendimiento)
  Tiempos de respuesta, productividad, precisión, disponibilidad, uso de los recursos.

- **Supportability** (Soporte)
  Adaptabilidad, facilidad de mantenimiento, internacionalización.

- **Implementación**
  Limitación de recursos, lenguajes y herramientas, hardware.

- **Interfaz**
  Restricciones impuestas para la interacción con sistemas externos.

- **Operaciones**
  Gestión del sistema en su puesta en marcha.

- **Legales**
  Licencias.

4.4.1 Requerimientos funcionales Los casos de uso son requisitos; ante todo son requisitos funcionales que indican que hará el sistema. En términos de los tipos de requisitos FURPS+, los casos de uso se refieren fundamentalmente a la “F” (funcional o de comportamiento), pero también pueden utilizarse para otros tipos, especialmente cuando esos otros tipos están estrechamente relacionados con un caso de uso. En el UP, los casos de uso son el mecanismo principal que se recomienda para su descubrimiento y definición. Los casos de uso definen una promesa o contrato de la manera en la que se comporta un sistema.

En otras palabras los casos de uso son requisitos aunque no todos los requisitos. Algunos piensan en requisitos sólo como listas de características y funciones de la forma “el sistema deberá hacer…”, No es así, y una idea clave de los casos de uso es (por lo general) reducir la importancia o el uso de listas de características detalladas al estilo antiguo y más bien, escribir casos de uso para los requisitos funcionales.

Los casos de uso son documentos de texto, no diagramas, y el modelado de casos de uso es, sobre todo, una acción de escribir texto, no dibujar. Sin embargo, UML, define un diagrama de casos de uso para ilustrar los nombres de casos de uso y actores, y sus relaciones.[1]

4.4.1.1 Caso de Uso UC1: Controlar Usuarios.

Actor Principal: Administrador de red
Personal Involucrado e intereses:

- **Administrador de red:** Quiere tener un control total sobre los usuarios que van a ser beneficiados por el sistema, y facilitar la prestación de sus servicios, a la vez de impedir que terceros abusen de un recurso propio de la institución.
- **Usuario: Quiere** aprovechar los servicios de red ofrecidos en la Institución para tener nuevas formas de acceso a la información, y ser así un elemento fundamental del sistema, para lo cual deberá estar registrado en este.
- **Precondiciones:** El administrador se identifica y se autentica. El usuario debe presentar algún documento que lo acredite como vinculado de la institución (cedula o carné laboral).
- **Garantías de Éxito (Postcondiciones):** El usuario quedará registrado permanentemente en el sistema para cualquier servicio que este último preste.

Escenario principal de éxito (ó Flujo Básico):

1. El usuario llega a la oficina principal de administración de Internet con su respectiva identificación, ya sea cédula o carné de la institución.
2. El administrador de red comienza la creación o modificación de un usuario, a través del sistema en la sección de control de usuarios.
3. El administrador de red introduce la información correspondiente al usuario, datos personales, y laborales.
4. El sistema brinda un resumen de la información del usuario a ser creada o modificada, para confirmación.
5. El administrador de red confirma la información mostrada por el sistema.

[1] UML y Patrones Craig Larman 2da Edición

6. El sistema crea o modifica el registro pertinente.
7. El sistema notifica al administrador y confirma el proceso realizado.
8. El administrador notifica al usuario y comprueba la creación o modificación de la cuenta del usuario.
9. El usuario crea su contraseña y la registra en el sistema.

Extensiones (o flujos Alternativos):

***a.** En cualquier momento el sistema falla:

1. El sistema reporta el error al administrador.
2. El administrador reinicia el sistema, inicia la sesión, y reinicia el proceso de control y manejo de usuarios.

***b.** En cualquier momento el Administrador puede cancelar la creación del sitio:

1. El administrador cancela, y/o elimina cualquier información ya registrada.

***c.** En cualquier momento el usuario puede cancelar su petición de servicio:

1. El administrador cancela, y/o elimina cualquier información ya registrada.

3a. El identificador del usuario ya existe:

1. El sistema informa sobre la existencia del usuario e impide continuar con el proceso.
2. El sistema brinda todas las opciones que el usuario ya registrado puede acceder.

6a. El sistema reporta error de conexión a la base de datos:

1. El sistema sugiere al administrador revisar la conexión a la base de datos.
2. El sistema cancela el registro y vuelve a iniciar el proceso.

7a. El registro tiene información errónea o incorrecta:

1. El administrador eliminar totalmente, ó edita la información de cualquier registro antes hecho.
2. El administrador vuelve a iniciar un nuevo proceso de registro, guarda la información modificada del registro, o bien cancela su operación.

Requisitos especiales:

- Tiempo de respuesta para la creación o modificación de una cuenta de usuario de menos de 1 minuto en el 90% de las veces.

Frecuencia: Frecuente.

4.4.1.2 Caso de Uso UC2: Controlar Infraestructura física.

Actor Principal: Administrador de red
Personal Involucrado e intereses:

- **Administrador de red:** Quiere que la LAN además de darle una dirección de red a cada equipo conectado a esta, brinde también la posibilidad de tener un orden a través de la infraestructura de la institución, ya sean sedes, bloque o edificios, piso, o incluso nombres de oficinas y realizar así una correcta distribución de subredes en un futuro.
- **Precondiciones:** El administrador se identifica y se autentica, el direccionamiento que el administrador elija para su LAN, debe prever las necesidades del futuro.

- **Garantías de Éxito (Postcondiciones):** El orden que el Administrador dé a la infraestructura deberá ser capaz de tener vigencia en el futuro, este se relaciona directamente con el direccionamiento lógico de cada host o equipo conectado a la LAN.

Escenario principal de éxito (ó Flujo Básico):

1. El administrador de red comienza la administración de la infraestructura física de la institución en el sistema.
2. El administrador de red introduce la información sobre las sedes, bloques, u oficinas dentro de la institución.
3. El sistema brinda un resumen de la información registrada ó modificada, para confirmación.
4. El administrador de red confirma la información mostrada por el sistema.
5. El sistema crea o modifica el registro pertinente.
6. El sistema notifica al administrador y confirma el proceso realizado.
7. El administrador comprueba la creación o modificación de la infraestructura procesada.
8. El administrador es capaz ahora de asignar nuevos equipos o hosts a la nueva ubicación.

Extensiones (o flujos Alternativos):

***a.** En cualquier momento el sistema falla:

1. El sistema reporta el error al administrador.
2. El administrador reinicia el sistema, inicia la sesión, y reinicia el proceso de control de infraestructura.

5a. El sistema reporta error de conexión a la base de datos:
1. El sistema sugiere al administrador revisar la conexión a la base de datos.
2. El sistema cancela el registro y vuelve a iniciar el proceso.

7a. El registro tiene información errónea o incorrecta:

1. El administrador eliminar totalmente, ó edita la información de cualquier registro antes hecho.
2. El administrador vuelve a iniciar un nuevo proceso administración de infraestructura, guarda la información modificada del registro, o bien cancela su operación.

Requisitos especiales:
- Tiempo de respuesta para la administración de cualquier proceso de infraestructura, menos de 2 minutos en el 90% de las veces.

Frecuencia: Poco usual.

4.4.1.3 Caso de Uso UC3: Administrar Publicaciones Web.

Actor Principal: Administrador de red
Personal Involucrado e intereses:

- **Administrador de red:** Quiere brindar a usuarios autorizados la posibilidad de que realicen sus publicaciones por si mismos, liberar el trabajo manual y directo al servidor, y mantener la información más actualizada ya que cada usuario autorizado se encargaría de su determinada sección.
- **Compañía y/o Institución:** Quiere que la academia llegue a los estudiantes por medio de nuevas formas, y metodologías, esta muy interesada en la educación virtual, en el empleo de la tecnología para bien de la educación.
- **Usuario de publicación:** Quiere tener control sobre la información que desea publicar, poder actualizar los contenidos de su sección, y/o hacer alguna modificación o corrección de los contenidos ya publicados.

- **Precondiciones:** El administrador se identifica y se autentica. El usuario debe estar registrado como usuario de correo electrónico para también identificarse y autenticarse al sistema.
- **Garantías de Éxito (Postcondiciones):** Se crea el espacio físico y lógico para la publicación en el servidor, se asignan los respectivos permisos al usuario.

Escenario principal de éxito (ó Flujo Básico):

1. El usuario llega a la oficina principal de administración de Internet con su respectiva identificación, ya sea cédula o carné de la institución, y con el respectivo visto bueno de coordinación.
2. El administrador de red comienza la creación de un nuevo sitio, en el servidor de publicación Web a través del sistema.
3. El administrador de red introduce la información correspondiente al nuevo sitio con un identificador dado por el sistema. El identificador será útil al momento de crear la URL del respectivo sitio.
4. El sistema brinda un resumen del sitio Web que se ha de crear, para confirmación.
5. El administrador de red confirma la información mostrada por el sistema.
6. El sistema realiza la creación del nuevo sitio de publicación a la vez que actualiza los datos del usuario, y el propósito del sitio.
7. El sistema notifica al administrador y confirma la creación del nuevo sitio Web, brindando la posibilidad de entrar directamente desde algún tipo de enlace.
8. El administrador notifica al usuario y comprueba el funcionamiento del sitio Web creado, accediendo a el a través del Navegador.
9. El usuario crea su página o sitio Web a través de herramientas propias del sistema.
10. El usuario guarda su información a través del sistema.
11. El usuario y la comunidad en general, observa los resultados directamente en el sitio Web creado.

Extensiones (o flujos Alternativos):

***a.** En cualquier momento el sistema falla:

1. El sistema reporta el error al administrador.
2. El administrador reinicia el sistema, inicia la sesión, y reinicia el proceso de creación de un nuevo sitio, si aparece información parcial registrada, elimina la información parcial, y reinicia la creación del sitio Web.

***b.** En cualquier momento el Administrador puede cancelar la creación del sitio:

1. El administrador cancela, y/o elimina cualquier información ya registrada.

***c.** En cualquier momento el usuario puede cancelar su petición de servicio:

1. El administrador cancela, y/o elimina cualquier información ya registrada.

3a. No existe el identificador del usuario o es inválido:

1. El sistema señala error e impide continuar con la creación del sitio.
2. El sistema asiste en que se debe hacer para continuar con el proceso.
2. El sistema brinda la posibilidad de crear el sitio Web bajo la responsabilidad de otro usuario.

6a. El sistema reporta error de conexión a la base de datos:

1. El sistema sugiere al administrador revisar la conexión a la base de datos.
2. El sistema cancela el registro y vuelve a iniciar el proceso.

7a. El registro tiene información errónea o la URL está mal asignada:

1. El administrador elimina totalmente, ó edita la información de cualquier registro antes hecho.
2. El administrador vuelve a iniciar un nuevo proceso de registro, registra la información modificada del registro, o bien cancela su operación.

9-11a. El usuario no puede publicar su Sitio Web:

1. El usuario escribe su solicitud vía e-mail a la dirección de soporte del sistema.
2. El Administrador es notificado por el sistema y procede a revisar los correspondientes permisos.
3. El Administrador regresa un e-mail dando solución al problema del usuario.
4. El usuario reinicia el proceso de publicación Web.

Requisitos especiales:

- Tiempo de respuesta para la creación del nuevo sitio Web menos de 1 minuto en el 90% de las veces.

Frecuencia: regular.

4.4.1.4 Caso de Uso UC4: Administrar Correo Electrónico.

Actor Principal: Administrador de red
Personal Involucrado e intereses:

- **Administrador de red:** Quiere brindar a usuarios autorizados por la compañía o institución mediante la respectiva dependencia, la posibilidad de tener una cuenta y buzón de correo electrónico, para uso personal, de la forma más eficiente y rápida posible, tanto para la administración, como para el manejo del usuario.
- **Compañía y/o Institución:** Quiere que la institución se represente y llegue a la sociedad a través de nuevos medios de comunicación, así como también, brindar un servicio mas a todos los usuarios adscritos a esta.
- **Usuario de correo:** Quiere tener control sobre la información recibe, poder enviar y recibir correos con toda seguridad, sin problemas de virus ó correos basura (SPAM), tener un acceso rápido, eficiente y amigable a través de una ágil interfaz gráfica que permita la mayor interactividad posible.
- **Precondiciones:** El administrador se identifica y se autentica. El usuario debe pertenecer de alguna forma a la institución y tener el visto bueno de la dependencia a cargo.
- **Garantías de Éxito (Postcondiciones):** Se crea el espacio físico y lógico para el almacenamiento del buzón de correo y su directorio en el servidor, se asignan los respectivos permisos al usuario.

Escenario principal de éxito (ó Flujo Básico):

1. El usuario llega a la oficina principal de administración de Internet con su respectiva identificación, ya sea cédula o carné de la institución, y con el respectivo visto bueno de coordinación.
2. El administrador de red comienza la creación de un nuevo correo electrónico, en el servidor de correo electrónico a través del sistema.
3. El administrador de red introduce la información correspondiente al nuevo correo electrónico incluyendo la información personal del usuario lo cual le permitirá obtener más servicios, cuyo identificador es dado por su documento de identificación (carné o cedula). El identificador será útil al momento de brindar otros servicios al mismo usuario.
4. El sistema le pide la contraseña deseada al usuario.
5. El usuario digita la contraseña y su respectiva confirmación.
6. El sistema brinda un resumen del correo electrónico que se ha de crear, para confirmación.
7. El administrador de red confirma la información mostrada por el sistema.
8. El sistema realiza la creación del nuevo correo electrónico a la vez que actualiza los datos personales del usuario.
9. El sistema notifica al administrador y confirma la creación del nuevo correo electrónico.
10. El administrador notifica al usuario y comprueba el funcionamiento del correo electrónico, accediendo a él a través del Navegador.

11. El usuario ingresa con su contraseña a su buzón de correo electrónico.
12. El usuario puede enviar, recibir, guardar sus mensajes de correo, crear su libreta de direcciones, o eliminar información inútil de su buzón, a través de la interfaz del sistema de correo.

Extensiones (o flujos Alternativos):

***a.** En cualquier momento el sistema falla:

1. El sistema reporta el error al administrador.
2. El administrador reinicia el sistema, inicia la sesión, y reinicia el proceso de creación de un nuevo correo electrónico, si aparece información parcial registrada, elimina la información parcial, y reinicia la creación del buzón de correo.

***b.** En cualquier momento el Administrador puede cancelar la creación de la cuenta de correo:

1. El administrador cancela, y/o elimina cualquier información ya registrada.

***c.** En cualquier momento el usuario puede cancelar su petición de servicio:

1. El administrador cancela, y/o elimina cualquier información ya registrada.

3a. El usuario ya existe:

1. El sistema señala error e impide continuar con la creación de la cuenta de correo.
2. El sistema asiste en que se debe hacer para continuar con el proceso.
3. El sistema brinda la posibilidad de crear el correo electrónico bajo la responsabilidad de otro usuario, o bien revisar la información del usuario reportado como existente para alguna modificación, ó para la asignación de más de una cuenta de correo al mismo usuario.

3b. Faltan datos por llenar:

1. El sistema señala error e impide continuar con la creación del correo.
2. El sistema muestra los datos faltantes o por llenar que son de vital importancia para el proceso.

3c. login de usuario ya existe:

1. El sistema señala error e impide continuar con la creación del correo.
2. El sistema informa la existencia del login del usuario y exige el cambio de este para continuar el proceso.
3. El usuario cambia su login.

5a. Las contraseñas no coinciden:

1. El sistema informa de tal acontecimiento.
2. El sistema vuelve a pedir la contraseña y su respectiva confirmación.
3. El usuario vuelve a escribir su contraseña y su confirmación.

5b. Contraseña muy corta:

1. El sistema advierte sobre la baja seguridad de la contraseña ingresada por el usuario.
2. El usuario decide sobre si continuar con esta contraseña o cambiarla por otra.

7a. El sistema reporta error de conexión a la base de datos:

1. El sistema sugiere al administrador revisar la conexión a la base de datos.
2. El sistema cancela el registro y vuelve a iniciar el proceso.

7b. El registro tiene información errónea o la dirección de correo está mal asignada:

1. El administrador elimina totalmente, ó edita la información de cualquier registro antes hecho.
2. El administrador vuelve a iniciar un nuevo proceso de registro, registra la información modificada del registro, o bien cancela su operación.

11-12a. El usuario no puede ingresar o utilizar su cuenta de correo:

1. El usuario informa su inconveniente al administrador.
2. El Administrador procede a revisar los correspondientes permisos.
3. El Administrador da una solución al problema del usuario.
4. El usuario reinicia el proceso de ingreso o utilización del buzón de correo.

Requisitos especiales:

- Tiempo de respuesta para la creación del nuevo correo electrónico, menos de 2 minutos el 90% de las veces.

Frecuencia: continuo.

4.4.1.5 Caso de Uso UC5: Administrar Nodos o puntos de Red.

Actor Principal: Administrador de red
Personal Involucrado e intereses:

- **Administrador de red:** Quiere registros precisos, rápidos y sin errores de tipeo de datos, ya que perjudicaría el orden global de la red como tal.
- **Compañía y/o Institución:** Quiere satisfacer los intereses de sus usuarios, fomentar la cobertura a todo el campus educativo, promover con mayor control y facilidad la creación de nuevos puntos de red, tener información concreta sobre el crecimiento y/o comportamiento de la red a través del tiempo.
- **Precondiciones:** El administrador se identifica y se autentica.
- **Garantías de Éxito (Postcondiciones):** Se registra en nuevo punto o nodo de red, se inserta el nodo de manera ordenada teniendo en cuenta la ubicación física en la compañía y/o institución ya que esto influye en la asignación de la dirección de red.

Escenario principal de éxito (ó Flujo Básico):

1. El Usuario llega a la oficina principal con su pertinente identificación, ya sea cedula, ó carné de la institución, y con el respectivo visto bueno de coordinación.
2. El administrador de red comienza un nuevo registro del nodo y/o del equipo
3. El administrador de red introduce la información correspondiente del equipo con un identificador dado por el sistema. La dirección de red se calcula dependiendo de la ubicación física del equipo anteriormente dada.
4. El sistema brinda un resumen del registro que se llevara a cabo, para confirmación.
5. El administrador de red confirma los datos a registrar.
6. El sistema realiza la creación del nuevo nodo de red actualizando también el inventario de equipos y las estadísticas concernientes.
7. El sistema notifica al administrador y confirma la creación del nuevo nodo de red.
8. El administrador notifica al usuario y comprueba el funcionamiento del equipo conectado a la red.
9. El usuario verifica el funcionamiento del nuevo nodo.

Extensiones (o flujos Alternativos):

***a.** En cualquier momento el sistema falla:

1. El sistema reporta el error al administrador.
2. El administrador reinicia el sistema, inicia la sesión, y reinicia el proceso de registro, si aparece información parcial registrada, elimina la información parcial, y reinicia el proceso de registro.

***b.** En cualquier momento el Administrador puede cancelar el registro.

1. El administrador cancela, y/o elimina cualquier información ya registrada.

***c.** En cualquier momento el usuario puede cancelar su petición de servicio:

1. El administrador cancela, y/o elimina cualquier información ya registrada.

3a. No existe la ubicación:

1. El sistema señala error e impide continuar con el proceso de registro hasta que se realice primero el registro del lugar físico del nuevo equipo a registrar.
2. El sistema informa que se debe hacer para continuar con el proceso.
3. El sistema brinda la posibilidad de ubicar el equipo en los lugares ya conocidos por este.

3b. No existe el usuario:

1. El sistema señala error e impide continuar con el proceso de registro hasta que se realice primero el registro del usuario y sus respectivos datos personales, quien será responsable del nuevo nodo de red.
2. El sistema informa que se debe hacer para continuar con el proceso.
3. El sistema brinda la posibilidad de asignar como responsable a usuarios ya conocidos y registrados por este.

5a. El administrador de red no confirma los datos a registrar.

1. El sistema brinda la posibilidad de editar la información antes digitada.
2. El sistema brinda la posibilidad de cancelar el registro completamente.

6a. El sistema reporta error de conexión a la base de datos:

1. El sistema sugiere al administrador revisar la conexión a la base de datos.
2. El sistema cancela el registro y vuelve a iniciar el proceso.

7a. El registro tiene información errónea:

1. El administrador eliminar totalmente, ó editar la información de cualquier registro antes hecho.
2. El administrador vuelve a iniciar un nuevo proceso de registro, registra la información modificada del registro, o bien cancela su operación.

8a. El equipo no se conecta a la red:

1. El administrador verifica a través del sistema la actividad física del equipo.
2. El administrador reiniciar el proceso de prueba de conexión (**Paso 8**).

8b. El equipo tiene actividad pero no tiene servicio:

1. El administrador verifica manualmente la configuración del equipo sin servicio.

Requisitos especiales:

- Tiempo de respuesta para la creación del nuevo punto de red, menos de 1 minuto el 90% de las veces.

Frecuencia: siempre continuo.

4.4.1.6 Caso de Uso UC6: Controlar ancho de banda.

Actor Principal: Administrador de red
Personal Involucrado e intereses:

- **Administrador de red:** Quiere brindar a la compañía o institución, la posibilidad de tener un control sobre el ancho de banda de la red, con el fin de llevar a cabo cualquier actividad de tipo académico - administrativo que necesite tener una velocidad de Internet muy superior a cualquier otro nodo de la red.

- **Compañía y/o Institución:** Quiere dar la posibilidad de crear eventos, que demanden altos recursos tecnológicos. Que utilicen nuevos medios de comunicación, así como también, brindar un servicio más eficiente a un evento determinado.

- **Usuario:** Quiere tener la posibilidad de solicitar este tipo de servicio para alguna eventualidad ya sea con fines académicos y/o administrativos de la institución.
- **Precondiciones:** El administrador se identifica y se autentica. El usuario se identifica y autentica directamente con su cuenta de correo electrónico, de lo contrario debe demostrar la pertenencia a la institución, para almacenar la información personal, el equipo a limitar o permitir un ancho de banda fijo, debe estar registrado como host dentro de la red.

- **Garantías de Éxito (Postcondiciones):** Se realiza la configuración lógica del servidor respectivo verificando los cambios realizados, y se asignan los respectivos permisos a la(s) máquina(s) o equipo(s) del usuario.

Escenario principal de éxito (ó Flujo Básico):

1. El usuario llega a la oficina principal de administración de Internet con su respectiva identificación, ya sea cédula o carné de la institución.
2. El administrador de red comienza el proceso de una nueva asignación de ancho de banda al equipo o equipos solicitados por el usuario, a través de la interfaz del sistema.

3. El administrador de red introduce la información necesaria para la nueva asignación del permiso de ancho de banda, teniendo en cuenta la información lógica del equipo y el responsable de este.
4. El sistema brinda un resumen del permiso de ancho de banda que se ha de asignar, para confirmación del administrador.
5. El administrador de red confirma la información mostrada por el sistema.
6. El sistema realiza la asignación del ancho de banda requerido a la vez que crea el tiempo de vigencia de dicho permiso.
7. El sistema notifica al administrador y confirma la asignación del nuevo permiso.
8. El administrador notifica al usuario y comprueba el funcionamiento del equipo o equipos cubiertos por el nuevo permiso, accediendo a la red y haciendo las pruebas concernientes propias de cada caso.
9. El usuario utiliza el nuevo permiso para un determinado evento.
10. Pasado el tiempo de vigencia del permiso, el sistema elimina el permiso y vuelve a su estado inicial.

Extensiones (o flujos Alternativos):

***a.** En cualquier momento el sistema falla:

1. El sistema reporta el error al administrador.
2. El administrador reinicia el sistema, inicia la sesión, y reinicia el proceso de asignación de permisos de ancho de banda, si aparece información parcial registrada, elimina la información parcial, y reinicia el proceso.

***b.** En cualquier momento el Administrador puede cancelar la creación de la cuenta de correo:

1. El administrador cancela, y/o elimina cualquier información ya registrada.

***c.** En cualquier momento el usuario puede cancelar su petición de servicio:

1. El administrador cancela, y/o elimina cualquier información ya registrada.

3a. No existe el equipo:

1. El sistema señala error e impide continuar con el proceso de registro hasta que se realice primero el registro lógico del nuevo equipo.
2. El sistema informa que se debe hacer para continuar con el proceso.
3. El sistema brinda la posibilidad de continuar el proceso con un equipo ya existente y registrado en el sistema.

3b. No existe el usuario:

1. El sistema señala error e impide continuar con el proceso de registro hasta que se realice primero el registro del usuario y sus respectivos datos personales, quien sería el responsable del equipo o equipos que recibirán el permiso de ancho de banda.

5a. El sistema reporta error de conexión a la base de datos:

1. El sistema sugiere al administrador revisar la conexión a la base de datos.
2. El sistema cancela el registro y vuelve a iniciar el proceso.

5b. El registro tiene información errónea o la configuración del permiso está mal asignada:

1. El administrador elimina totalmente, ó edita la información de cualquier registro antes hecho.
2. El administrador vuelve a iniciar un nuevo proceso de asignación de permisos de ancho de banda, registra la información modificada del registro, o bien cancela su operación.

7-9a. El usuario no observa ningún cambio en la velocidad:

1. El usuario informa su inconveniente al administrador.
2. El Administrador procede a revisar los correspondientes permisos y procesos del sistema.
3. El Administrador da una solución al problema del usuario.
4. El usuario reinicia el proceso de prueba y verificación.

7-9b. El usuario observa poco cambio en la velocidad:

1. El usuario informa su inconveniente al administrador.
2. El Administrador procede a modificar el permiso para darle mayor prioridad.
3. El Administrador da una solución al problema del usuario.
4. El usuario reinicia el proceso de prueba y verificación.

10a. El sistema no regresa el permiso dado a su punto inicial:

1. El administrador revisa la configuración del permiso de asignación de ancho de banda, y verifica sus datos.
2. El administrador prueba de nuevo el permiso.

10b. El sistema no elimina el permiso:

1. El administrador verifica los permisos del sistema operativo sobre el permiso de red y reinicia el sistema.

Requisitos especiales:

- Tiempo de respuesta para una nueva asignación de ancho de banda de menos de 1 minuto el 95% de las veces.

Frecuencia: regular.

4.4.1.7 Caso de Uso UC7: Administrar Servidor Proxy.

Actor Principal: Administrador de red
Personal Involucrado e intereses:

- **Administrador de red:** Quiere tener el mayor control posible sobre la red, y el tipo de archivos que esta va a soportar, quiere controlar el acceso de ciertos tipos de archivos (videos, música, imágenes de CD o DVD), que representan una gran congestión de la red debido a su gran tamaño o a las grandes exigencias frente al ancho de banda de la red para su ejecución, y que muchas veces no están ligados a los objetivos que tiene la institución como tal, quiere también controlar el espacio físico del caché del servidor Proxy, estar al tanto del espacio que este está utilizando y realizar limpieza del caché cuando el tamaño del caché, supera el 80% del máximo permitido.
- **Precondiciones:** El administrador se identifica y se autentica. Cualquier modificación en la configuración del servidor Proxy, será aplicado a toda la red interna, y por concerniente a todos sus equipos o nodos conectados a la red, sin discriminación alguna, la administración del servidor Proxy de divide en otros subprocesos.
- **Garantías de Éxito (Postcondiciones):** Se realiza la configuración lógica del servidor respectivo verificando los cambios realizados.

Escenario principal de éxito (ó Flujo Básico):

1. El administrador en cualquier momento ingresa al sistema para monitorizar el estado del servidor Proxy, bien sea para observar el registro de acceso de los usuarios conectados, verificar el tamaño del caché y realizar tareas de mantenimiento de este, así como para controlar el acceso a ciertos tipos de archivos (audio - video), o bien dar acceso a Internet a través del Proxy a nuevas redes.
2. El sistema brinda las diferentes opciones del servidor Proxy.
3. El administrador selecciona la opción deseada y procede a realizar el proceso correspondiente.
4. El administrador ingresa los datos requeridos por el proceso seleccionado.

5. El sistema presenta un resumen de datos a procesar.
6. El administrador de red confirma la información mostrada por el sistema.
7. El sistema realiza la operación especificada.
8. El sistema notifica al administrador y confirma la correcta ejecución del proceso especificado.
9. El Administrador verifica y comprueba el cambio hecho al servidor Proxy.
10. El administrador sigue monitorizando (**Paso 1)** ó sale del sistema.

Extensiones (o flujos Alternativos):

***a.** En cualquier momento el sistema falla:

1. El sistema reporta el error al administrador.
2. El administrador reinicia el sistema, inicia la sesión, y reinicia el proceso monitorización del servidor Proxy, si aparece información parcial registrada, elimina la información parcial, y reinicia el proceso.

***b.** En cualquier momento el Administrador puede cancelar el proceso de monitorización:

1. El administrador cancela, y/o elimina cualquier información ya registrada.

4.4.1.8 Caso de Uso UC7.1: Control de Subredes de Proxy

Actor Principal: Administrador de red
Personal Involucrado e intereses:

- **Administrador de red:** Quiere una vez que la nueva subred este soportada por una red o interfaz de red del sistema operativo, esta tendrá que ser reportada al servidor Proxy, para que tenga acceso al Proxy de forma transparente y de allí todos herede los respectivos servicios de red.
- **Precondiciones:** El administrador se identifica y se autentica. Cualquier modificación en la configuración del servidor Proxy, será aplicado a toda la red interna, y por concerniente a todos sus equipos o nodos conectados a la red.
- **Garantías de Éxito (Postcondiciones):** Se realiza la configuración lógica de subredes en el servidor Proxy respectivo verificando los cambios realizados.

Escenario principal de éxito (ó Flujo Básico):

1. El administrador una vez confirme que la nueva subred estará soportada por una interfaz de red en el equipo servidor, procede a dar acceso a Proxy a determinada subred en el sistema.

2. El administrador ingresa la información necesaria para brindar acceso a la nueva subred.
3. El sistema presenta un resumen de datos a registrar.
4. El administrador de red confirma la información mostrada por el sistema.
5. El sistema realiza el registro especificado.
6. El sistema notifica al administrador y confirma la correcta ejecución del proceso especificado.
7. El Administrador verifica y comprueba el cambio hecho al servidor Proxy.

Extensiones (o flujos Alternativos):

***a.** En cualquier momento el sistema falla:

1. El sistema reporta el error al administrador.
2. El administrador reinicia el sistema, inicia la sesión, y reinicia el proceso de administrar y controlar el acceso a las subredes de la LAN.

***b.** En cualquier momento el Administrador puede cancelar el proceso de otorgamiento de acceso a Proxy a las determinadas subredes.

1. El administrador cancela, y/o elimina cualquier información ya registrada.

7a. No se presenta ningún cambio en la configuración interna del Servidor Proxy:

1. El administrador verifica la actividad de los procesos del servidor Proxy en el sistema operativo.
2. El administrador reinicia los procesos concernientes al Proxy.
3. El administrador reinicia el proceso de control de subredes del servidor Proxy
4. El administrador verifica cambios realizados.

Requisitos especiales:

- Tiempo de respuesta para otorgar acceso a Proxy a una nueva subred, menos de 2 minutos el 90 % de las veces.

Frecuencia: muy poco usual.

4.4.1.9 Caso de Uso UC7.2: Controlar Tipos de Archivo

Actor Principal: Administrador de red
Personal Involucrado e intereses:

- **Administrador de red:** Quiere tener control sobre los tipos de archivos que se van a permitir o a restringir en la LAN, ya sea por que son archivos que por lo general poseen un gran tamaño como (Videos, imágenes de CD, entre otros.), así como también por ser archivos que requieran grandes recursos o un gran ancho de banda para su ejecución como video en vivo e incluso alguna emisoras de Internet.
- **Precondiciones:** El administrador se identifica y se autentica. Cualquier modificación en la configuración del servidor Proxy, será aplicado a toda la red interna, y por concerniente a todos sus equipos o nodos conectados a la red.
- **Garantías de Éxito (Postcondiciones):** Se realiza la configuración lógica del control de tipos de archivo en el servidor Proxy respectivo verificando los cambios realizados.

Escenario principal de éxito (ó Flujo Básico):

1. El administrador decide que tipo de archivo va a restringir y procede a usar el sistema.
2. El administrador ingresa la información necesaria para restringir un nuevo tipo o clase de archivo.
3. El sistema presenta un resumen de datos a registrar.
4. El administrador de red confirma la información mostrada por el sistema.
5. El sistema realiza la modificación necesaria al archivo de configuración principal del servidor Proxy.
6. El sistema notifica al administrador y confirma la correcta denegación de acceso al tipo de archivo seleccionado.
7. El Administrador verifica y comprueba el cambio hecho al servidor Proxy.

Extensiones (o flujos Alternativos):
***a.** En cualquier momento el sistema falla:

1. El sistema reporta el error al administrador.
2. El administrador reinicia el sistema, inicia la sesión, y reinicia el proceso de restricción de tipos de archivo en el Proxy.

***b.** En cualquier momento el Administrador puede cancelar el proceso de restricción de tipos de archivo o revertir los cambios antes hechos.

1. El administrador cancela, y/o elimina cualquier información ya registrada.

7a. No se presenta ningún cambio en la configuración interna del Servidor Proxy:

1. El administrador verifica la actividad de los procesos del servidor Proxy en el sistema operativo.
2. El administrador reinicia los procesos concernientes al Proxy.
3. El administrador reinicia el proceso de control de tipos de archivos del servidor Proxy.
4. El administrador verifica cambios realizados.

Requisitos especiales:

- Tiempo de respuesta para restringir un nuevo tipo de archivo en el Proxy, menos de 1 minutos el 90 % de las veces.

Frecuencia: muy poco usual.

4.4.1.10 Caso de Uso UC7.3: Mantenimiento del caché del servidor

Actor Principal: Administrador de red
Personal Involucrado e intereses:

- **Administrador de red:** Se preocupa por brindar los servicios de red, en especial Internet, en mayor tiempo posible, sin interrupciones y lo más eficiente posible. Quiere tener un caché no muy grande para que la máquina sea capaz de realizar búsquedas más fáciles, así como también de no saturar el espacio físico, o almacenamiento secundario del la máquina servidora.
- **Precondiciones:** El administrador se identifica y se autentica. Cualquier modificación en la configuración del servidor Proxy, será aplicado a toda la red interna, y por concerniente a todos sus equipos o nodos conectados a la red.
- **Garantías de Éxito (Postcondiciones):** Se comprueba el estado del servidor Proxy a través de sus archivos logs así como también el espacio físico ocupado por el caché del servidor, este debe estar vacío.

Escenario principal de éxito (ó Flujo Básico):

1. El administrador ingresa al sistema y monitoriza en estado de almacenamiento del caché dentro de la partición o directorio asignado.
2. El administrador selecciona las opciones pertinentes para la limpieza del Proxy.
3. El sistema presenta un informe de tareas a procesar.
4. El administrador de red confirma la información mostrada por el sistema.
5. El sistema realiza el proceso especificado.
6. El sistema notifica al administrador y confirma la correcta ejecución del proceso.

7. El Administrador verifica y comprueba el cambio hecho al servidor Proxy.

Extensiones (o flujos Alternativos):

***a.** En cualquier momento el sistema falla:

1. El sistema reporta el error al administrador.
2. El administrador reinicia el sistema, inicia la sesión, y reinicia el proceso mantenimiento del caché del servidor Proxy.

2a. El administrador observa que no es necesario un mantenimiento del caché en ese momento.

1. El administrador termina el proceso de monitorización y sale del sistema.

Requisitos especiales:

- Tiempo de respuesta para limpieza y mantenimiento general del caché del servidor Proxy de no más de 10 min. en el mayor de los casos, o dependiendo del espacio total ocupado por el caché en el servidor.

Frecuencia: poco usual.

4.4.1.11 Caso de Uso UC7.4: Control de Eventos Externos

Actor Principal: Administrador de red
Personal Involucrado e intereses:

- **Administrador de red:** Quiere realizar operaciones de monitorización o revisiones de estado ya sea de un solo equipo, subredes, redes o la LAN entera, en cualquier momento o cuando exista un evento que impida el servicio a determinado o determinados equipos.
- **Precondiciones:** El administrador se identifica y se autentica. Cualquier modificación en la configuración del servidor Proxy, será aplicado a toda la red interna, y por concerniente a todos sus equipos o nodos conectados a la red.
- **Garantías de Éxito (Postcondiciones):** Se realiza la configuración lógica del control de tipos de archivo en el servidor Proxy respectivo verificando los cambios realizados.

Escenario principal de éxito (ó Flujo Básico):

1. El administrador ingresa a monitorizar el estado del servidor Proxy.
2. El administrador ingresa las opciones necesarias para monitorizar la LAN completa, o algún equipo en específico.
3. El sistema presenta información en tiempo real, tanto de la actividad del equipo, como del acceso que este tiene.
4. El administrador analiza la información mostrada por el sistema.
5. El administrador decide que procedimiento seguir, y/o puede utilizar cualquier otro módulo del sistema para tal fin.

Extensiones (o flujos Alternativos):

***a.** En cualquier momento el sistema falla:

1. El sistema reporta el error al administrador.
2. El administrador reinicia el sistema, inicia la sesión, y reinicia el proceso de monitorización de la LAN en el servidor Proxy.

***b.** En cualquier momento el Administrador puede salir del proceso de monitorización:

1. El administrador cancela el proceso de monitorización y regresa al sistema principal.

3a. El sistema no muestra ninguna información del equipo o equipos seleccionados:

1. El administrador debe optar por realizar una revisión física, en el lugar o equipo afectado.
2. El administrador sale al sistema principal.

Requisitos especiales:

- Tiempo de respuesta para monitorizar un equipo o host, menos de 30 segundos el 100% de las veces.

Frecuencia: Continuo.

4.4.1.12 Caso de Uso UC8: Administrar Filtro Web.

Actor Principal: Administrador de red
Personal Involucrado e intereses:

- **Administrador de red:** Quiere brindar a la compañía o institución, el tener una red útil y productiva en cuanto a los contenidos de la Web o Internet, con el fin de

llevar a cabo la finalidad de la institución. Aprovechar al máximo Internet como el recurso tecnológico por excelencia, y proteger a la comunidad interna de contenidos peligrosos y/o obscenos tanto para el equipo conectado a la red como para el mismo usuario respectivamente.

- **Precondiciones:** El administrador se identifica y se autentica. Cualquier modificación el filtro Web, será aplicado a toda la red interna, y por concerniente a todos sus equipos o nodos conectados a la red, sin discriminación alguna.
- **Garantías de Éxito (Postcondiciones):** Se realiza la configuración lógica del servidor respectivo verificando los cambios realizados.

Escenario principal de éxito (ó Flujo Básico):

1. El Administrador en cualquier momento revisa el tráfico del puerto 80 (la mayor parte de URLS trabajan sobre este puerto) y observa por alguna URL sospechosa y/o (Palabras vulgares, obscenas ó de contenido sexual).
2. El administrador captura la URL sospechosa, y comprueba su contenido con un Navegador Web, o bien capturar la IP de usuario para futuras sugerencias o reclamos.
3. El administrador desaprueba el contenido de la URL verificada y procede a su bloqueo.
4. El administrador ingresa la URL sospechosa al sistema.
5. El sistema pregunta sobre el bloqueo de esta URL, para confirmación del administrador.
6. El administrador de red confirma la información mostrada por el sistema.
7. El sistema realiza el bloqueo de la URL especificada.
8. El sistema notifica al administrador y confirma la asignación del nuevo cambio en el filtro.
9. El Administrador verifica y comprueba el bloqueo de la URL a través del Navegador Web.
10. El administrador sigue monitorizando (**Paso 1)** ó sale del sistema.

Extensiones (o flujos Alternativos):

***a.** En cualquier momento el sistema falla:

1. El sistema reporta el error al administrador.
2. El administrador reinicia el sistema, inicia la sesión, y reinicia el proceso monitorización de tráfico de red, si aparece información parcial registrada, elimina la información parcial, y reinicia el proceso.

***b.** En cualquier momento el Administrador puede cancelar el proceso de monitorización.

1. El administrador cancela, y/o elimina cualquier información ya registrada.

3a. El administrador aprueba la URL pero no ciertas palabras en esta:

1. El administrador ingresa la(s) palabra(s) a bloquear al sistema
2. El sistema realiza el bloqueo de la(s) palabra(s) especificada(s).
3. El sistema notifica al administrador y confirma sobre el nuevo cambio en el filtro Web.
4. **Paso 9.**

9a. No hay cambio alguno a la URL especificada al sistema:

1. El administrador verifica el registro antes hecho y comprueba la información registrada.
2. El administrador reinicia el servicio de filtro Web.
3. El administrador verifica los cambios hechos en el navegador Web.

Requisitos especiales:

- Tiempo de respuesta para un bloque de URL o palabra, menos de 1 minuto el 98% de las veces.

Frecuencia: muy continuo.

4.4.1.13 Caso de Uso UC9: Administrar Corta fuegos (firewall).

Actor Principal: Administrador de red
Personal Involucrado e intereses:

- **Administrador de red:** Quiere tener el mayor control sobre los servicios que brinda la red y que soportara en un futuro, dar una jerarquía a los usuarios de la LAN que necesiten mayores servicios dependiendo de su función ó labor dentro de la Empresa, así como también restringir el acceso de servicios que perjudiquen la velocidad global de la LAN (conexiones peer to peer, etc.).
- **Usuario:** Quiere tener la posibilidad de solicitar servicios a nivel de red, apertura de puertos especiales, y/o utilizar un equipo de la red interna como servidor y que tenga la posibilidad de ser visto desde el exterior (Internet) lo que es más conocido como un servicio de traducción de direcciones o NAT.
- **Precondiciones:** El administrador se identifica y se autentica. Los cambios en el cortafuegos pueden realizarse a un equipo específico, a una subred, o a toda la LAN.
- **Garantías de Éxito (Postcondiciones):** Se realiza la configuración lógica del firewall respectivo y se observan los cambios realizados.

Escenario principal de éxito (ó Flujo Básico):

1. El usuario llega a la oficina principal de administración de Internet con su respectiva identificación, ya sea cédula o carné de la institución y la autorización de coordinación.
2. El administrador inicia un nuevo procedimiento en el firewall o corta fuegos, dependiendo de las necesidades que el usuario tenga.
3. El sistema brinda las diferentes opciones de configuración del firewall.
4. El administrador selecciona la opción deseada y procede a realizar el proceso correspondiente.
5. El administrador ingresa los datos requeridos por el proceso seleccionado.
6. El sistema presenta un resumen de datos a procesar.
7. El administrador confirma la información suministrada por el sistema.
8. El sistema realiza la modificación o creación de reglas de firewall pertinentes.
9. El sistema confirma el correcto funcionamiento del firewall
10. El administrador pone a prueba la regla creada o modificada.
11. El administrador informa al usuario de la asignación de su nuevo servicio de red.

Extensiones (o flujos Alternativos):

***a.** En cualquier momento el sistema falla:

1. El sistema reporta el error al administrador.
2. El administrador reinicia el sistema, inicia la sesión, y reinicia el proceso de administración del firewall.

***b.** En cualquier momento el Administrador puede cancelar el respectivo proceso de control de firewall:

1. El administrador cancela cualquier ingreso de datos o proceso en el cortafuegos y regresa al sistema principal.

9a. El sistema no confirma ningún funcionamiento del firewall:

1. El sistema muestra el error si lo tuviese, de la sintaxis del archivo de firewall o bien informar que no a podido realizar la operación requerida debido a un error de sintaxis en la regla dada por el administrador.
2. El administrador verifica el error dado por el sistema y reinicia el proceso.

10a. La regla no brinda el funcionamiento deseado por el administrador:

1. El administrador ingresa al sistema y puede eliminar la regla que desee o bien modificarla.

Requisitos especiales:

- Tiempo de respuesta para creación o modificación de una nueva regla de firewall, menos de 2 minutos el 95% de las veces.

Frecuencia: Continuo.

4.4.1.14 Caso de Uso UC9.1: Administración de puertos y servicios básicos de red.

Actor Principal: Administrador de red
Personal Involucrado e intereses:

- **Administrador de red:** Quiere brindar al usuario de poder tener servicios seguros y exclusivos, dependiendo de las necesidades que el usuario tenga, al mismo tiempo quiere brindar una muy buena seguridad a la hora de cerrar por completo todos aquellos puertos que no se usen y que por ende no son necesarios los cuales pueden representar una gran vulnerabilidad.
- **Usuario:** Quiere tener la posibilidad de solicitar servicios a nivel de red, tales como HTTP, FTP, SSH, entre otros.
- **Precondiciones:** El administrador se identifica y se autentica. Los cambios en el cortafuegos pueden realizarse a un equipo específico, a una subred, o a toda la LAN.
- **Garantías de Éxito (Postcondiciones):** Se realiza la configuración lógica del firewall respectivo y se observan los cambios realizados.

Escenario principal de éxito (ó Flujo Básico):

1. El usuario llega a la oficina principal de administración de Internet con su respectiva identificación, ya sea cédula o carné de la institución y la autorización de coordinación.
2. El usuario solicita un nuevo servicio de red ó la apertura de un puerto específico.
3. El administrador entra al sistema en la sección. de administración de puertos y servicios básicos de red.
4. El administrador ingresa los datos requeridos para la creación de la nueva regla firewall que permita la asignación del nuevo servicio ó puerto al usuario.
5. El sistema presenta un resumen de la regla a procesar.
6. El administrador confirma la información suministrada por el sistema.
7. El sistema realiza la creación de la regla de firewall pertinente.
8. El sistema confirma el correcto funcionamiento del firewall
9. El administrador pone a prueba la nueva regla creada.

10. El administrador informa al usuario de la asignación de su nuevo servicio de red o puerto.

Extensiones (o flujos Alternativos):

***a.** En cualquier momento el sistema falla:

1. El sistema reporta el error al administrador.
2. El administrador reinicia el sistema, inicia la sesión, y reinicia el proceso de administración de servicios básicos de red y puertos de red.

***b.** En cualquier momento el Administrador puede cancelar el respectivo proceso de control de servicios básicos y puertos de red:

1. El administrador cancela cualquier ingreso de datos o proceso en la sección de firewall y regresa al sistema principal.

8a. El sistema no confirma ningún funcionamiento del firewall:

1. El sistema muestra el error si lo tuviese, de la sintaxis del archivo de firewall o bien informar que no a podido realizar la operación requerida debido a un error de sintaxis en la regla dada por el administrador.
2. El administrador verifica el error dado por el sistema y reinicia el proceso.

9a. La regla no brinda el funcionamiento deseado por el administrador:

1. El administrador ingresa al sistema y puede eliminar los cambios realizados o reglas que se superpongan a la recién creada o bien modificarla.

Requisitos especiales:

- Tiempo de respuesta para creación o modificación y correcta implementación de la regla de firewall, menos de 5 minutos el 95% de las veces.

Frecuencia: Continuo.

4.4.1.15 Caso de Uso UC9.2: Administración Servicios especiales de red.

Actor Principal: Administrador de red
Personal Involucrado e intereses:

- **Administrador de red:** Quiere brindar al usuario el poder obtener servicios especiales de red que permitan al usuario la posibilidad de brindar nuevos servicios propios(a nivel de aplicación) hacia otros usuarios.
- **Usuario:** Quiere tener la posibilidad de brindar servicio a otros usuarios dependientes de este mismo, servicios a nivel de aplicación que tiene su fundamento en servicios de red especiales como son (NAT y DNAT).
- **Precondiciones:** El administrador se identifica y se autentica. Los cambios en el cortafuegos pueden realizarse a un equipo específico, a una subred, o a toda la LAN.
- **Garantías de Éxito (Postcondiciones):** Se realiza la configuración lógica del firewall respectivo y se observan los cambios realizados.

Escenario principal de éxito (ó Flujo Básico):

1. El usuario llega a la oficina principal de administración de Internet con su respectiva identificación, ya sea cédula o carné de la institución y la autorización de coordinación.
2. El usuario solicita un servicio de red especial para brindar nuevos servicios a otros usuarios.
3. El administrador entra al sistema en la sección. de administración de servicios especiales de red (NAT DNAT)
4. El administrador ingresa los datos requeridos para la creación de la nueva regla firewall que permita la asignación del nuevo servicio especial.
5. El sistema presenta un resumen de la regla a procesar.
6. El administrador confirma la información suministrada por el sistema.
7. El sistema realiza la creación de la regla de firewall pertinente.
8. El sistema confirma el correcto funcionamiento del firewall
9. El administrador pone a prueba la nueva regla creada.
10. El administrador informa al usuario de la asignación de su nuevo servicio de red o puerto.

Extensiones (o flujos Alternativos):

***a.** En cualquier momento el sistema falla:

1. El sistema reporta el error al administrador.
2. El administrador reinicia el sistema, inicia la sesión, y reinicia el proceso de administración de servicios básicos de red y puertos de red.

***b.** En cualquier momento el Administrador puede cancelar el respectivo proceso de control de servicios básicos y puertos de red:

1. El administrador cancela cualquier ingreso de datos o proceso en la sección de firewall y regresa al sistema principal.

8a. El sistema no confirma ningún funcionamiento del firewall:

1. El sistema muestra el error si lo tuviese, de la sintaxis del archivo de firewall o bien informa que no ha podido realizar la operación requerida debido a un error de sintaxis en la regla dada por el administrador.

2. El administrador verifica el error dado por el sistema y reinicia el proceso.

9a. La regla no brinda el funcionamiento deseado por el administrador:

1. El administrador ingresa al sistema y puede eliminar los cambios realizados o reglas que se superpongan a la recién creada o bien modificarla.

Requisitos especiales:

- Tiempo de respuesta para creación o modificación y correcta implementación de la regla de firewall, menos de 5 minutos el 95% de las veces.

Frecuencia: Muy poco usual.

4.4.1.16 Caso de Uso UC9.3: Monitorización de Tráfico

Actor Principal: Administrador de red
Personal Involucrado e intereses:

- **Administrador de red:** Quiere tener una rápida y sencilla vista del comportamiento de tráfico de la red LAN a través de gráficos estadísticos, fáciles de leer, en tiempo real que permita guardar un seguimiento histórico a través del tiempo así como permitir reconocer problemas de congestión y/o saturación de la red..
- **Precondiciones:** La monitorización bien puede ser vista por cualquier persona adscrita a la dependencia o por el administrador del sistema.
- **Garantías de Éxito (Postcondiciones):** Se realiza la monitorización, dependiendo de los resultados vistos se realiza una toma de decisiones por parte del administrador

Escenario principal de éxito (ó Flujo Básico):

1. El administrador entra al sistema en la sección. de monitorización de la red.
2. El sistema presenta un resumen del tráfico entrante y saliente de la red.
3. El administrador analiza la información mostrada por el sistema.
4. El administrador confirma el correcto funcionamiento de la LAN.
5. El administrador sale del sistema o regresa al sistema principal

Extensiones (o flujos Alternativos):

***a.** En cualquier momento el sistema falla:

1. El sistema reporta el error al administrador.
2. El administrador reinicia el sistema, inicia la sesión, y reinicia el proceso de monitorización de la red.

***b.** En cualquier momento el Administrador puede cancelar la monitorización de tráfico:

1. El administrador simplemente regresa al sistema principal.

Requisitos especiales:

- El monitoreo de tráfico de la red puede ser hecha en cualquier momento a cualquier hora y el tiempo del proceso depende del tiempo que el administrador quiera seguir observando el tráfico.

Frecuencia: siempre continuo.

4.4.1.17 Caso de Uso UC9.4: Suspensión de Servicio

Actor Principal: Administrador de red
Personal Involucrado e intereses:

- **Administrador de red:** Quiere realizar operaciones de restricción de servicio rápidas, y eficaces, que por lo general se realizan cuando existe un abuso de servicio por algún usuario adrede, o por la inestabilidad o daño de algún equipo o host conectado a la red (Virus, Programas Espía, entre otros).
- **Precondiciones:** El administrador se identifica y se autentica. Los cambios en el cortafuegos pueden realizarse a un equipo específico, a una subred, o a toda la LAN.

- **Garantías de Éxito (Postcondiciones):** Se realiza la configuración lógica del firewall respectivo y se observan los cambios realizados.

Escenario principal de éxito (ó Flujo Básico):

1. El administrador entra al sistema en la sección de suspensión y restricción de servicio.
2. El administrador ingresa los datos requeridos para la creación de la nueva suspensión de servicio, ya sea a un equipo en particular, a una subred o a toda la LAN
3. El sistema presenta un resumen de la regla a procesar.
4. El administrador confirma la información suministrada por el sistema.
5. El sistema realiza la creación de la regla de firewall pertinente.
6. El sistema confirma el correcto funcionamiento del firewall
7. El administrador pone a prueba la nueva regla creada.

Extensiones (o flujos Alternativos):

***a.** En cualquier momento el sistema falla:

1. El sistema reporta el error al administrador.
2. El administrador reinicia el sistema, inicia la sesión, y reinicia el proceso de administración de servicios básicos de red y puertos de red.

***b.** En cualquier momento el Administrador puede cancelar el respectivo proceso de control de servicios básicos y puertos de red:

1. El administrador cancela cualquier ingreso de datos o proceso en la sección de firewall y regresa al sistema principal.

6a. El Sistema no confirma ningún funcionamiento del firewall:

1. El sistema muestra el error si lo tuviese, de la sintaxis del archivo de firewall o bien informa que no ha podido realizar la operación requerida debido a un error de sintaxis en la regla dada por el administrador.

2. El administrador verifica el error dado por el sistema y reinicia el proceso.

7a. La regla no brinda el funcionamiento deseado por el administrador:

1. El administrador ingresa al sistema y puede eliminar los cambios realizados o reglas que se superpongan a la recién creada o bien modificarla.

Requisitos especiales:

- Tiempo de respuesta para creación o modificación y correcta implementación de la regla de firewall, menos de 5 minutos el 95% de las veces.

Frecuencia: Poco usual.

4.4.1.18 Caso de Uso UC10: Autenticar

Actor Principal: Administrador de red
Personal Involucrado e intereses:

- **Administrador de red:** Quiere tener el poder de autenticarse para la administración de cualquier servicio soportado por ANUBIS, así como también ser capaz de crear otros usuarios que dependan de este.
- **Usuario:** Quiere tener independencia y seguridad a la hora de ingresar a cualquier servicio soportado por ANUBIS, así como también tener confianza en el administrador del sistema ya que la clave de acceso solo será conocida por el mismo usuario.
- **Precondiciones:** El administrador se identifica y se autentica, si es por primera vez, ingresa con una contraseña propia del sistema, para crear una nueva.
- **Garantías de Éxito (Postcondiciones):** El administrador es capaz de autenticarse, cambiar su contraseña de acceso así como también crear nuevas cuentas de usuario ya sean de correo electrónico ó cuentas de conexión a Internet.

Escenario principal de éxito (ó Flujo Básico):

1. El sistema pide una contraseña, para acceder al sistema, si es primera vez, se debe ingresar con una contraseña por defecto.
2. El administrador ingresa su login y contraseña.
3. El sistema inicia sesión.
4. El administrador empieza a utilizar el sistema.

Extensiones (o flujos Alternativos):

***a.** En cualquier momento el sistema falla:

1. El sistema reporta el error al administrador.
2. El administrador reinicia el sistema, inicia la sesión, y reinicia el proceso de autenticación.

***b.** En cualquier momento el Administrador puede cancelar el inicio de sesión:

1. El administrador cancela cualquier ingreso de datos y sale del sistema

Requisitos especiales:

- Tiempo de respuesta para inicio de sesión, menos de 10 segundos el 99% de las veces.

Frecuencia: Muy continúo.

4.4.2 **Requerimientos de facilidad de uso (usability).** La suite de aplicaciones de ANUBIS deberá presentar una agradable interfaz gráfica y ayuda en línea que brinde en gran parte la facilidad de uso del sistema. Cabe destacar que el sistema estará desarrollado con el fin de que un ingeniero, ó al menos técnico en sistemas, redes o telecomunicaciones pueda usarlo. No estará desarrollado para cualquier usuario debido al objetivo del sistema y a conceptos técnicos que no se pueden generalizar (Excepto la interfaz de correo electrónico para el usuario final y la interfaz de publicaciones Web); es decir se deberán tener conceptos básicos claros de la administración de redes de datos así como también de las ventajas que un sistema operativo GNU/Linux puede brindar.

El sistema deberá contar con todas las herramientas necesarias para administrar los servicios mencionados, sin embargo si el Administrador del sistema necesita modificar los archivos primarios con más detalle, lo podrá hacer editando manualmente los archivos de configuración propios del sistema operativo, a través de las opciones avanzadas o modo experto en el sistema. Nuevamente el administrador en tal caso debe tener un detallado conocimiento de cada uno de los archivos de configuración y buen manejo de sistemas basadas en UNIX como lo es GNU/Linux.

4.4.3 **Requerimientos de fiabilidad (reliability).** El sistema ANUBIS brindará un muy buen nivel de fiabilidad en el manejo de sus procesos, debido a que se compenetra íntegramente con archivos de configuración propios de los sistemas GNU/Linux. En otras palabras, la fiabilidad a parte de la programación y codificación del sistema dependerá de la estabilidad y actualización del Kernel de sistema operativo usado.

4.4.4 **Requerimientos de rendimiento (performance).** El sistema ANUBIS deberá tener un excelente rendimiento siempre y cuando posea los suficientes recursos físicos para proveer de manera segura y eficaz los servicios propuestos, refiriéndose en la siguiente tabla.

Número de Usuarios	Características Mínimas
1-20	Disco 10 GB, 256 MB RAM, Pentium II 500MHz o superior.
20-50	Disco 20 GB, 512 MB RAM, Pentium III de 1 GHz o superior.
50 – 100	Disco 20 GB SCSI, 1024 MB RAM, Pentium IV de 2 GHz o superior
100 – 200	Disco 30 GB SCSI, 1024 MB RAM, Pentium IV de 3GHZ o superior
200 ó Más	Disco Ultra SCSI 40 GB, 2048 MB RAM, Pentium IV Dual Core de 2GHz o superior, preferiblemente Intel XEON 3GHz a 64 bits.

Tabla 1. Relación usuarios y características mínimas de hardware.

4.4.5 **Requerimientos de soporte (supportability)** El sistema ANUBIS contará con la adaptabilidad de poder ser instalado en cualquier distribución de GNU/Linux con Kernel superior a 2.4.x con el fin de utilizar los recursos de IPTABLES disponibles únicamente desde estas versiones de Kernel en adelante.

El sistema estará desarrollado de forma modular lo que permitirá un fácil mantenimiento y aún más, una fácil capacidad de expansión a nuevos módulos. Téngase muy en cuenta que el sistema pretende abordar los servicios de red más conocidos y utilizados dentro de sistemas GNU/Linux, sin embargo, se pueden sistematizar más de 50 servicios, no solo de red sino de varias aplicaciones como son (correo, mensajería instantánea, Voz IP, servidor de tiempo, tareas automatizadas, hasta videoconferencias, etc.). En pocas palabras el sistema brinda nuevas líneas de investigación a futuros estudiantes y por que no a los actuales docentes universitarios que quieran profundizar más en el tema. Lo más importante es que el sistema ANUBIS brinda la filosofía y el camino guía de cómo hacerlo.

4.4.6 **Implementación.** El sistema ANUBIS será desarrollado mediante distintos lenguajes de programación dependiendo de los requerimientos que el sistema pida.

El sistema necesitará de alguna forma realizar procesos o modificar archivos que necesiten privilegios de root o de súper usuario, se utilizara PERL, C++, y manejo de Shell del sistema operativo para dicho fin, o bien se utilizará PHP como lenguaje de programación orientado a objetos desde su versión 5 para página Web dinámicas, HTML para la interfaz de usuario, y JavaScript para la validación de formularios.

- **Operaciones**

Se pretende poner en marcha el sistema, en la red de datos de la Universidad de Nariño.

- **Legales**

La propiedad intelectual del sistema será de la Universidad de Nariño por tratarse de un trabajo de grado, pero podría proponerse la liberación de código fuente al resto de la comunidad académica a través de licencia publica general GPL.

4.5 CLIENTES DEL SISTEMA

- Estudiantes
- Trabajadores
- Docentes
- Personal Administrativo

4.6 METAS DEL SISTEMA

La meta general del sistema es de ejecutar los procesos descritos eficientemente, en el menor tiempo posible y de forma tranparente al usuario. Así como también la de brindar nuevas ideas de desarrollo e investigación a la comunidad universitaria de la facultad de ingeniería de la Universidad de Nariño, teniendo en cuenta que es la primera vez que se realiza un proyecto de este tipo.

Para lograr éste cometido se pretende:

1. Modular el sistema entre las distintas partes que este conlleva como son la de Administración de nodos, servidor proxy, firewall, correo electrónico, ancho de banda, filtro web y manejo de publicaciones web.

2. Automatizar los procesos de la oficina de administración de servicios de Internet de la Universidad de Nariño

3. Tener un mejor control respecto al ingreso de usuarios a la red, tener en cuenta no solo el equipo del usuario, sino también la información personal de cada uno de ellos, información importante al momento de querer contactar al usuario o al momento de hacer algún tipo de reportes, o estadísticas.

4. Demostrar a la comunidad académica de la facultad de ingeniería una novedosa metodología para la sistematización de cualquier herramienta que pueda ser integrada en sistemas GNU/LINUX ya que con este trabajo se pretende demostrar que existe un sinnúmero de posibilidades para crear nuevos proyectos a partir de este.

5. Despertar la necesidad a profesores y estudiantes, de conocer y manejar más a fondo lo sistemas basados en UNIX como lo es GNU/LINUX, y aprender los beneficios que estos nos brindan tanto académicamente como profesionalmente hablando.

5. MODELADO DEL NEGOCIO DEL SISTEMA ANUBIS "SUITE DE APLICACIONES DESTINADAS A LA ADMINISTRACION DE SERVICIOS DE REDES AREA LOCAL TIPO IP BAJO PLATAFORMA GNU/LINUX"

El siguiente diagrama representa los diferentes subsistemas en los que se ha dividido la Oficina de administración de servicios de red mediante un nivel de abstracción como es el siguiente:

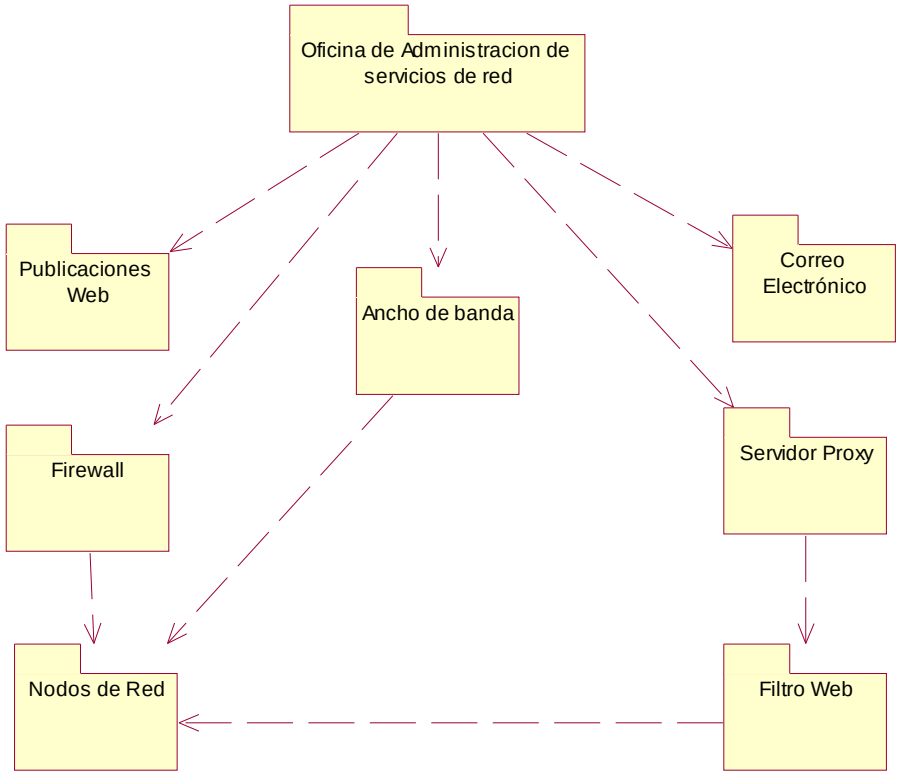


Figura 3. Diagrama General o de Abstracción del sistema.

A continuación se presentan los modelos definidos en el RUP como modelo de negocio en donde se cubre el modelado de "Casos de uso del negocio", "Modelo del dominio", "Modelos de objetos del negocio", para el sistema.

5.1 MODELO DE CASOS DE USO DE NEGOCIO

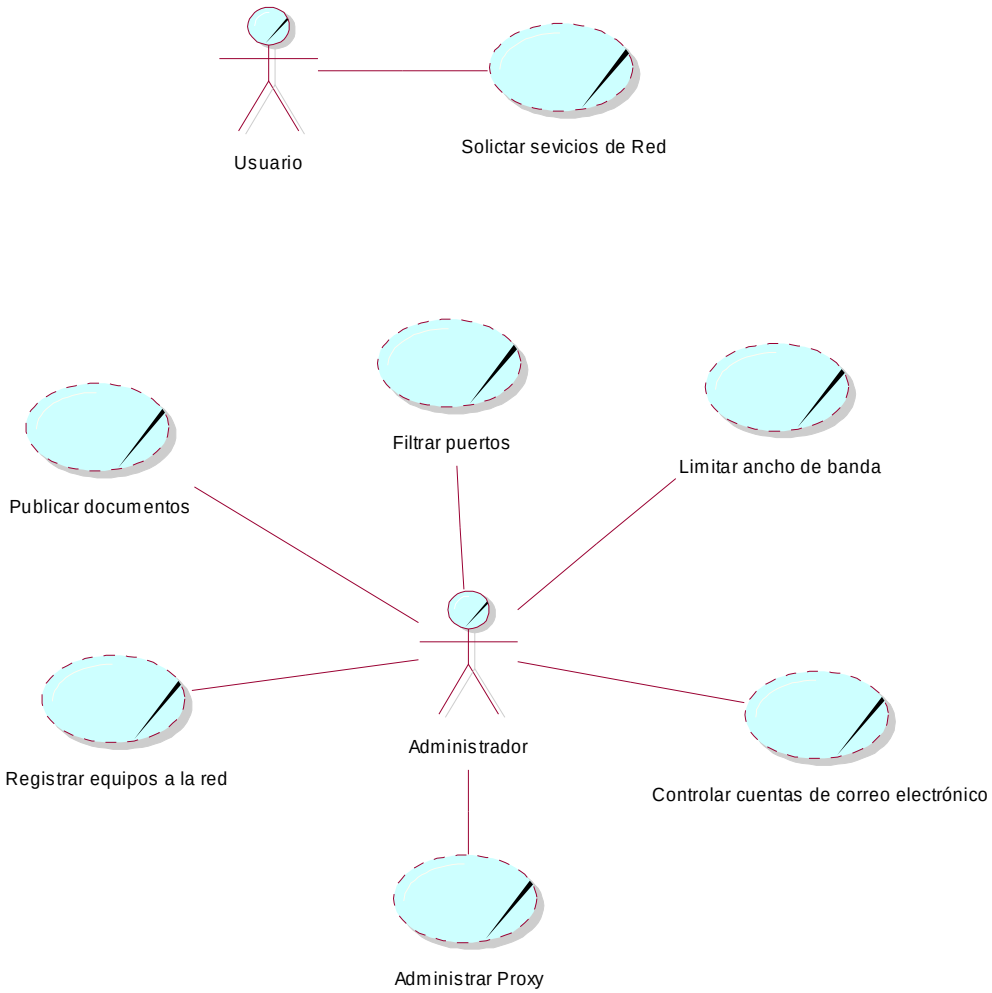


Figura 4. Modelo de Casos de uso de Negocio**.**

5.2 MODELO DE DOMINIO DEL NEGOCIO

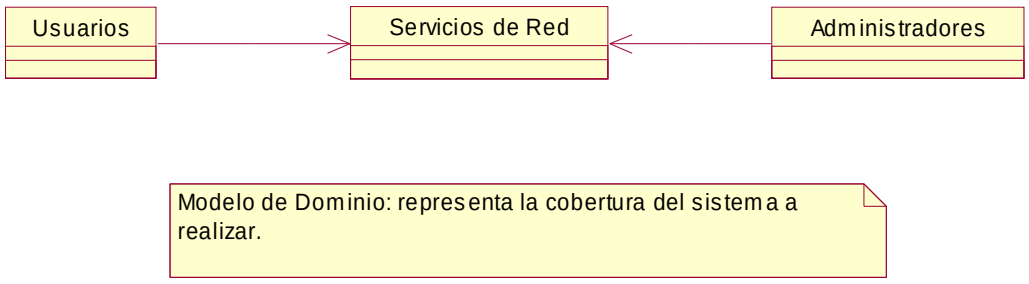


Figura 5. Dominio del sistema.

5.3 MODELO DE OBJETOS DEL NEGOCIO

5.3.1 Modelo de objeto de solicitar servicio de publicaciones

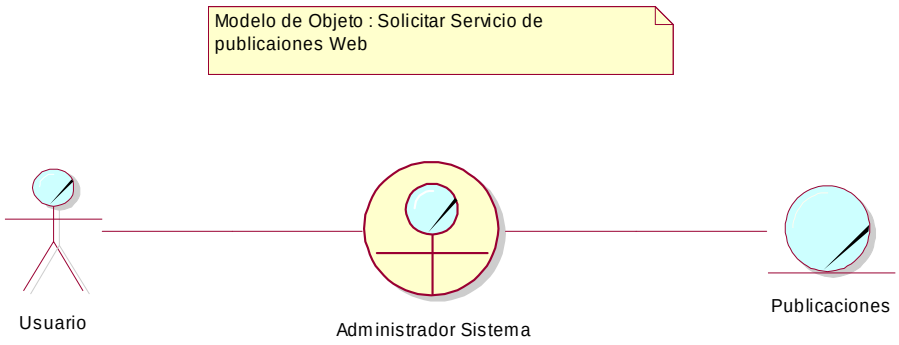


Figura 6. Modelo de objeto de solicitar servicio de publicaciones.

5.3.2 Modelo de objeto de solicitar servicio de correo electrónico

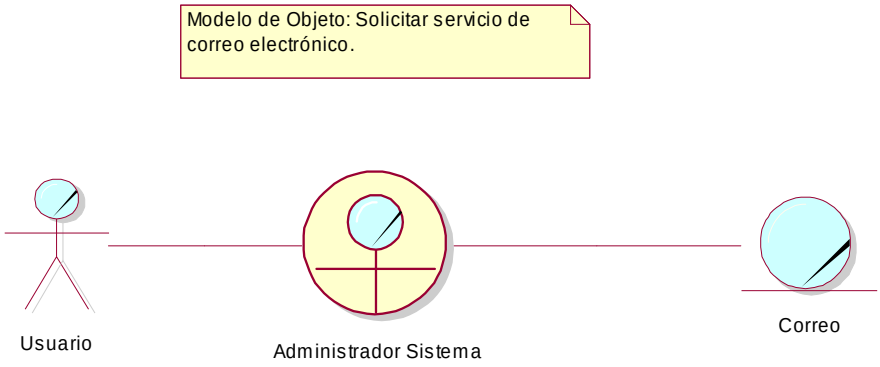


Figura 7. Modelo de objeto de solicitar servicio de correo electrónico

5.3.3 Modelo de objeto de solicitar creación de nuevo punto de red

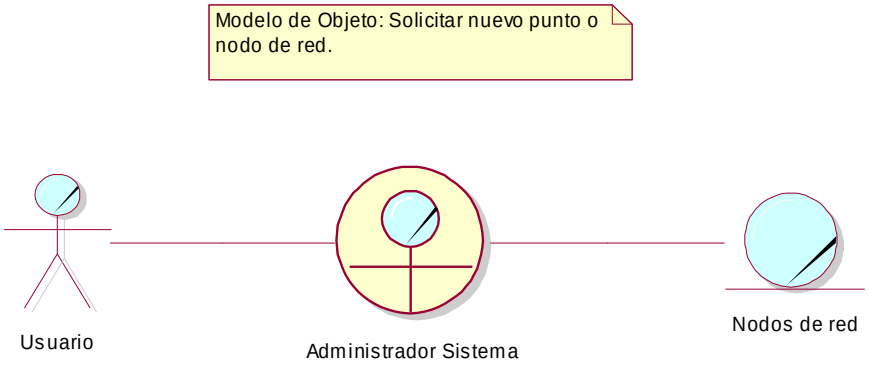


Figura 8. Modelo de Objeto de solicitar creación de nuevo punto de red.

5.3.4 Modelo de objeto de solicitar servicio de modificación de ancho de banda

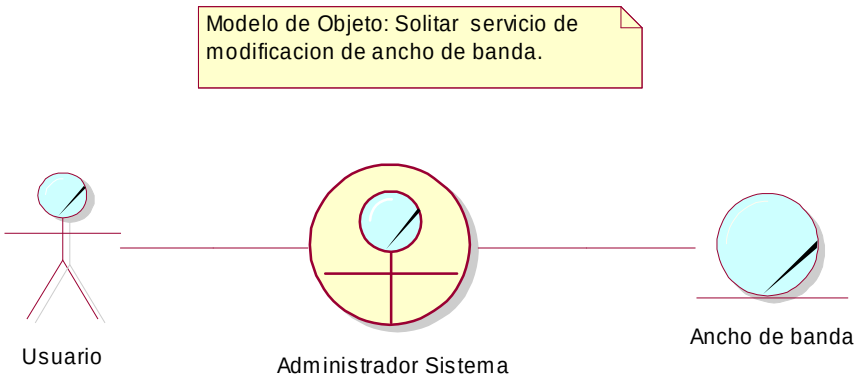


Figura 9. Modelo de objeto de solicitar modificación de ancho de banda.

5.3.5 Modelo de objeto de solicitar apertura de puertos de red

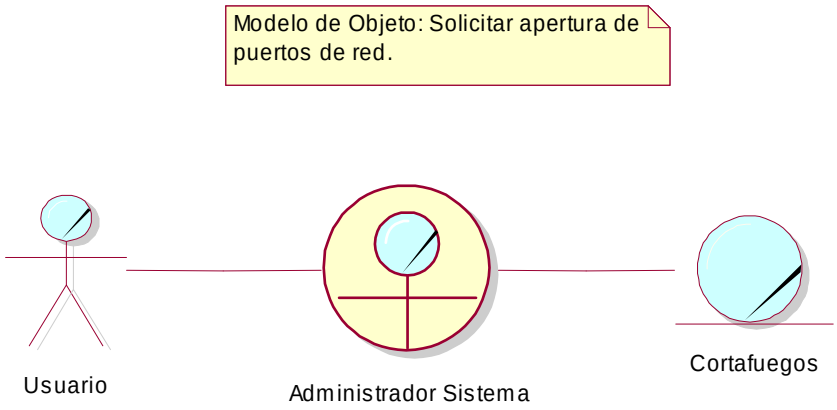


Figura 10. Modelo de objeto de solicitar apertura de puertos de red

5.3.6 Modelo de objeto de realizar mantenimiento del servidor proxy.

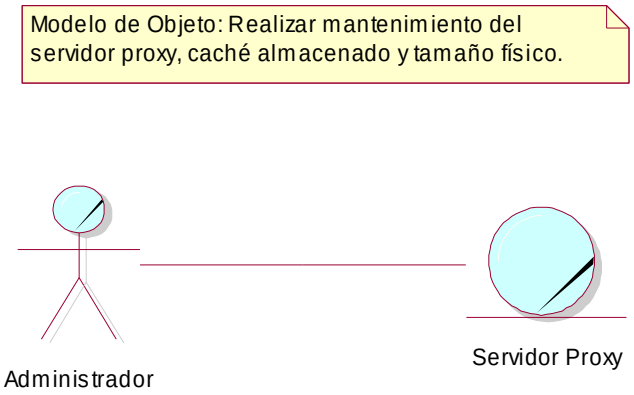


Figura 11. Modelo de objeto de realizar mantenimiento del servidor Proxy.

5.3.7 Modelo de objeto de realizar actualización del filtro web

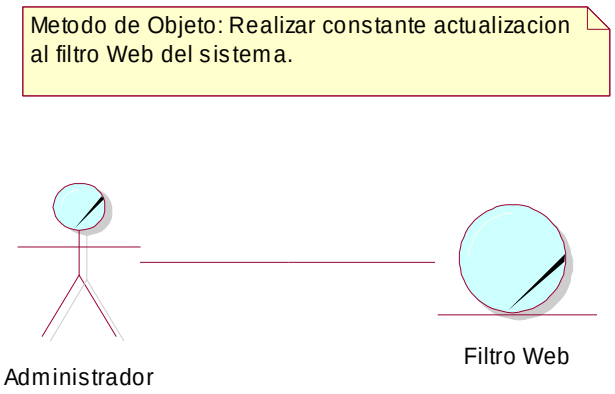
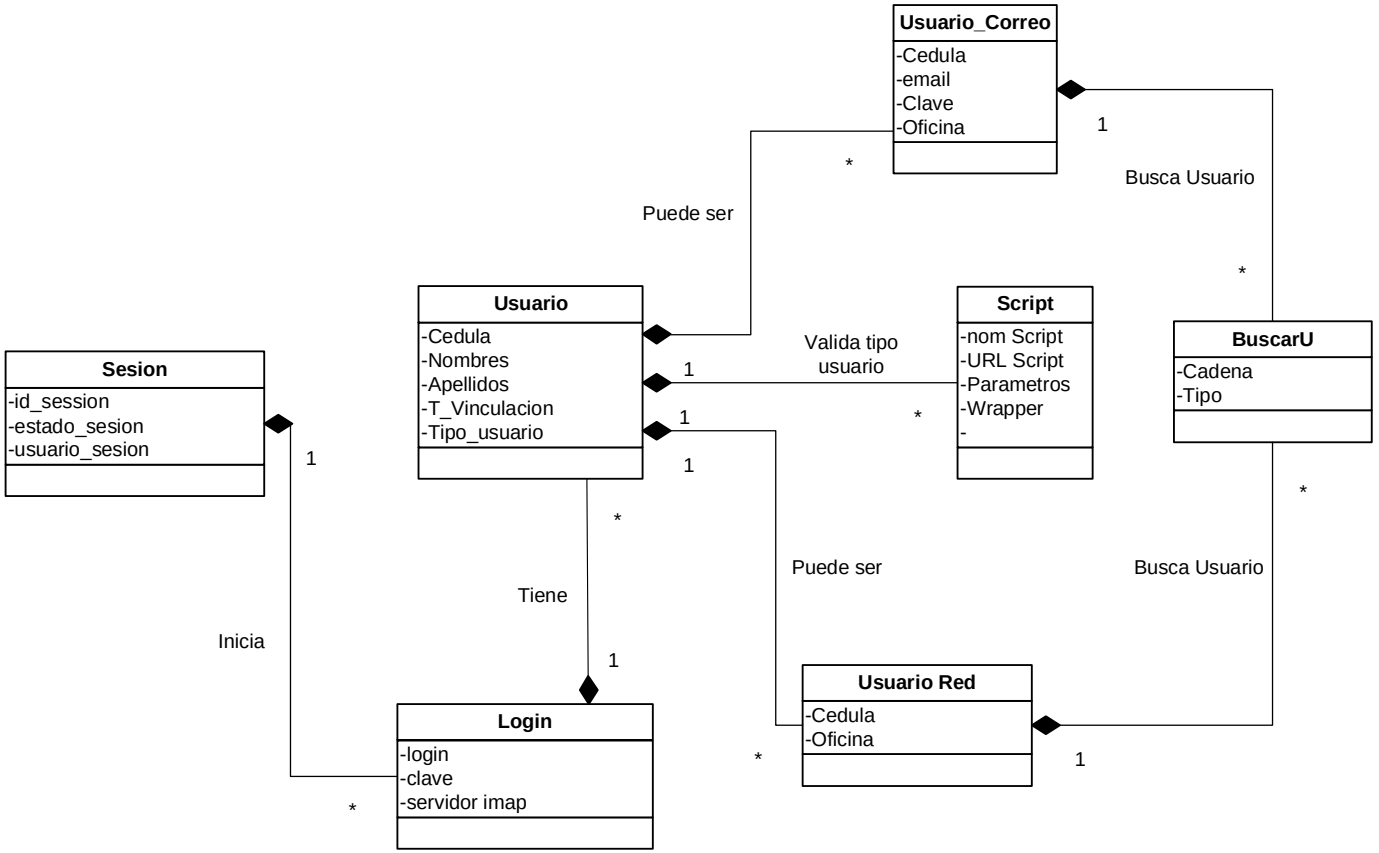


Figura 12. Modelo de objeto de Realizar actualización frecuente del filtro Web.

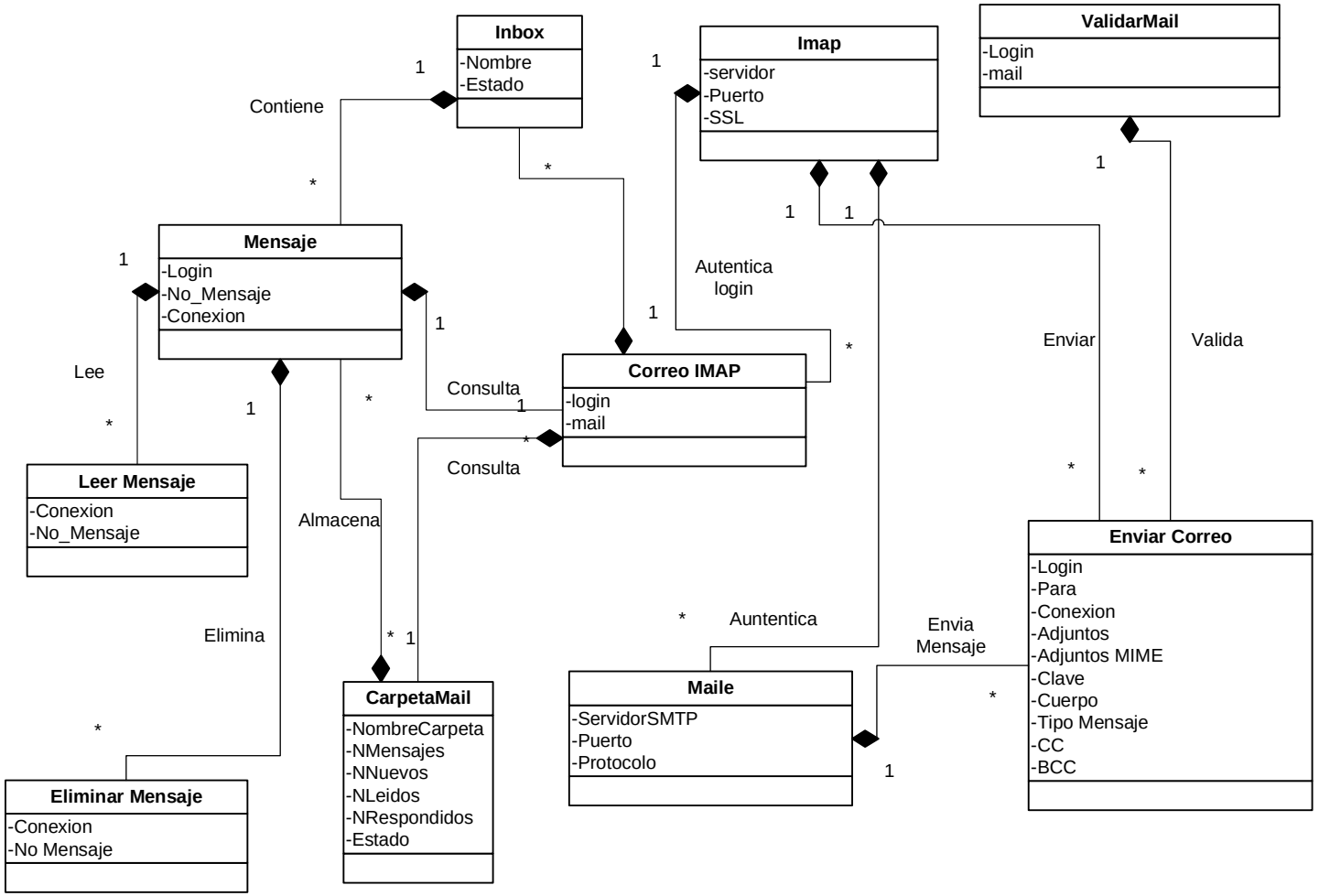
5.4 DIAGRAMA CONCEPTUAL

5.4.1 Diagrama conceptual de control de usuarios



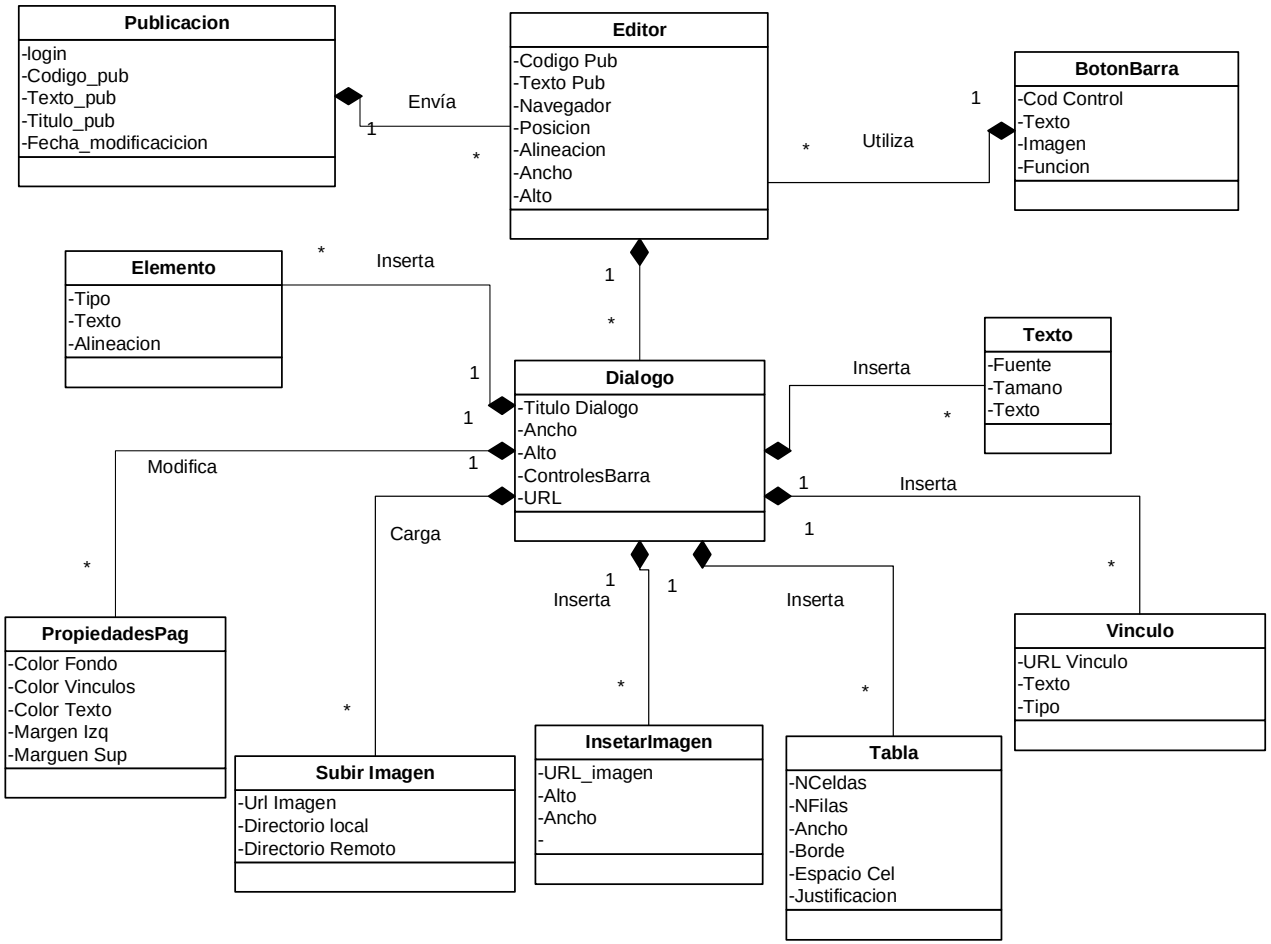
Esquema 6. Diagrama conceptual de control de usuarios.

5.4.2 Diagrama conceptual de correo electrónico



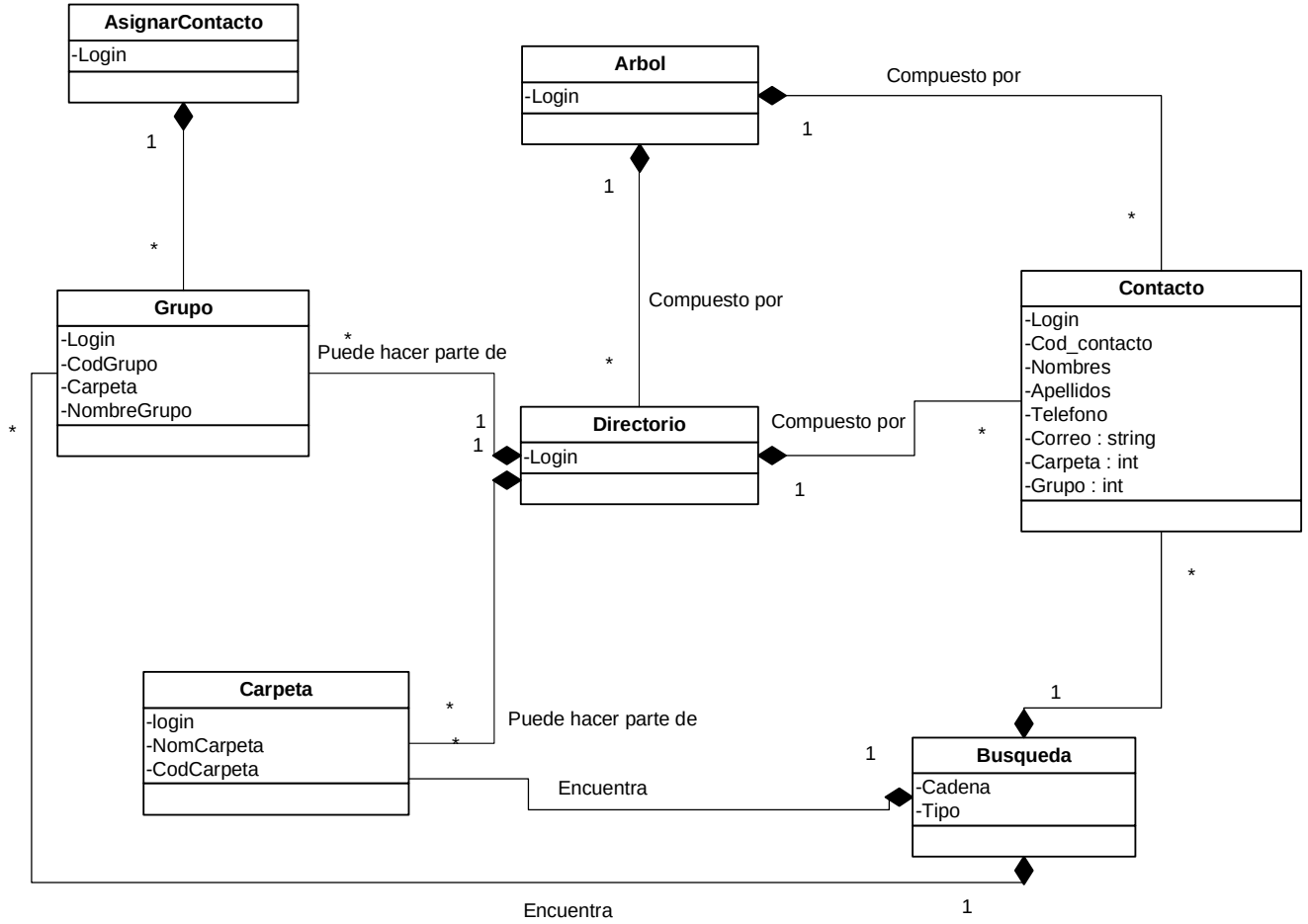
Esquema 7. Diagrama conceptual de correo electrónico.

5.4.3 Diagrama conceptual de publicaciones web



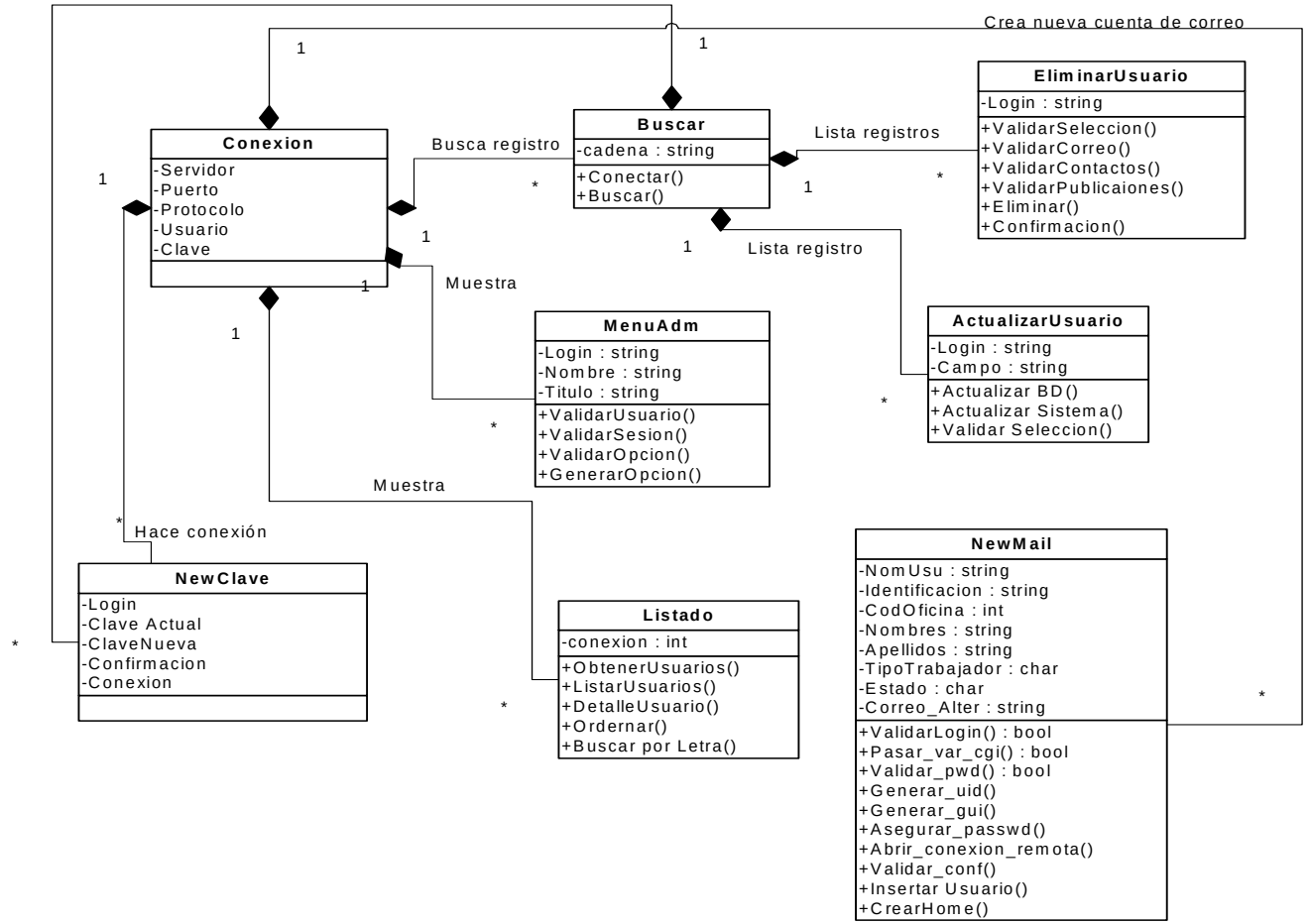
Esquema 8. Diagrama conceptual de publicaciones Web

5.4.4 Diagrama conceptual de contactos de correo y directorio



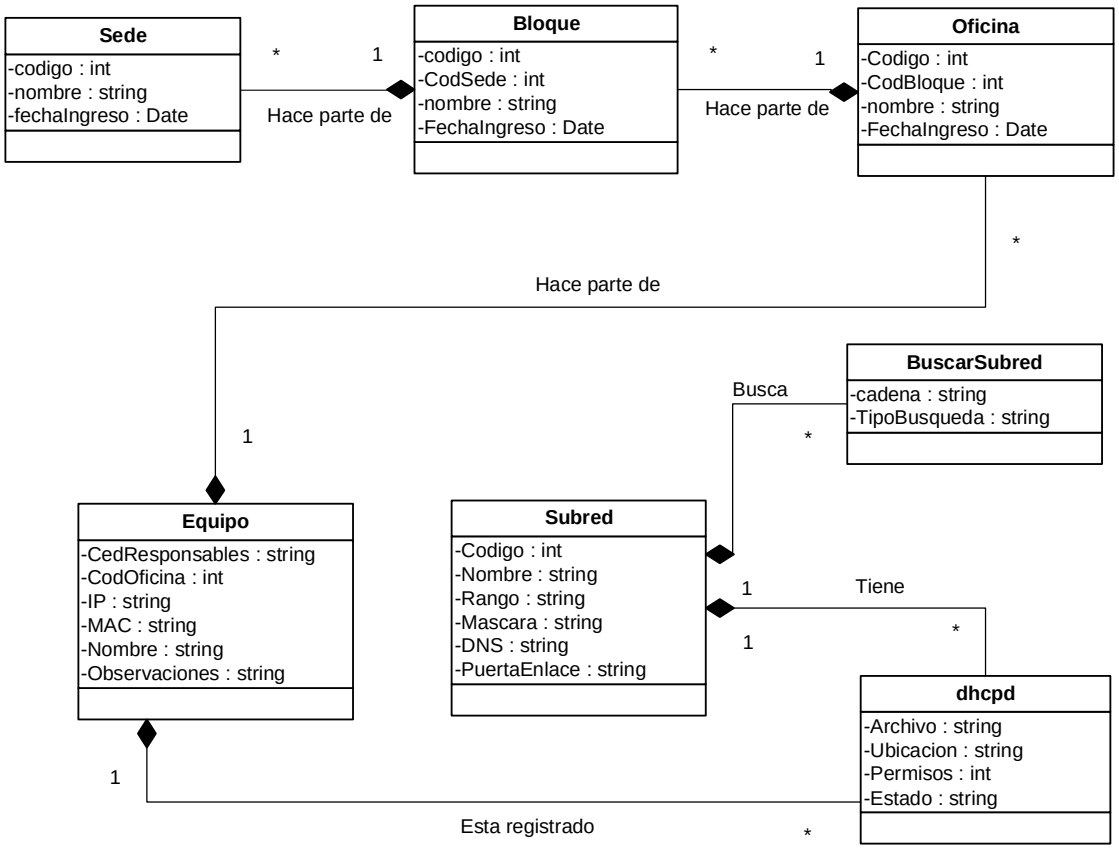
Esquema 9. Diagrama conceptual de contactos de correo y directorio.

5.4.5 Diagrama conceptual de administración de correo electrónico modo administrador



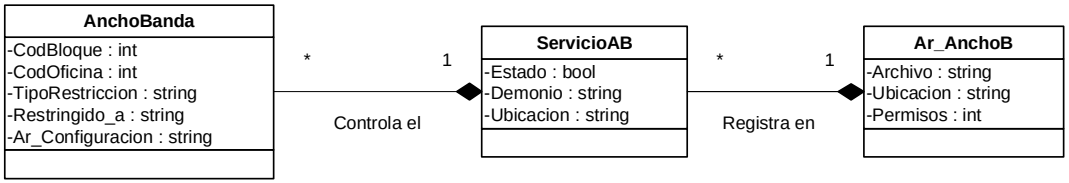
Esquema 10. Diagrama conceptual de administración de correo electrónico modo administrador.

5.4.6 Diagrama conceptual de administración de nodos de red.



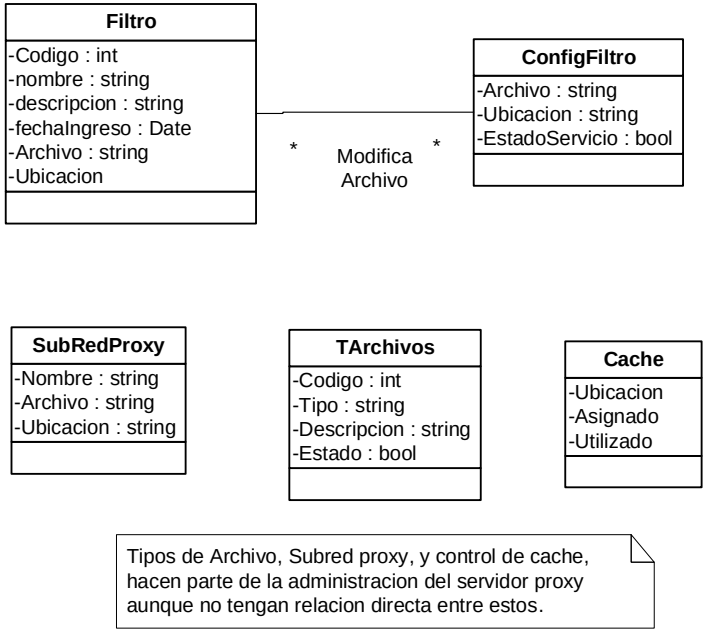
Esquema 11. Diagrama conceptual de administración de nodos de red.

5.4.7 Diagrama conceptual de control de ancho de banda.



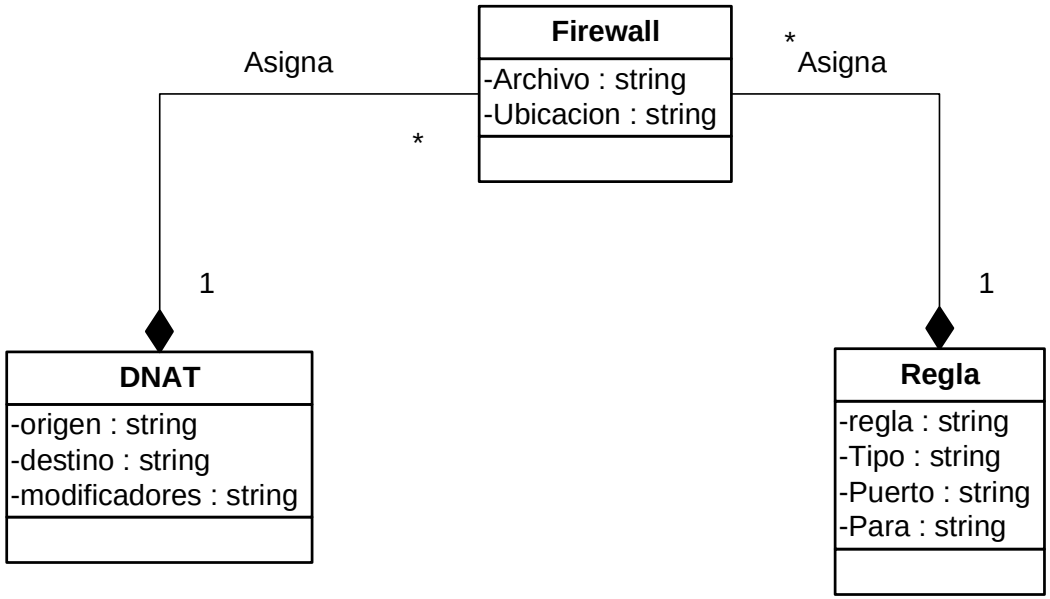
Esquema 12. Diagrama conceptual de control de ancho de banda

5.4.8 Diagrama conceptual de administración de servidor proxy y filtro web.



Esquema 13. Diagrama conceptual de administración de servidor proxy y filtro web.

5.4.9 Diagrama conceptual de administración de cortafuegos (firewall).



Esquema 14. Diagrama conceptual de administración de servidor proxy y filtro web.

5.5 DIAGRAMAS DE CASOS DE USO DEL SISTEMA

5.5.1 Diagrama general de administración de servicios de red

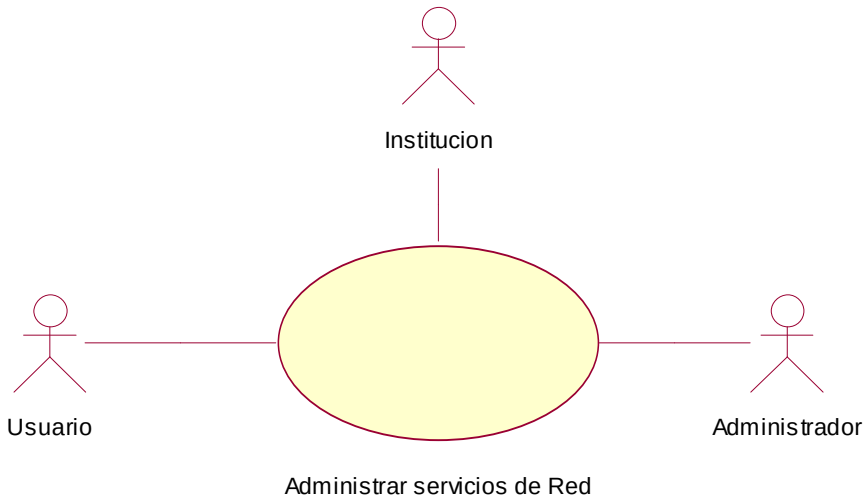


Figura 13. Diagrama general de administración de servicios de red.

5.5.2 Diagrama de caso de uso: control de usuarios e infraestructura física

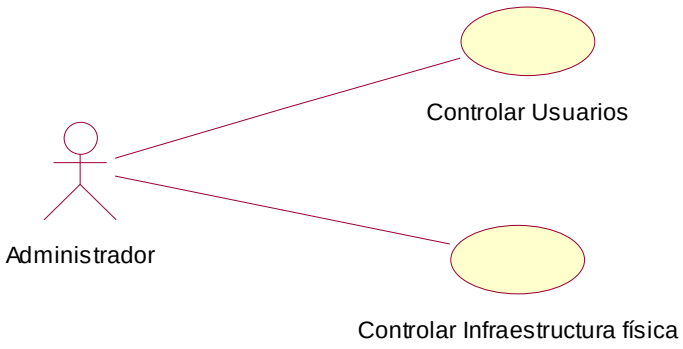


Figura 14. Control de usuarios e infraestructura física.

5.5.3 Diagrama de caso de uso: administrar publicaciones web

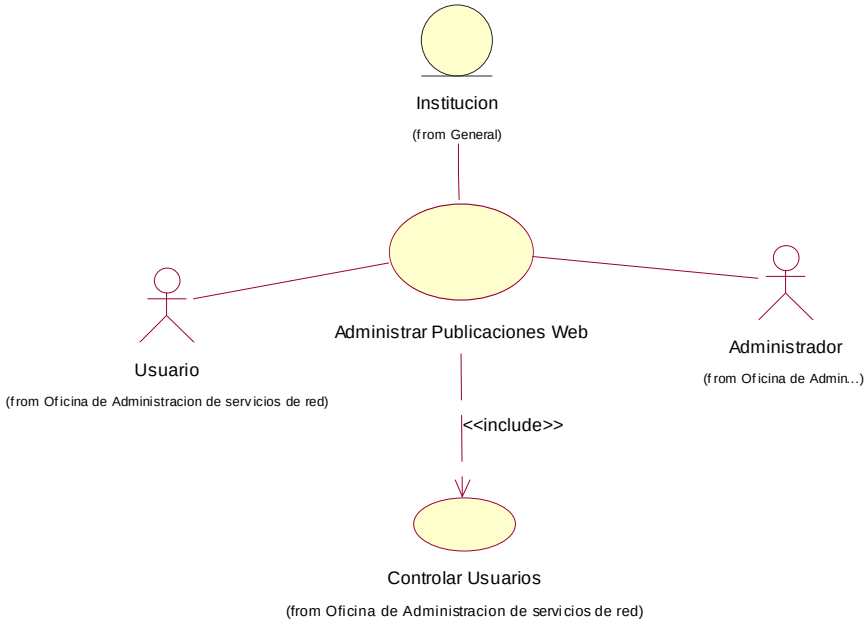


Figura 15. Administrar Publicaciones Web.

5.5.4 Diagrama de caso de uso: administrar correo electrónico

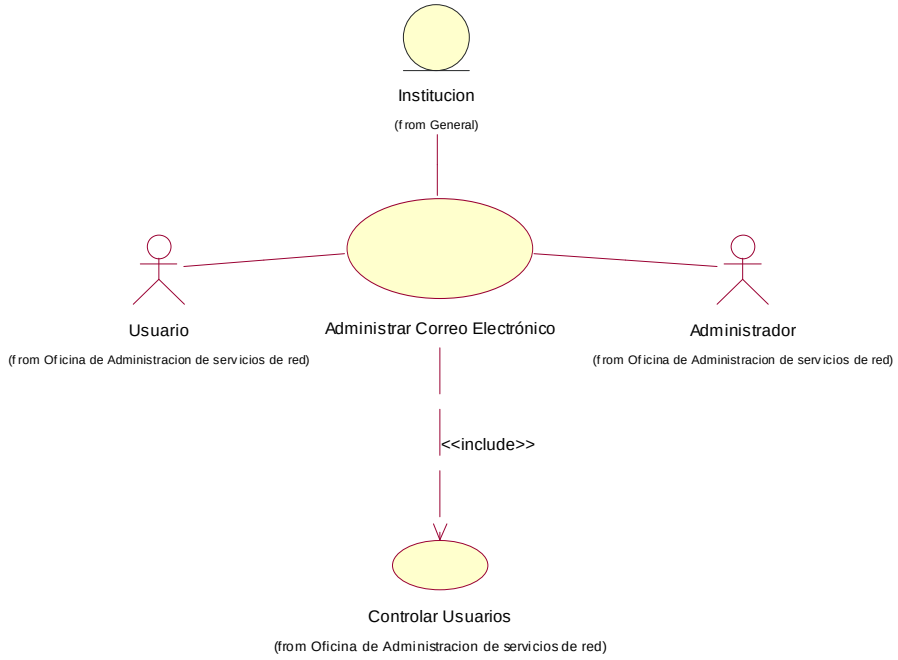


Figura 16. Administrar Correo electrónico.

5.5.5 Diagrama de caso de uso: administrar nodos o puntos de red

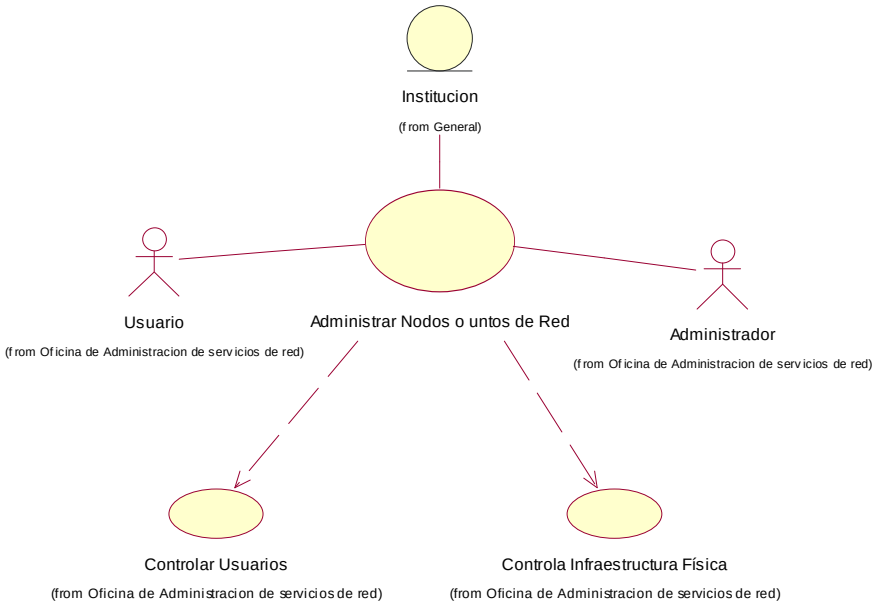


Figura 17. Administrar nodos o puntos de red.

5.5.6 Diagrama de caso de uso: controlar ancho de banda

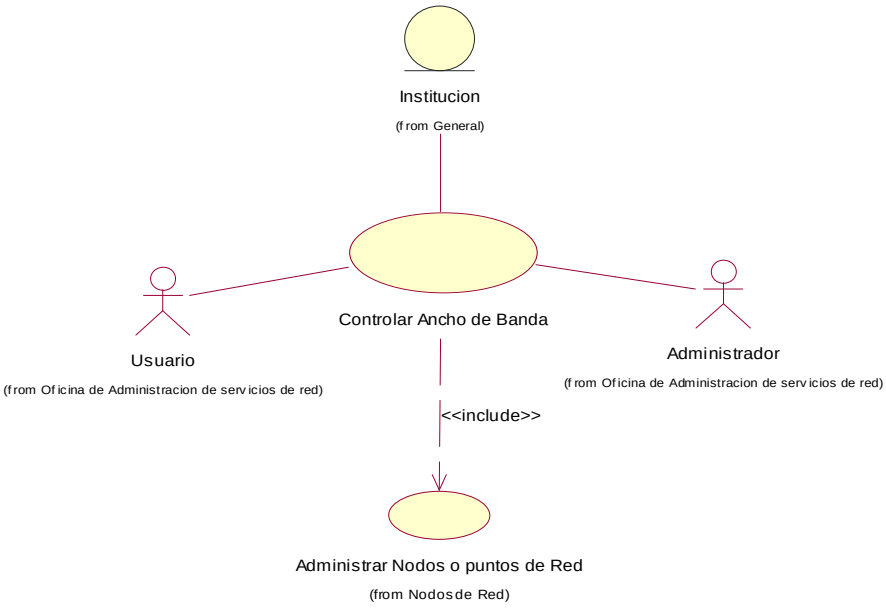


Figura 18. Controlar ancho de banda.

5.5.7 Diagrama de caso de uso: administración de servidor proxy

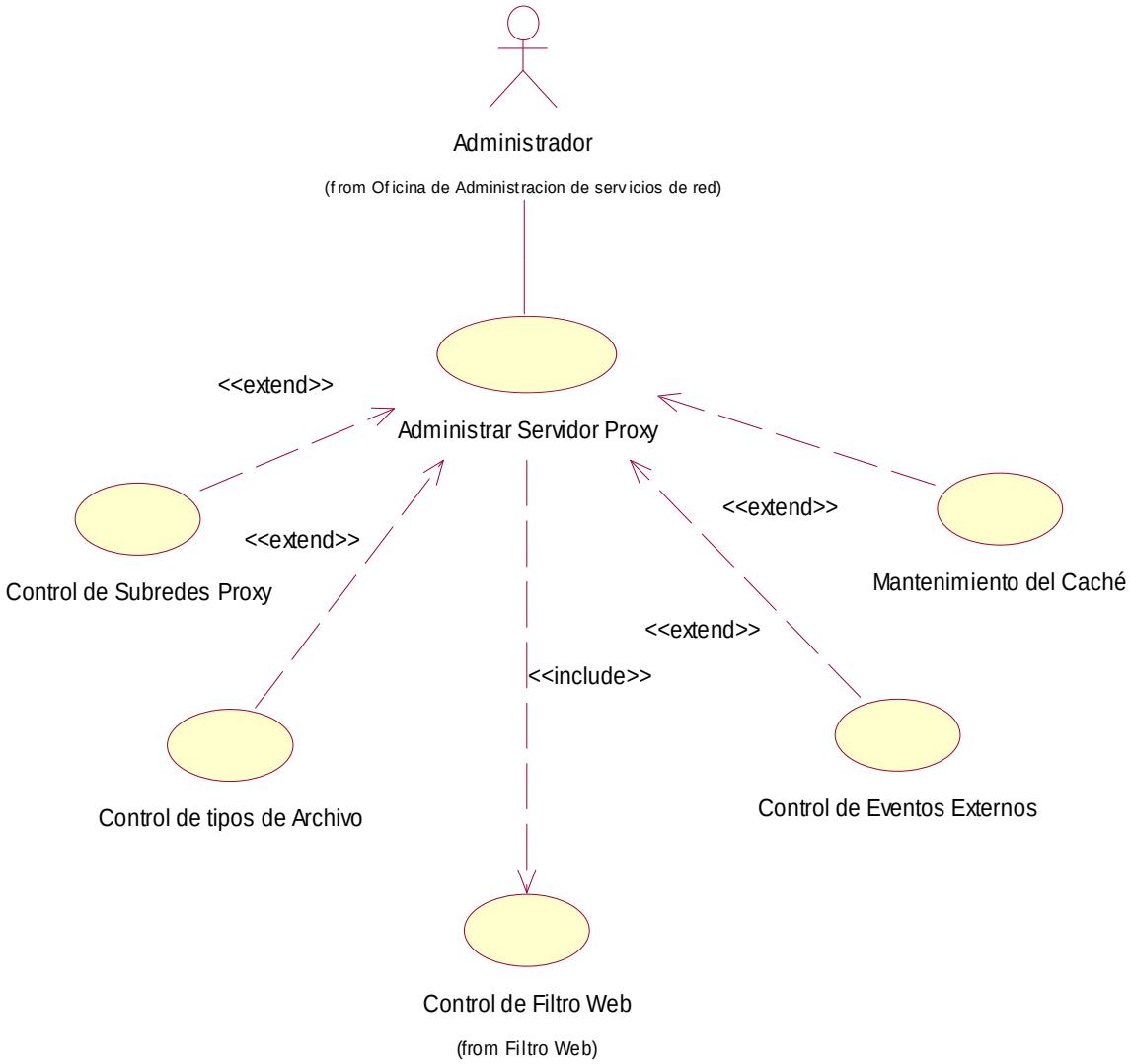


Figura 19. Administración de servidor Proxy.

5.5.8 Diagrama de caso de uso: control de filtro web

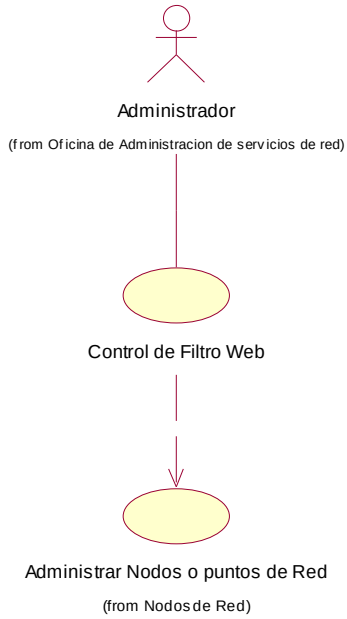


Figura 20. Control de filtro Web.

5.5.9 Diagrama de caso de uso: administrar corta fuegos o firewall

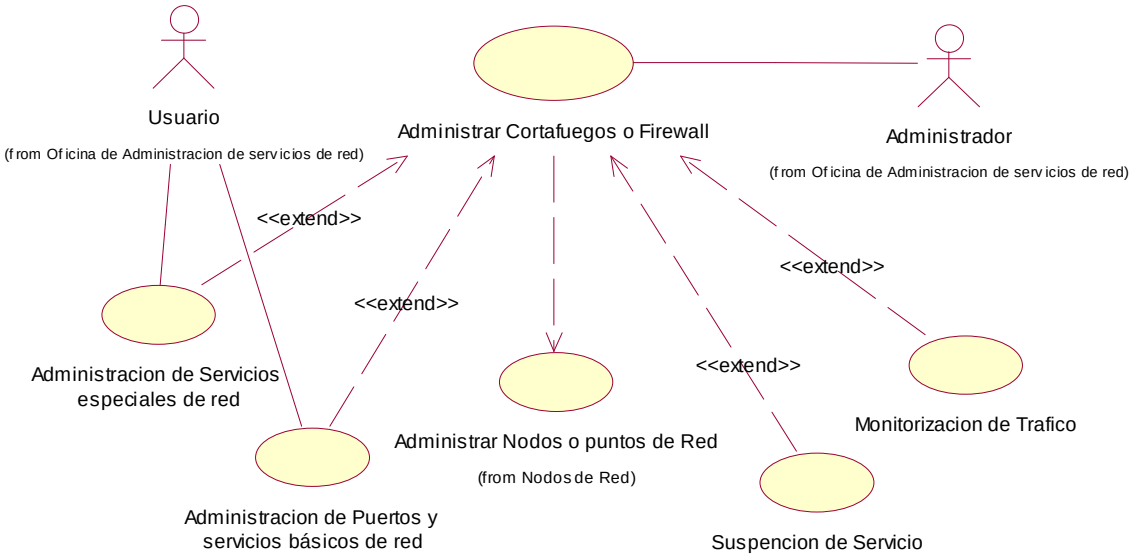


Figura 21. Administración Firewall.

5.5.10 Diagrama de caso de uso: autenticar

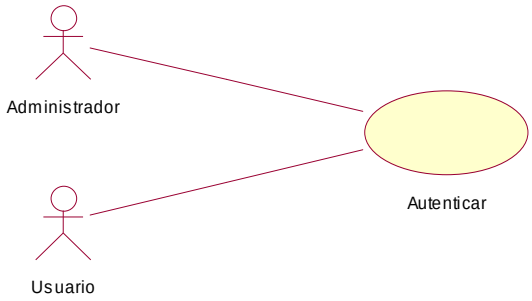


Figura 22. Autenticar Usuario.

5.6 DIAGRAMAS DE INTERACCION

5.6.1 Diagramas de secuencia

5.6.1.1 Diagrama de Secuencia: Controlar Usuarios

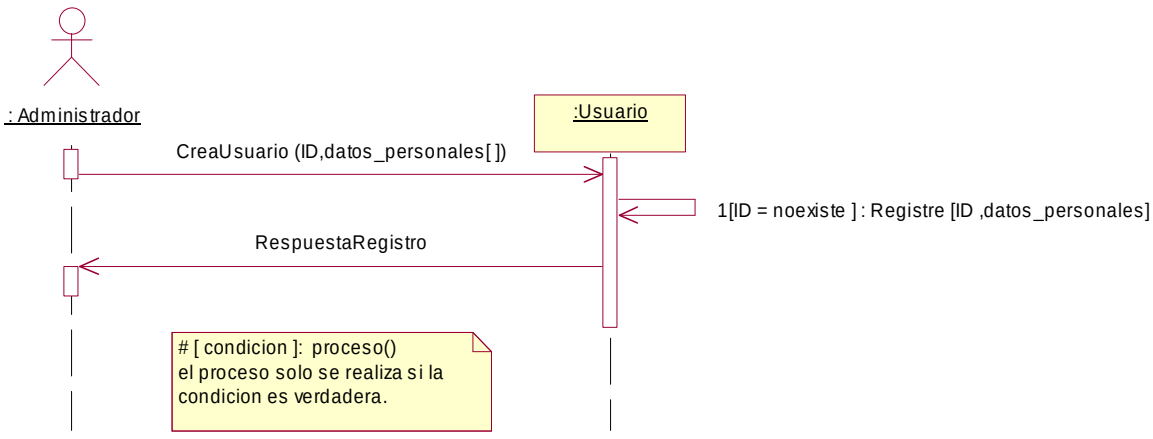


Figura 23. Secuencia, Controlar usuarios.

5.6.1.2 Diagrama de Secuencia: Controlar infraestructura Física

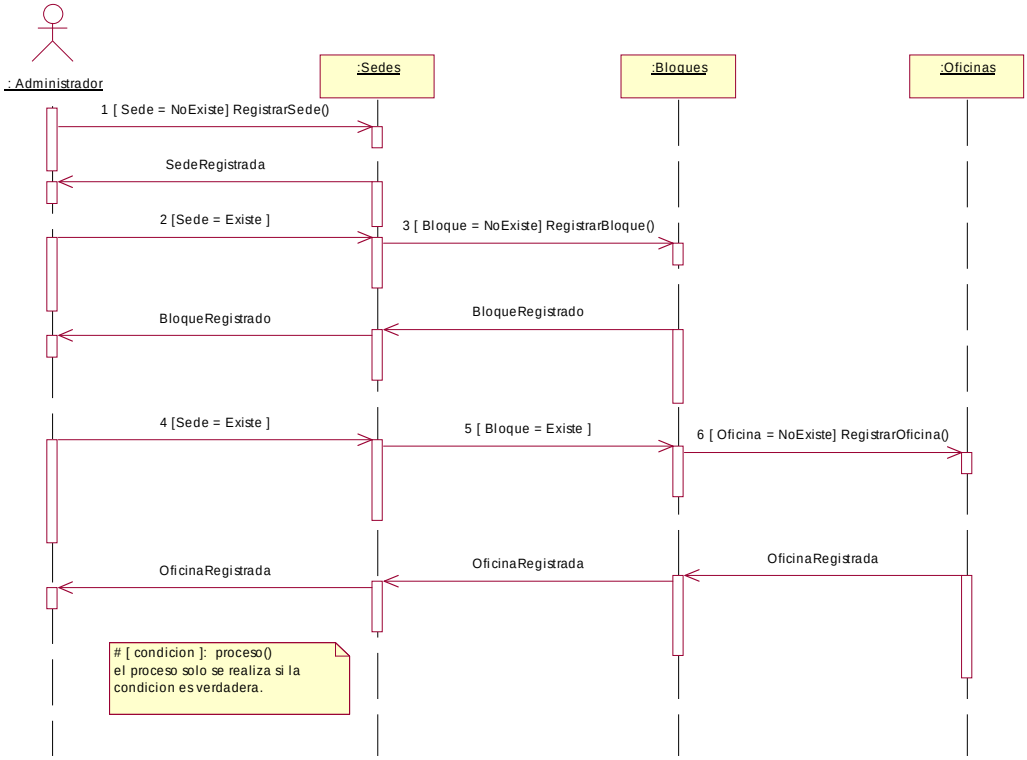


Figura 24. Secuencia, Controlar infraestructura física.

5.6.1.3 Diagrama de Secuencia: Administrar Publicaciones Web (Administrador)

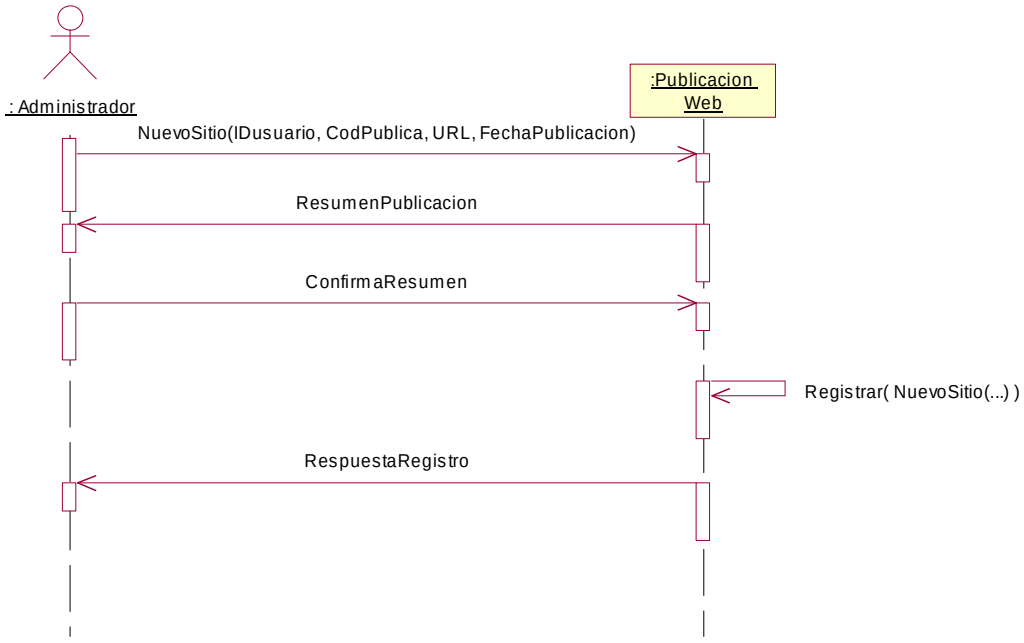


Figura 25. Secuencia, Administrar publicaciones Web (Administrador).

5.6.1.4 Diagrama de Secuencia: Administrar Publicaciones Web (Usuario)

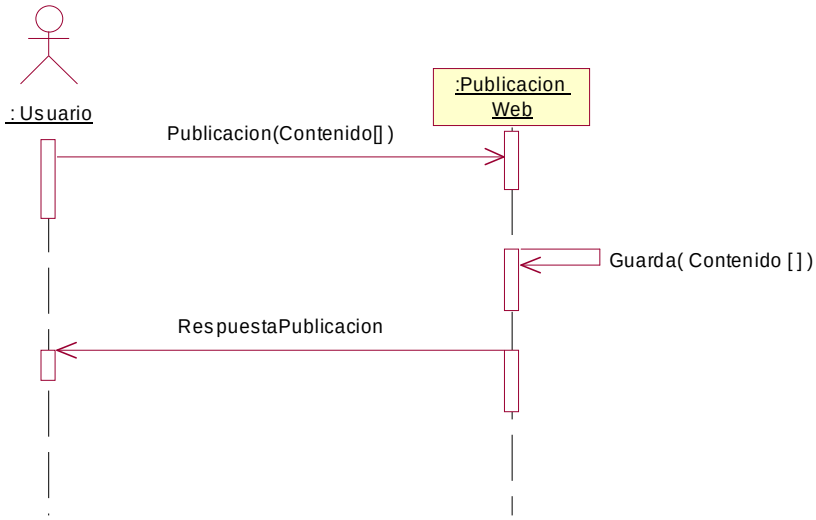


Figura 26. Secuencia, Administrar publicaciones Web (Usuario).

5.6.1.5 Diagrama de secuencia: Administrar Correo Electrónico (Administrador)

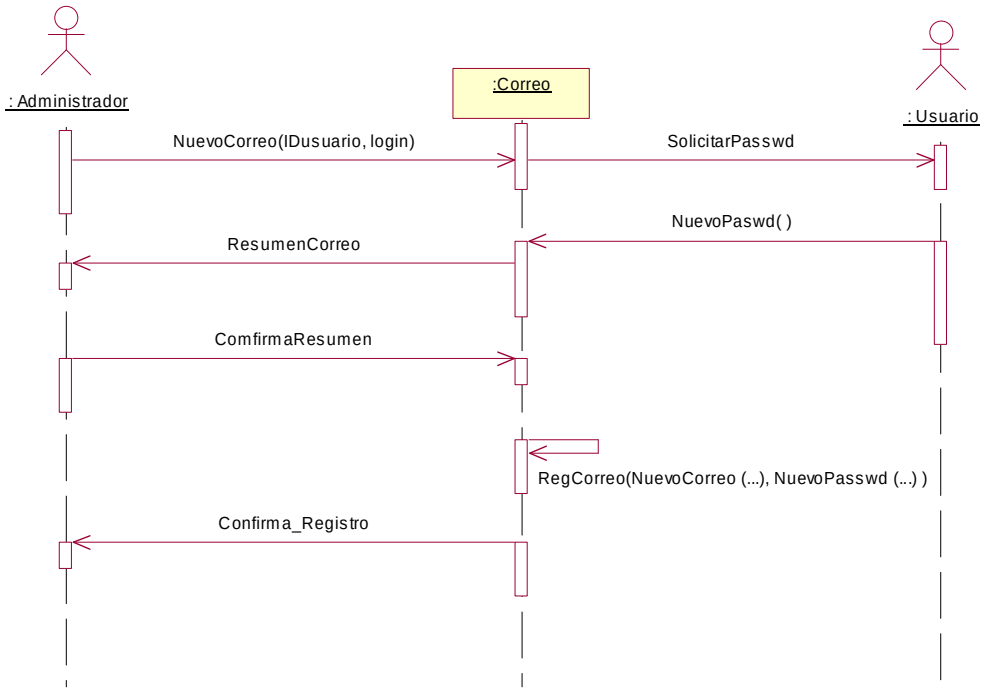


Figura 27. Secuencia, Administrar correo electrónico.

5.6.1.6 Diagrama de Secuencia: Administrar Correo Electrónico (Usuario)

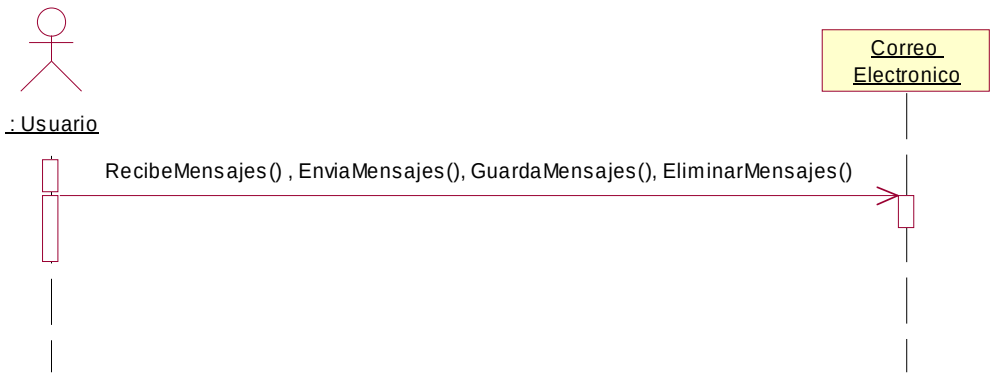


Figura 28. Secuencia, Administrar correo electrónico (Usuario).

5.6.1.7 Diagrama de Secuencia: Administrar nodos o puntos de red.

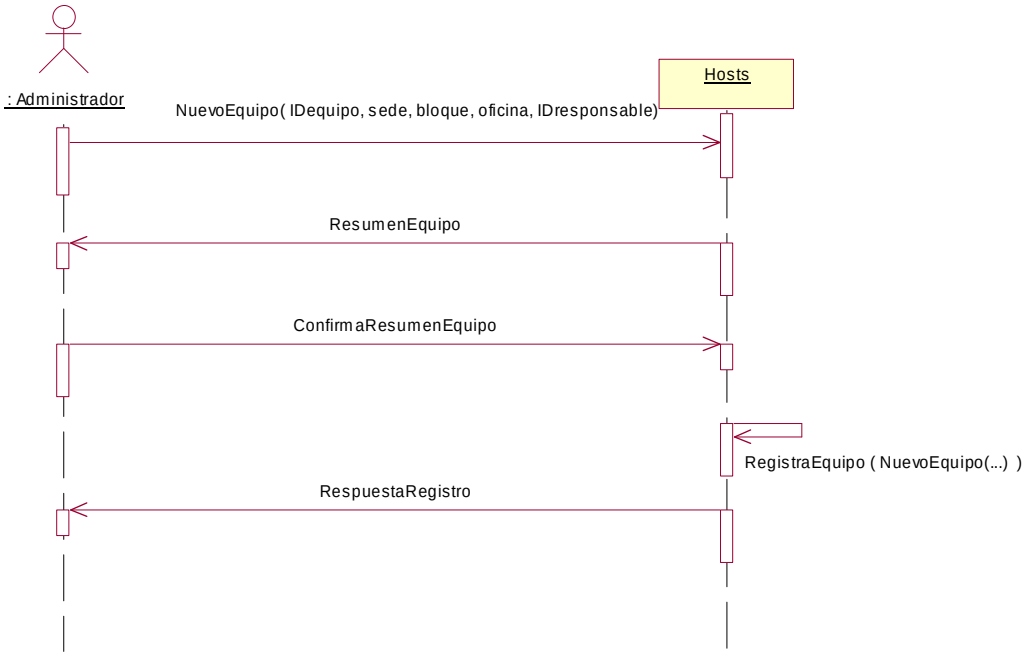


Figura 29. Secuencia, Administrar nodos o puntos de red.

5.6.1.8 Diagrama de Secuencia: Controlar Ancho de Banda

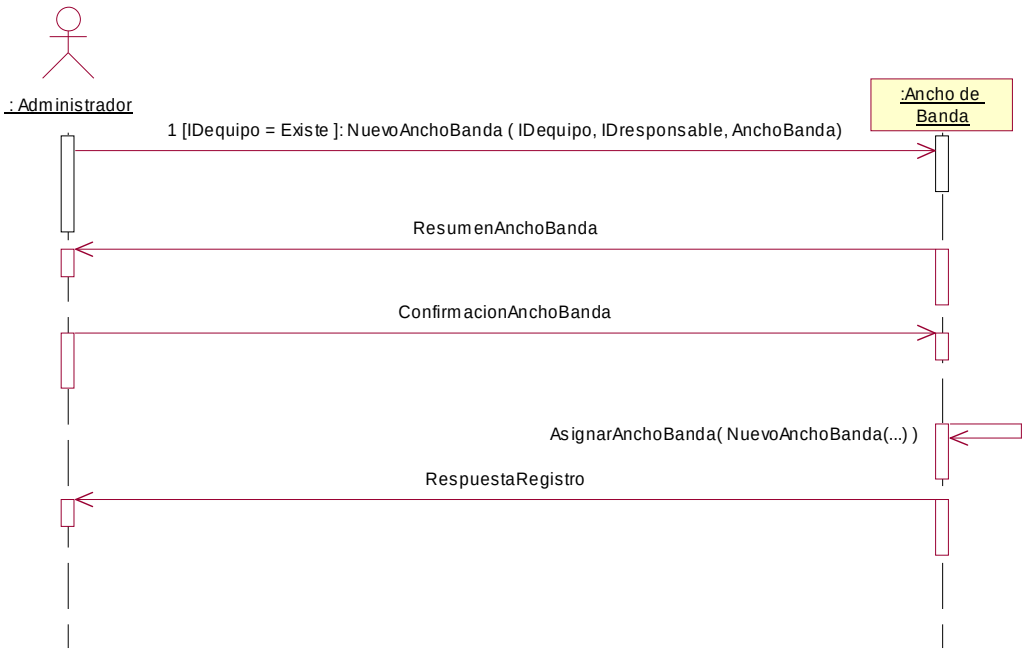


Figura 30. Secuencia, Controlar ancho de banda.

5.6.1.9 Diagrama de Secuencia: Administrar Servidor Proxy

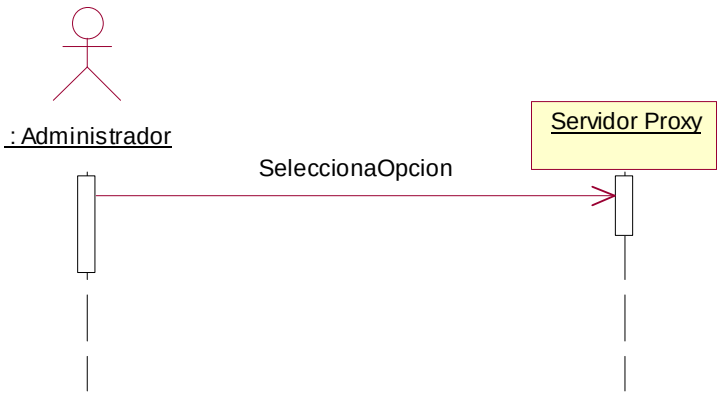


Figura 31. Secuencia, Administrar servidor Proxy.

5.6.1.10 Diagrama de Secuencia: Administrar Servidor Proxy (Subredes Proxy)

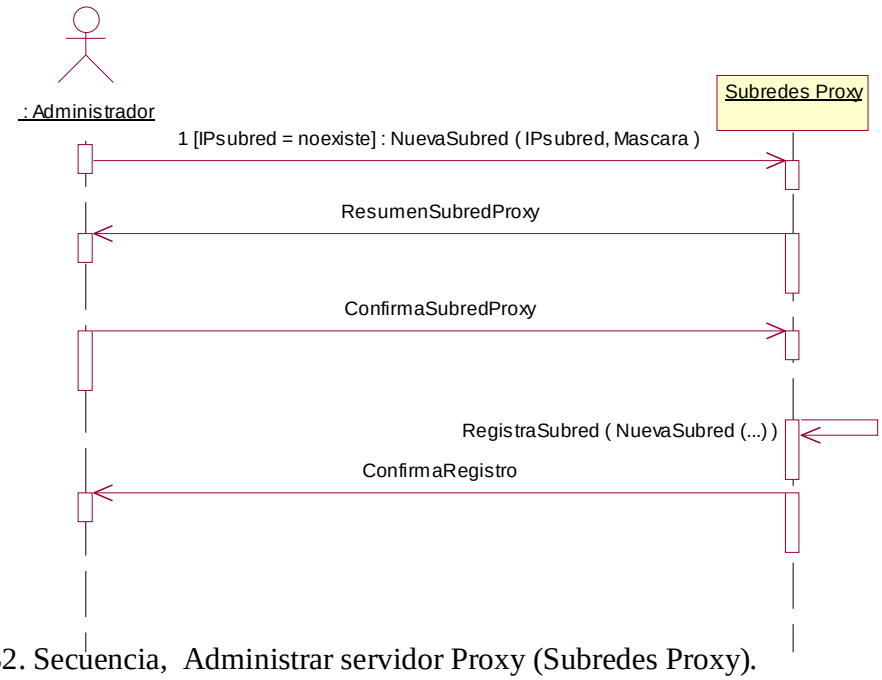


Figura 32. Secuencia, Administrar servidor Proxy (Subredes Proxy).

5.6.1.11 Diagrama de Secuencia: Administrar Servidor Proxy (Controlar Tipos de Archivo)

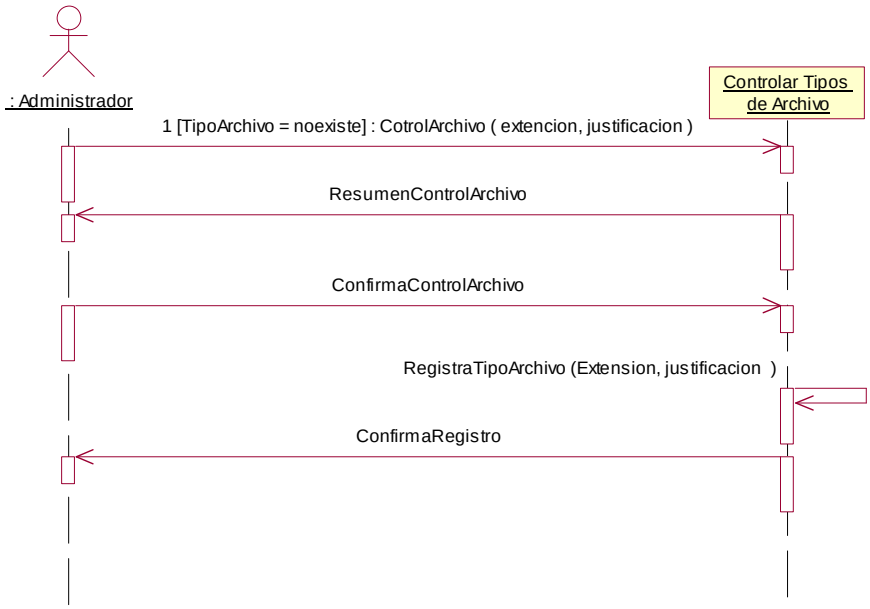


Figura 33. Secuencia, Administrar servidor Proxy (Controlar tipos de archivo).

5.6.1.12 Diagrama de Secuencia: Administrar Servidor Proxy (Mantenimiento Caché)

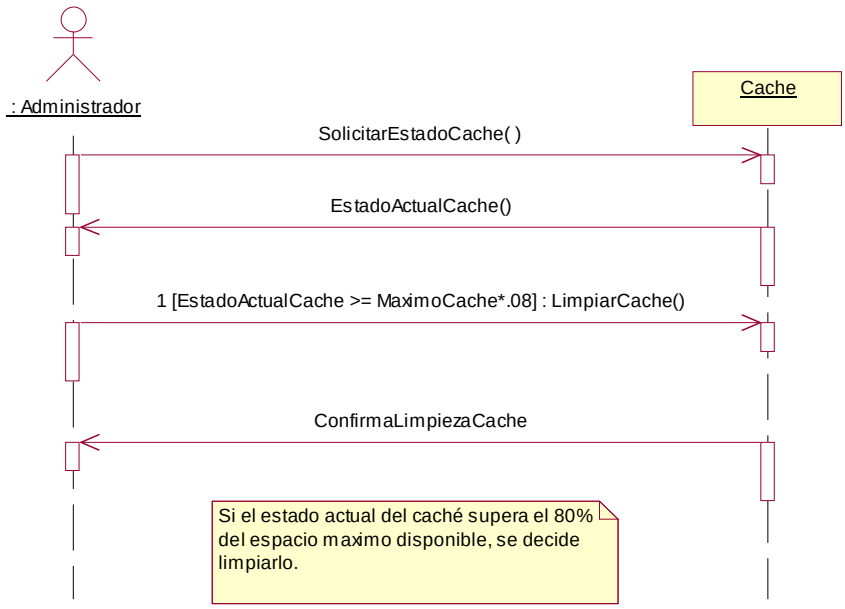


Figura 34. Secuencia, Administrar servidor Proxy (Mantenimiento Caché).

5.6.1.13 Diagrama de Secuencia: Administrar Servidor Proxy (Control de Eventos Internos)

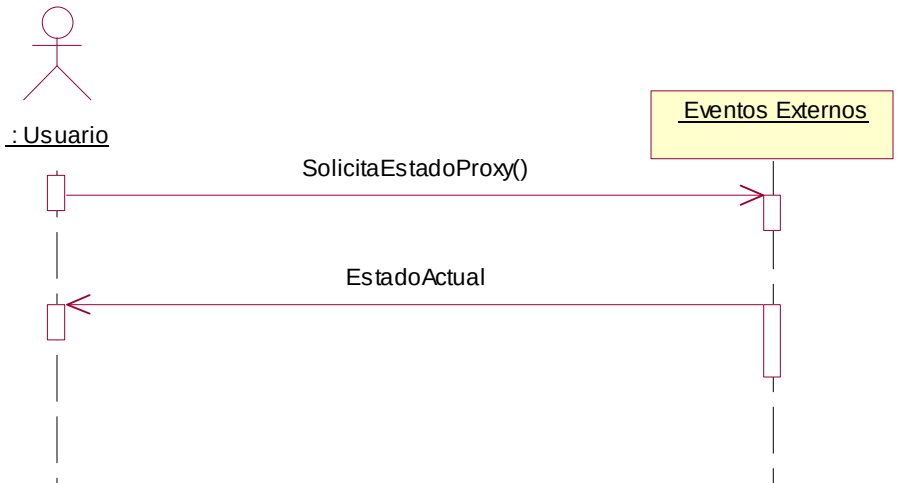


Figura 35. Secuencia, Administrar servidor Proxy (Control de eventos Internos).

5.6.1.14 Diagrama de Secuencia: Administrar Filtro Web

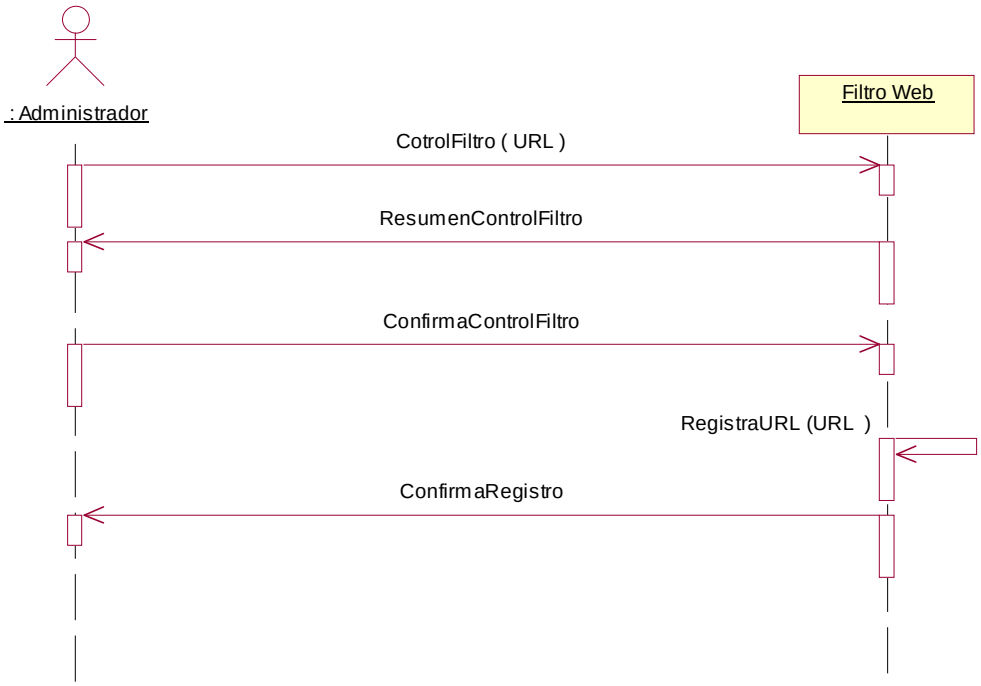


Figura 36. Secuencia, Administrar filtro Web.

5.6.1.15 Diagrama de Secuencia: Administrar Corta fuegos (firewall)

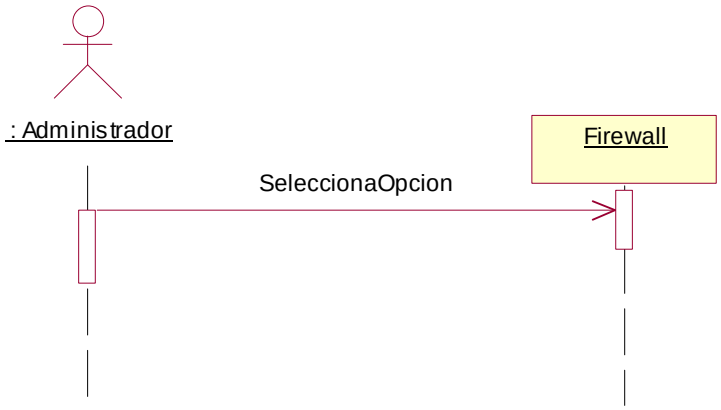


Figura 37. Secuencia, Administrar Firewall.

5.6.1.16 Diagrama de Secuencia: Administración de puertos y servicios básicos de red

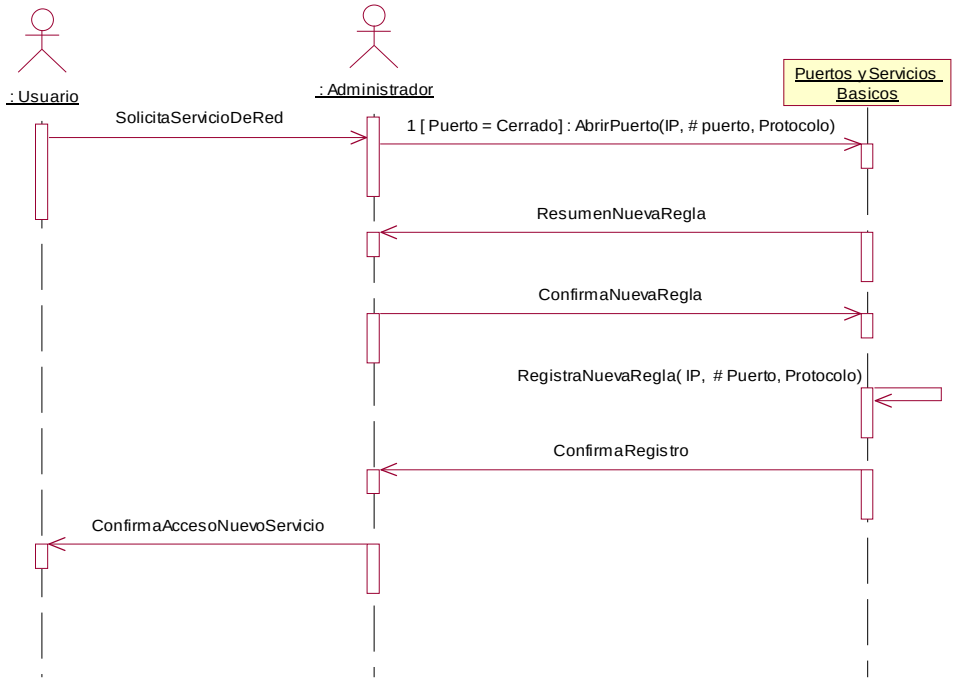


Figura 38. Secuencia, Administrar puertos y servicios básicos de red.

5.6.1.17 Diagrama de Secuencia: Administración Servicios especiales de red

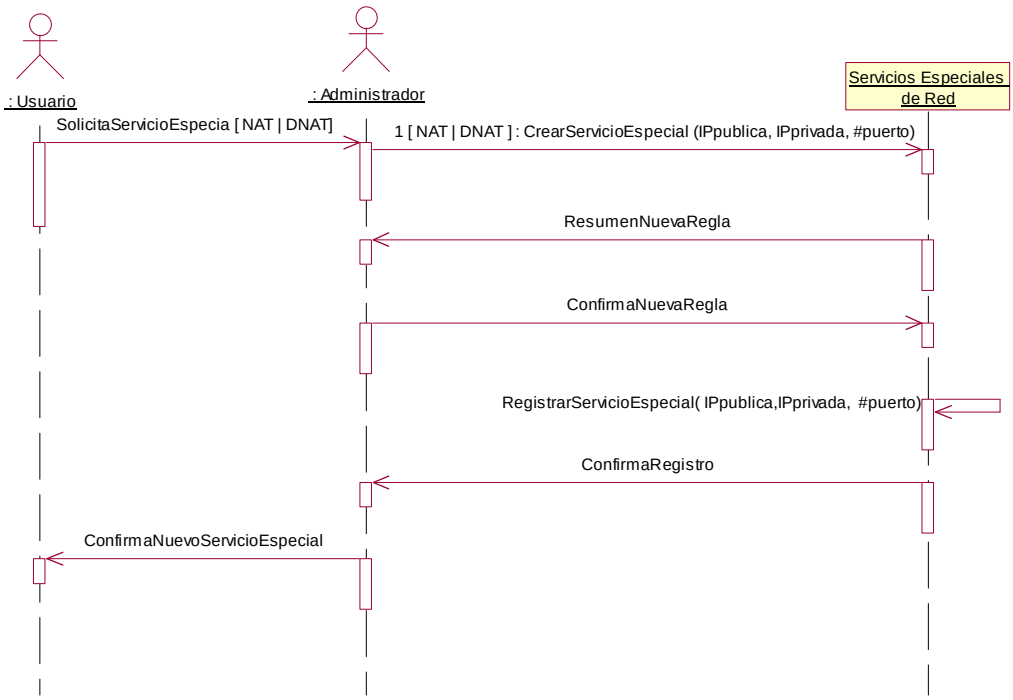


Figura 39. Secuencia, Administrar servicios especiales de red.

5.6.1.18 Diagrama de Secuencia: Monitorizar de Tráfico

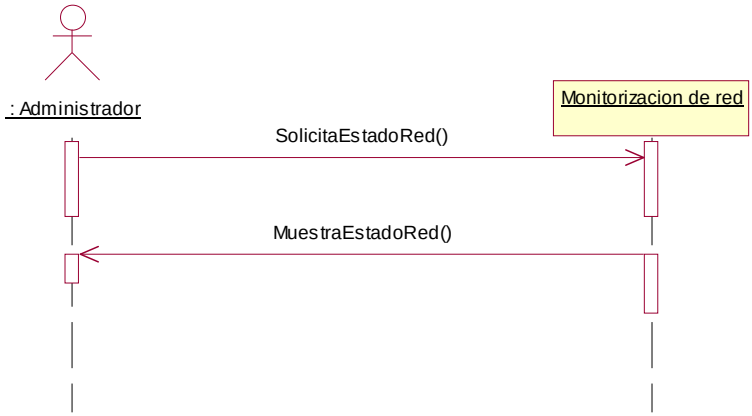


Figura 40. Secuencia, Monitorizar Tráfico.

5.6.1.19 Diagrama de Secuencia: Suspensión de Servicio

Figura 41. Secuencia, Suspensión de servicio.

5.6.1.20 Diagrama de Secuencia: Autenticar

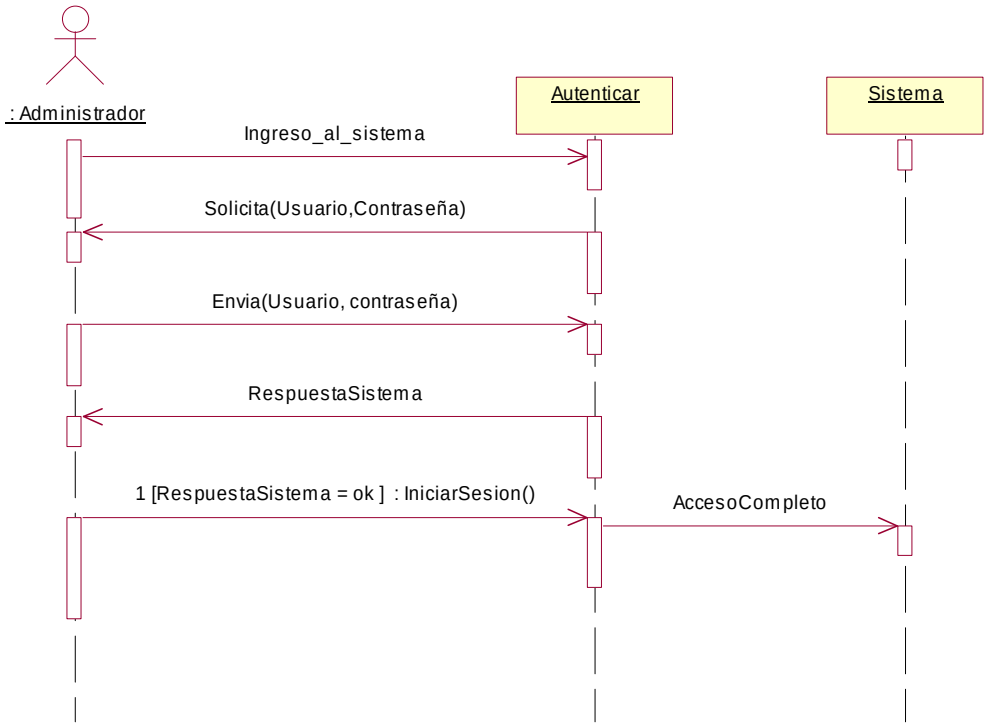


Figura 42. Secuencia, Autenticar usuario.

5.6.2 Diagramas de colaboración

5.6.2.1 Diagrama de Colaboración: Controlar Usuarios

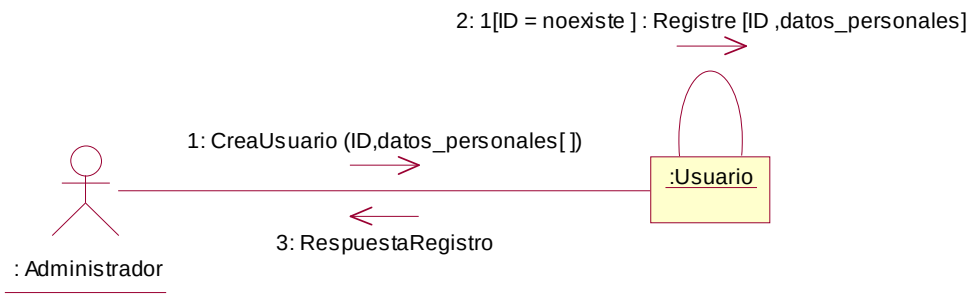


Figura 43. Colaboración, Controlar usuarios.

5.6.2.2 Diagrama de Colaboración: Controlar infraestructura Física

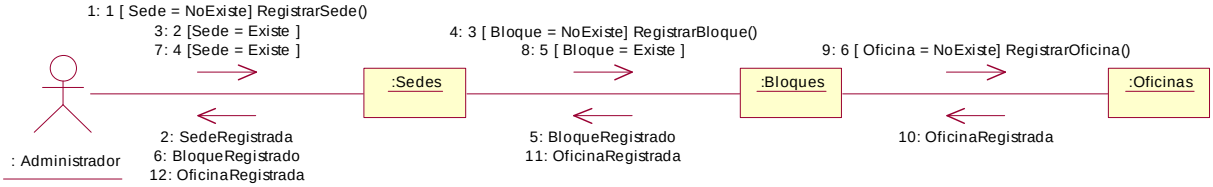


Figura 44. Colaboración, Controlar infraestructura física.

5.6.2.3 Diagrama de Colaboración: Administrar Publicaciones Web (Administrador)

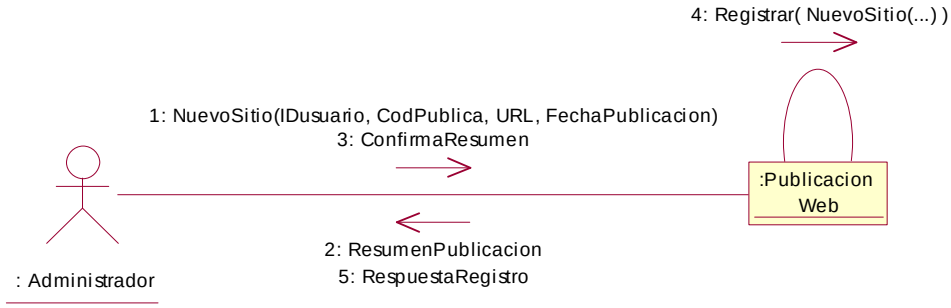


Figura 45. Colaboración, Administrar publicaciones Web (Administrador).

5.6.2.4 Diagrama de Colaboración: Administrar Publicaciones Web (Usuario)

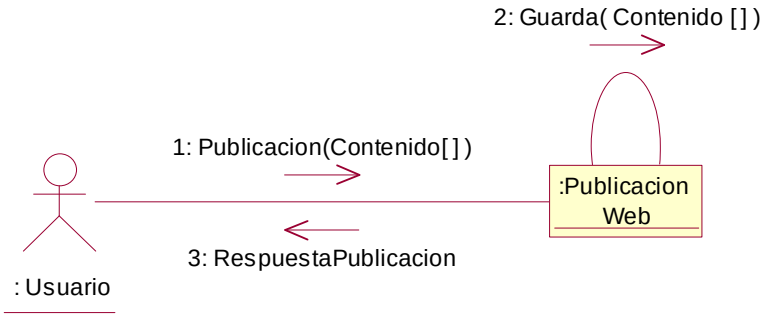


Figura 46. Colaboración, Administrar publicaciones Web (Usuario).

5.6.2.5 Diagrama de Colaboración: Administrar Correo Electrónico (Administrador)

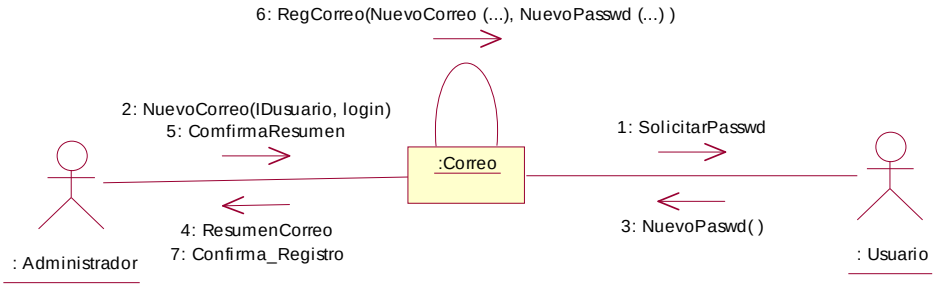


Figura 47. Colaboración, Administrar correo electrónico (Administrador).

5.6.2.6 Diagrama de Colaboración: Administrar Correo Electrónico (Usuario)

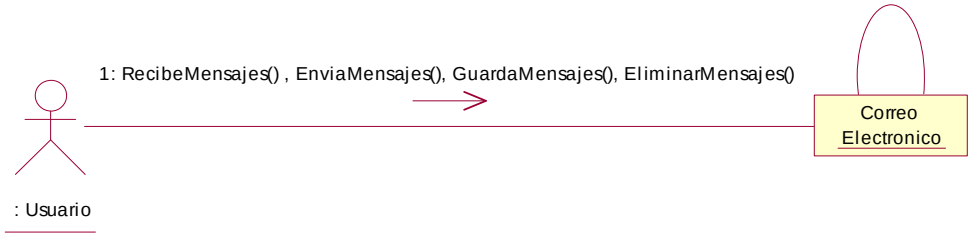


Figura 48. Colaboración, Administrar correo electrónico (Usuario).

5.6.2.7 Diagrama de Colaboración: Administrar nodos o puntos de red.

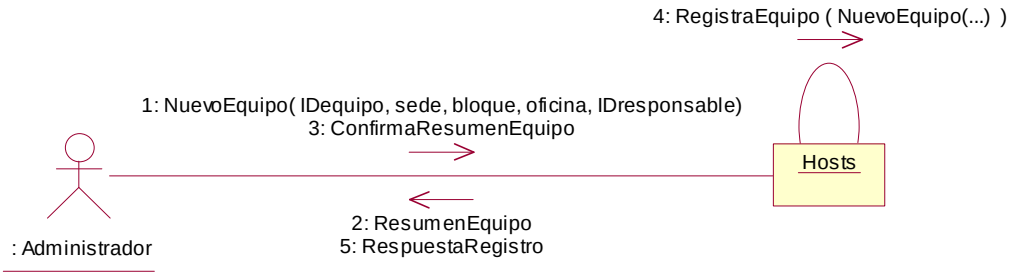


Figura 49. Colaboración, Administrar nodos o puntos de red.

5.6.2.8 Diagrama de Colaboración: Controlar Ancho de Banda

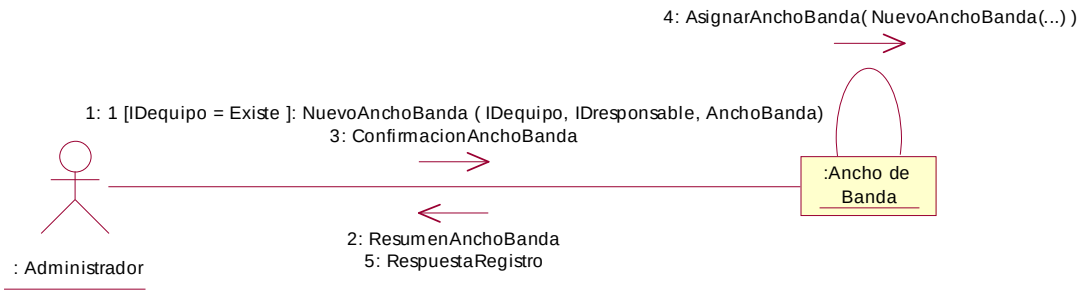


Figura 50. Colaboración, Controlar ancho de banda.

5.6.2.9 Diagrama de Colaboración: Administrar Servidor Proxy

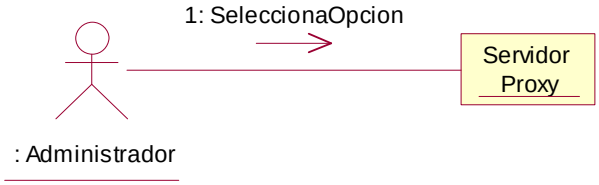


Figura 51. Colaboración, Administrar servidor Proxy.

5.6.2.10 Diagrama de Colaboración: Administrar Servidor Proxy (Subredes Proxy)

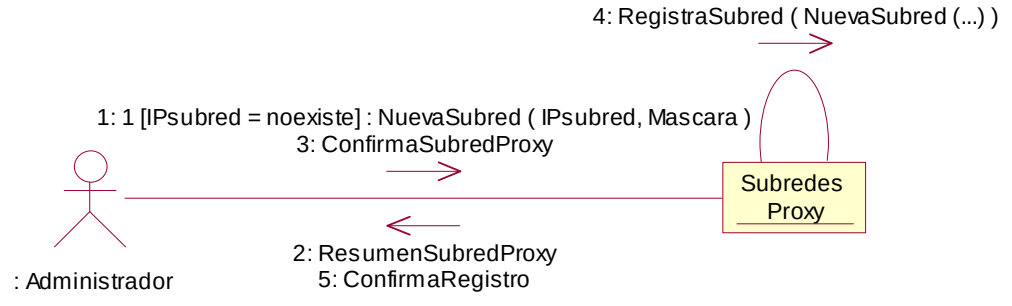


Figura 52. Colaboración, Administrar Servidor Proxy (Subredes Proxy).

5.6.2.11 Diagrama de Colaboración: Administrar Servidor Proxy (Controlar Tipos de Archivo)

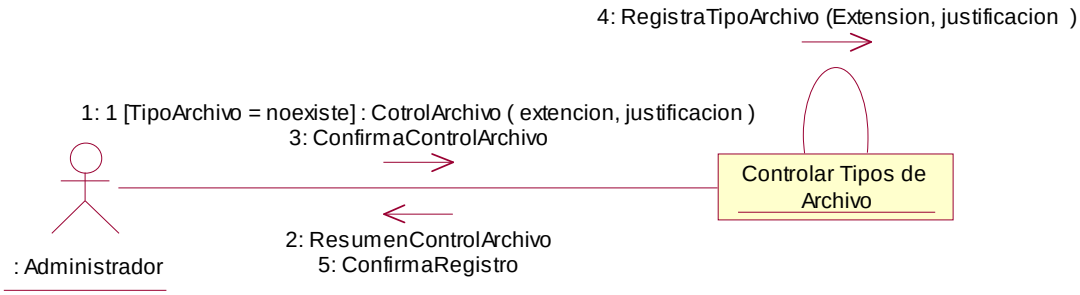


Figura 53. Colaboración, Administrar servidor Proxy (Controla tipos de archivo).

5.6.2.12 Diagrama de Colaboración: Administrar Servidor Proxy (Mantenimiento Caché)

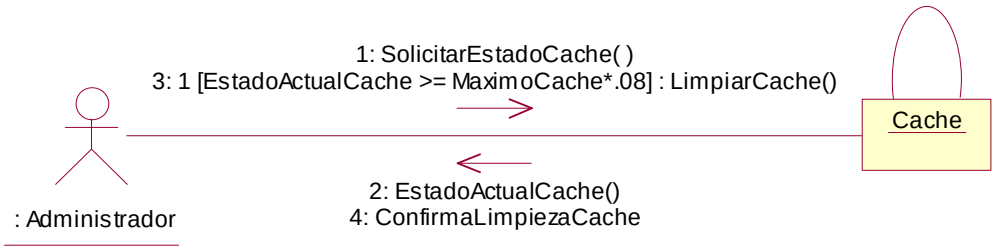


Figura 54. Colaboración, Administrar Servidor Proxy (Mantenimiento de Caché).

5.6.2.13 Diagrama de Colaboración: Administrar Servidor Proxy (Control de Eventos Externos)

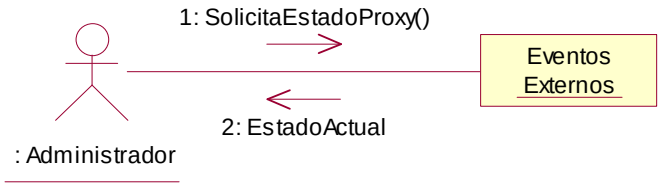


Figura 55. Colaboración: Administrar Servidor Proxy (Control de Eventos Externos).

5.6.2.14 Diagrama de Colaboración: Administrar Filtro Web

Figura 56. Colaboración: Administrar filtro Web.

5.6.2.15 Diagrama de Colaboración: Administrar Corta fuegos (firewall)

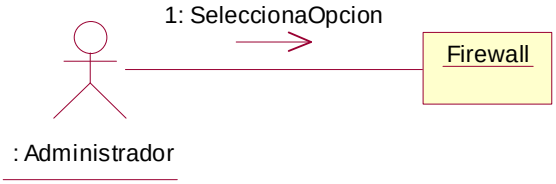


Figura 57. Colaboración, Administrar Corta fuegos (firewall)).

5.6.2.16 Diagrama de Colaboración: Administración de puertos y servicios básicos de red

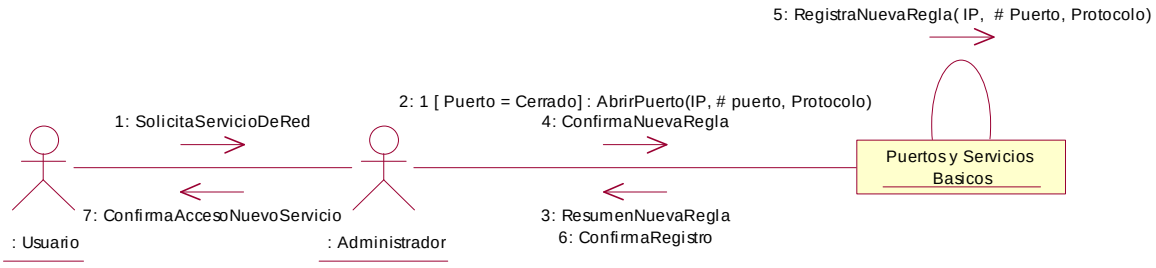


Figura 58. Colaboración, Administrar Corta fuegos (firewall).

5.6.2.17 Diagrama de Colaboración: Administración Servicios especiales de red

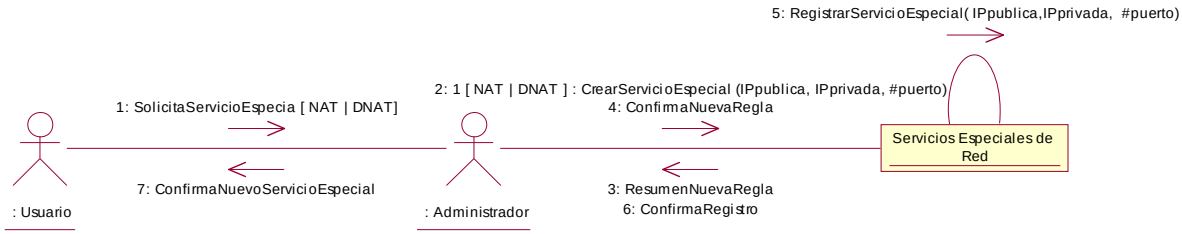


Figura 59. Colaboración, Administrar Corta fuegos (firewall).

5.6.2.18 Diagrama de Colaboración: Monitorización de Tráfico

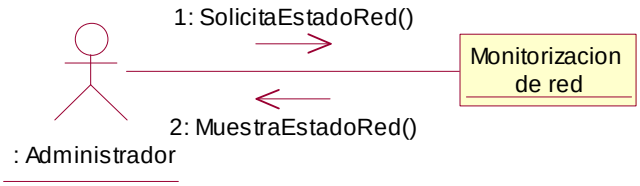


Figura 60. Colaboración, Monitorizar Tráfico.

5.6.2.19 Diagrama de Colaboración: Suspensión de Servicio

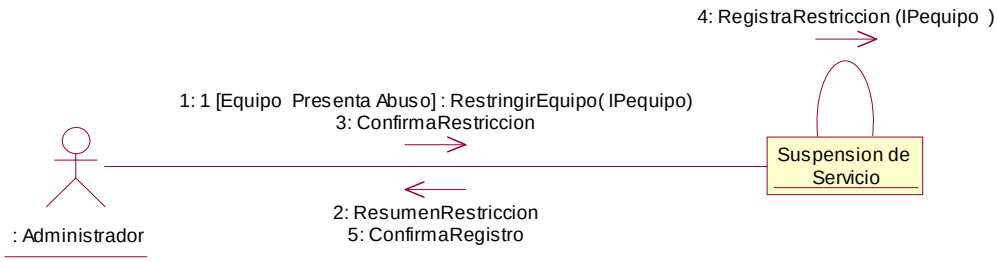


Figura 61. Colaboración, Suspensión de Servicio.

5.6.2.20 Diagrama de Colaboración: Autenticar

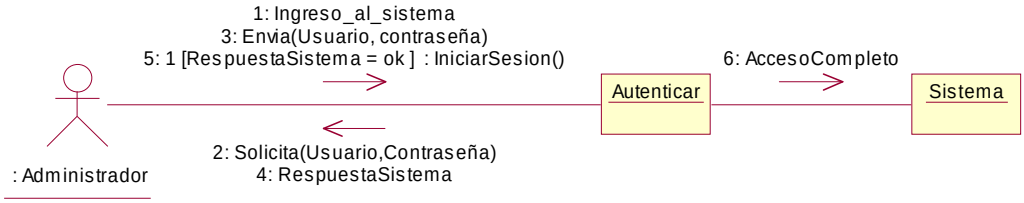
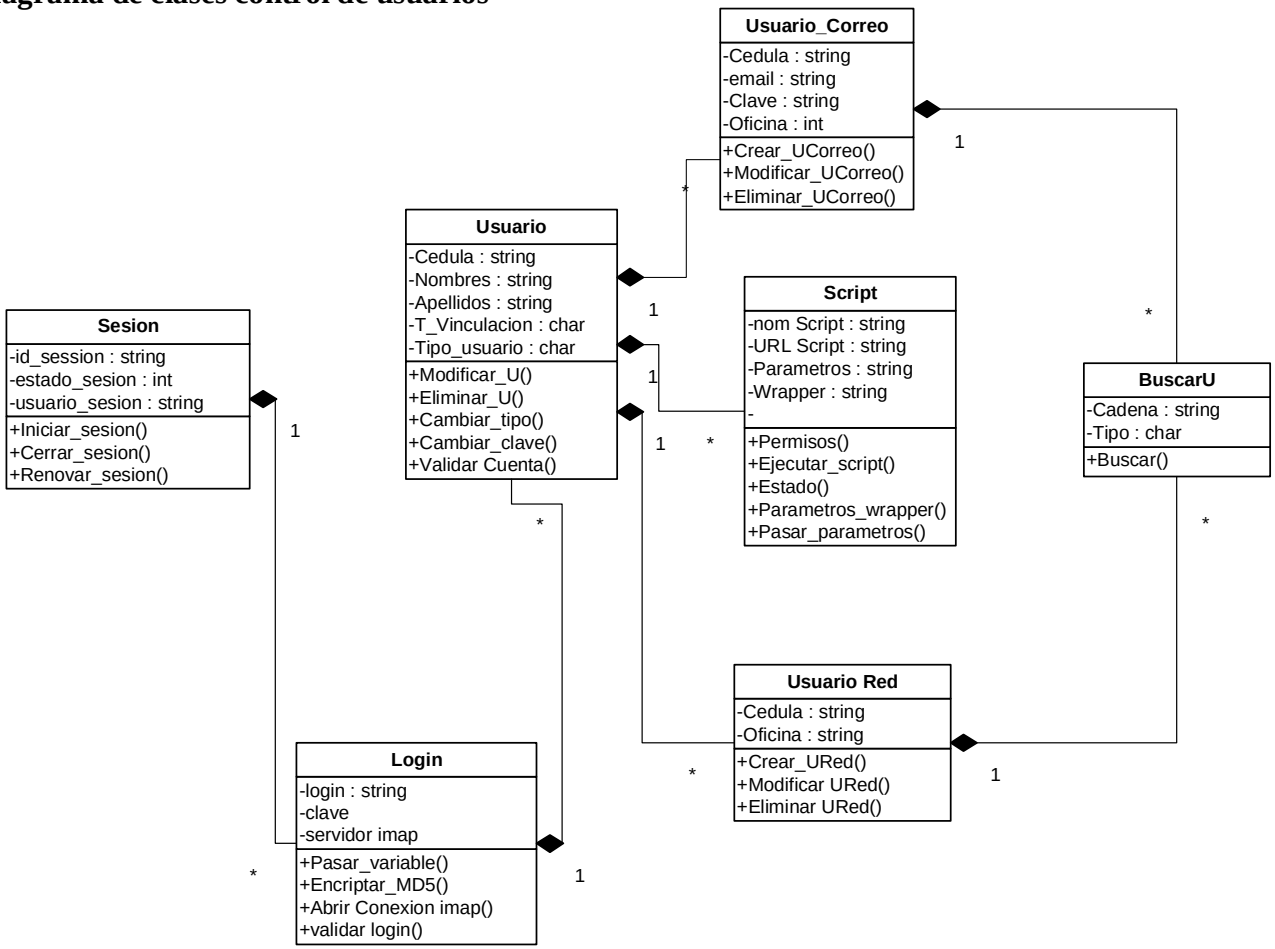


Figura 62. Colaboración, Autenticar usuario.

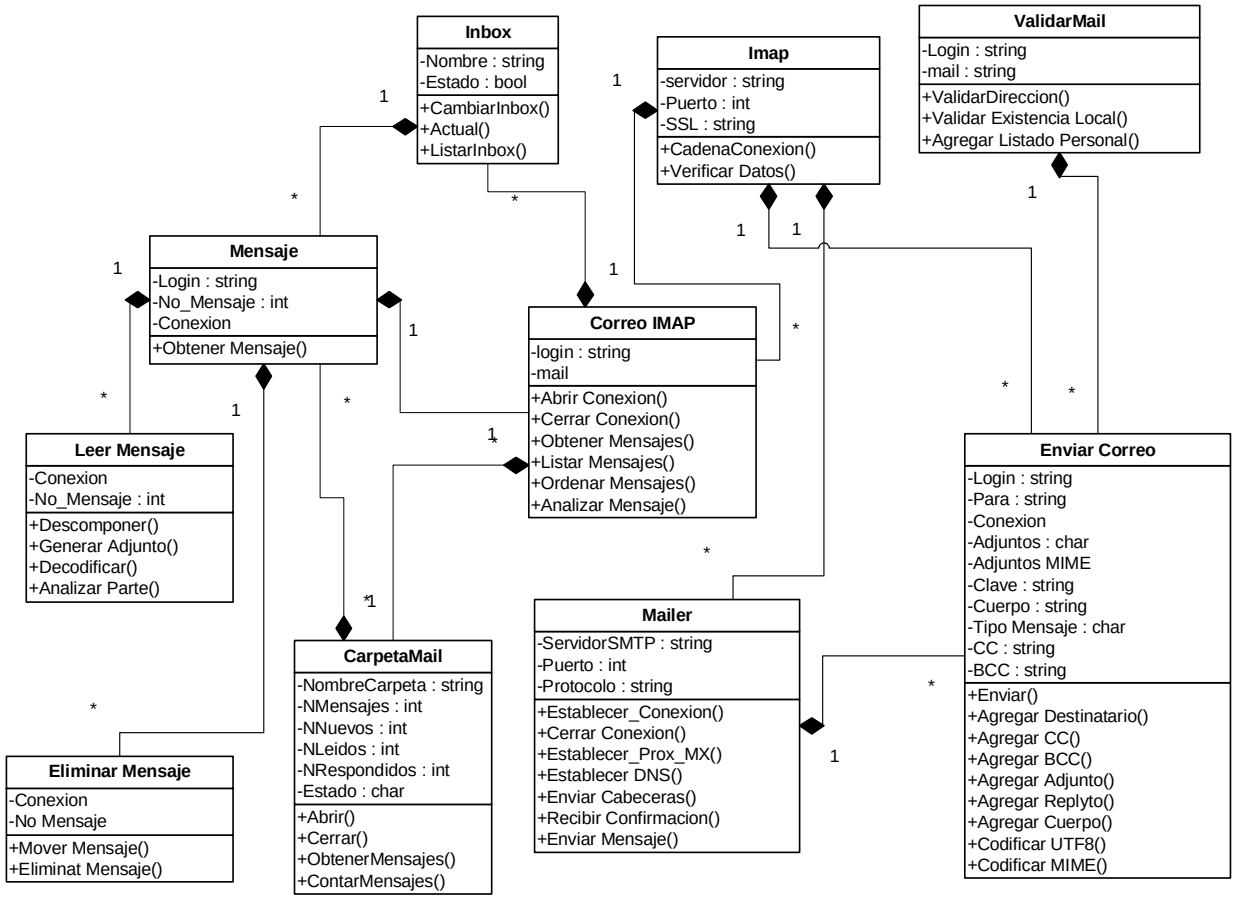
5.7 DIAGRAMA DE CLASES

5.7.1 Diagrama de clases control de usuarios



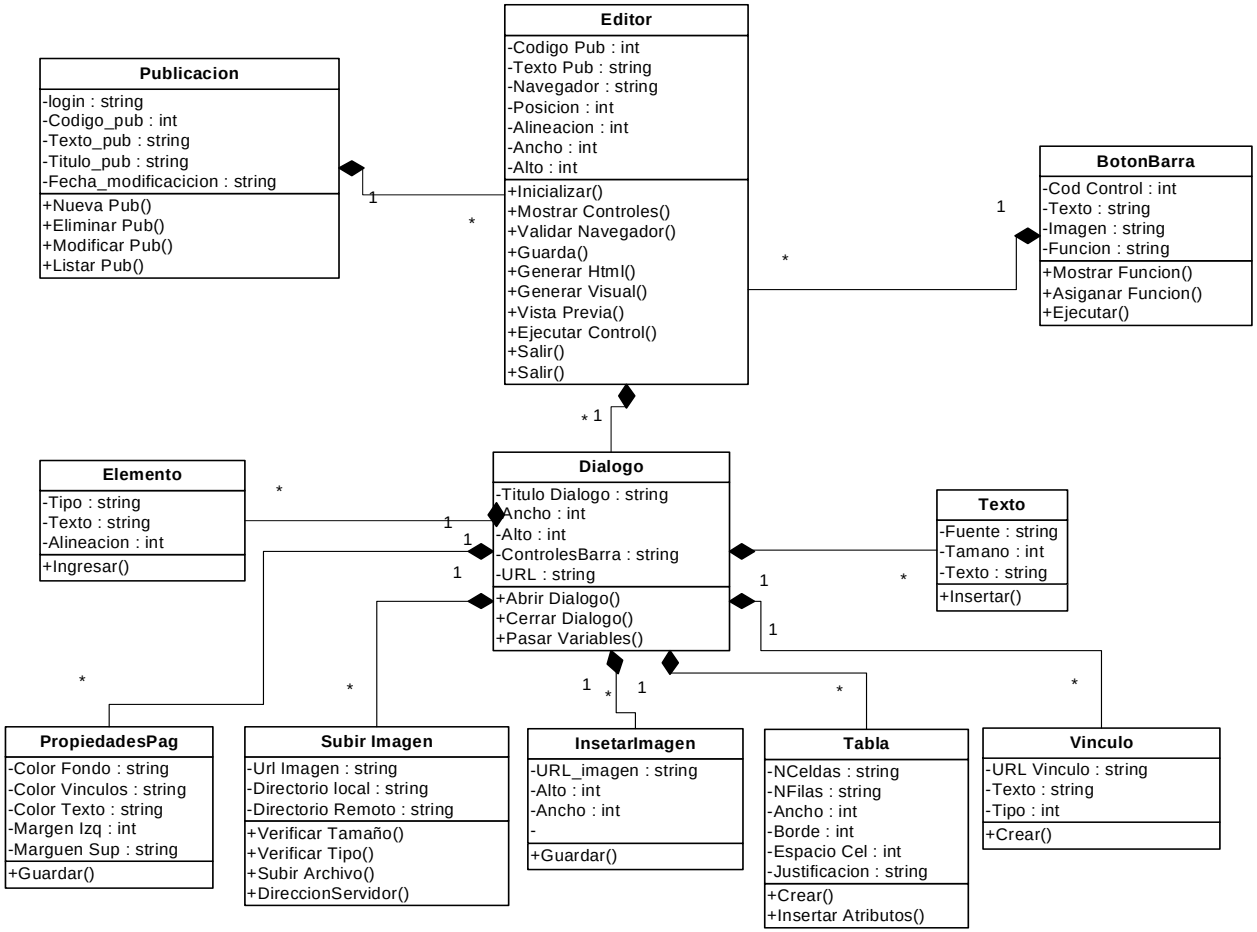
Esquema 15. Diagrama de clases control de usuarios.

5.7.2 Diagrama de clases correo electrónico



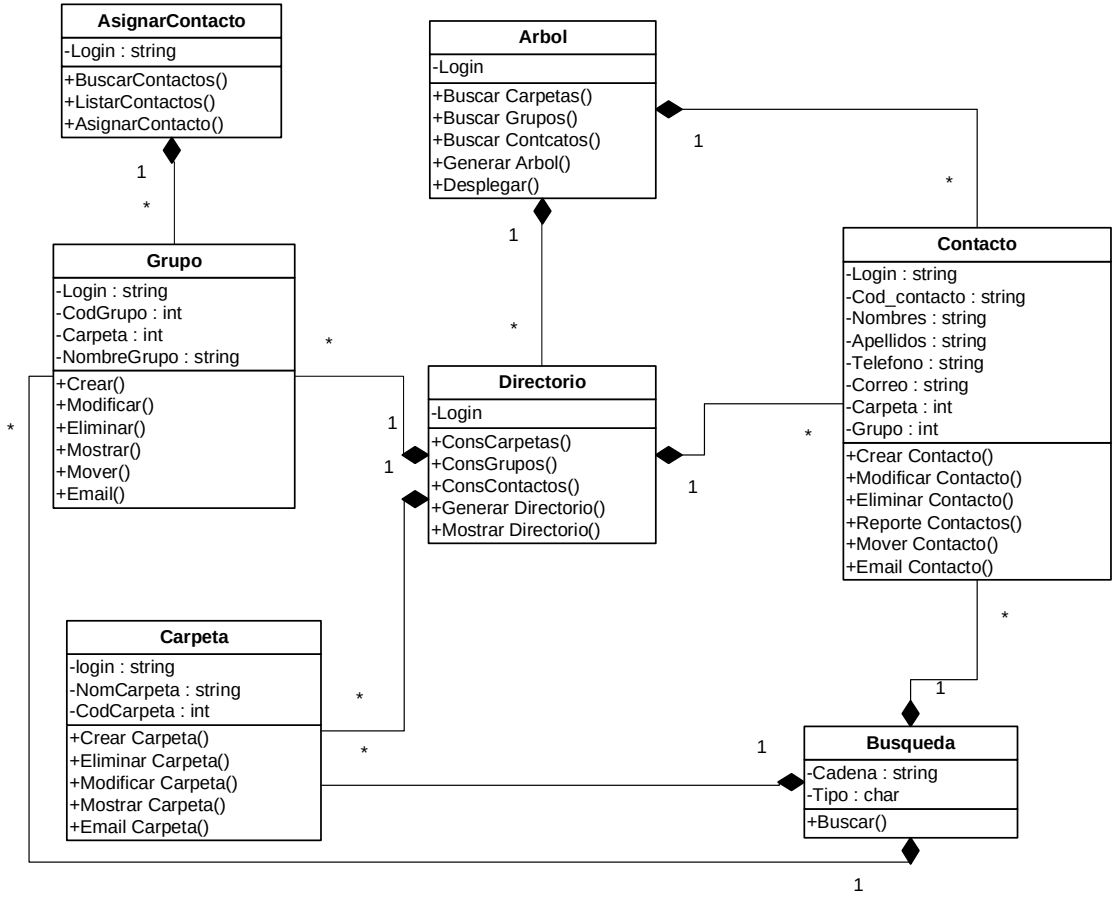
Esquema 16. Diagrama de clases correo electrónico.

5.7.3 Diagrama de clases publicaciones web



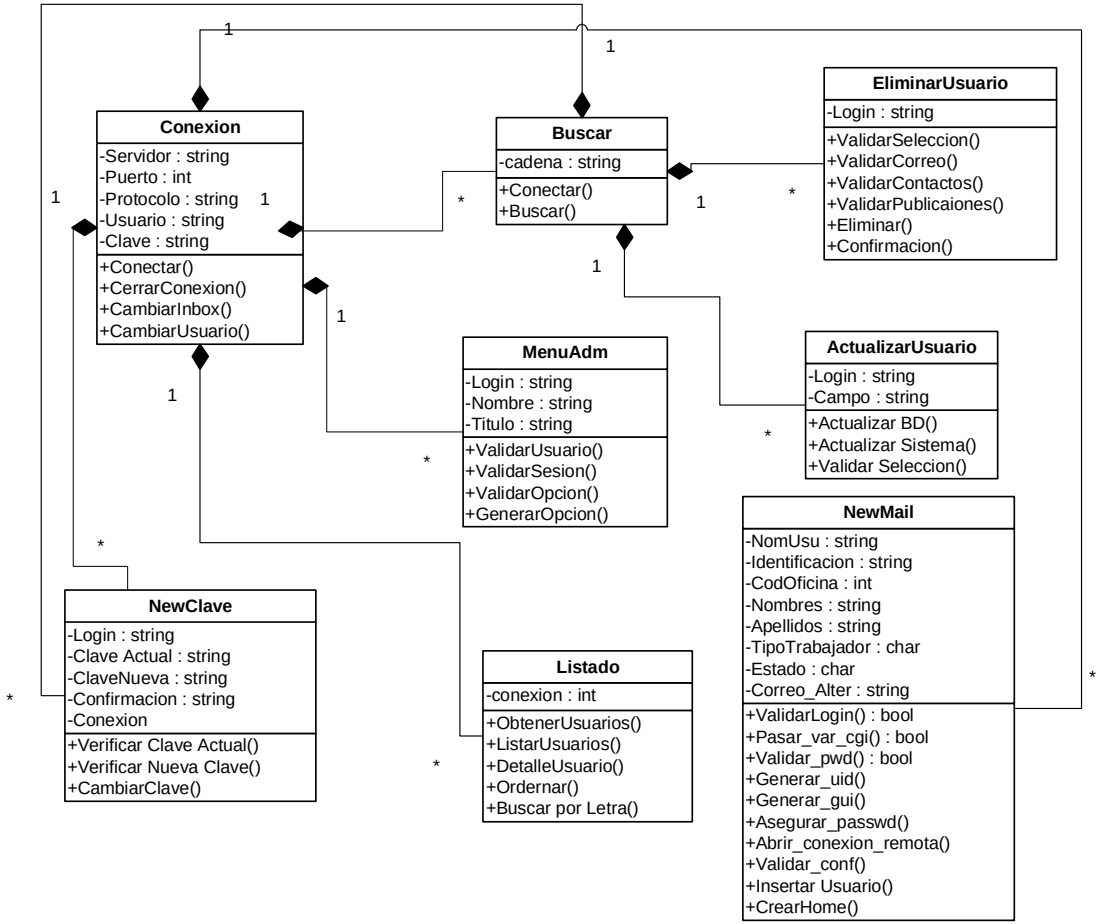
Esquema 17. Diagrama de clases de publicaciones Web.

5.7.4 Diagrama de clases de contactos de correo y directorio.



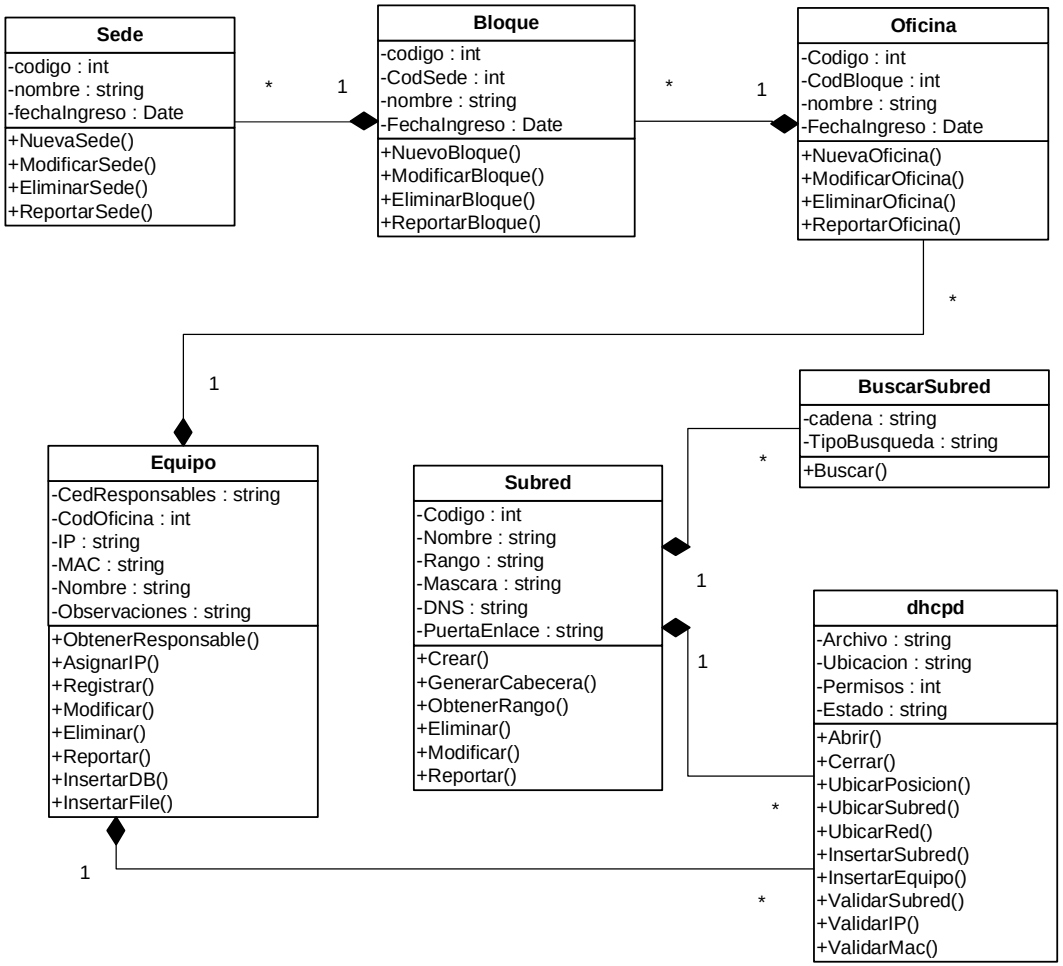
Esquema 18. Diagrama de clases de contactos de correo y directorio.

5.7.5 Diagrama de clases de administración de correo electrónico (modo administrador).



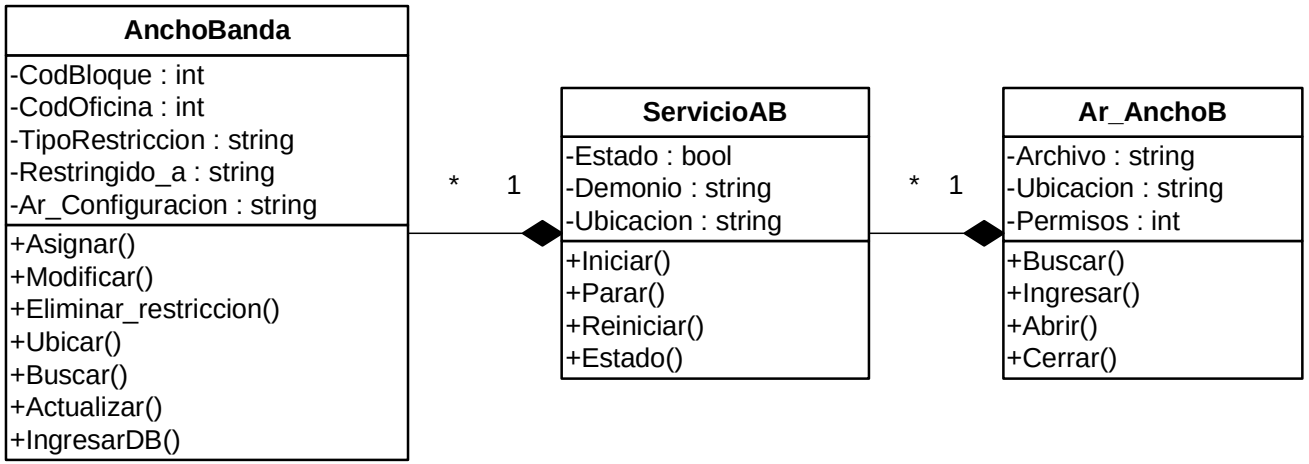
Esquema 19. Diagrama de clases de administración de correo electrónico (modo administrador).

5.7.6 Diagrama de clases administración de nodos de red.



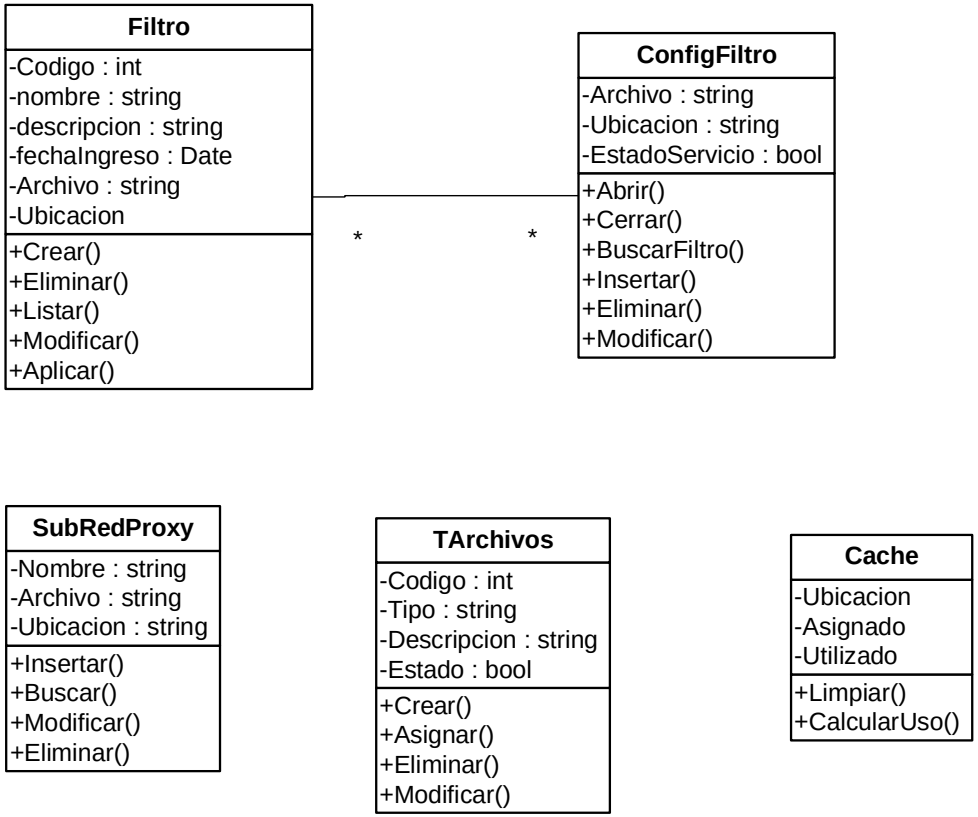
Esquema 20. Diagrama de clases administración de nodos de red.

5.7.7 Diagrama de clases control de ancho de banda.



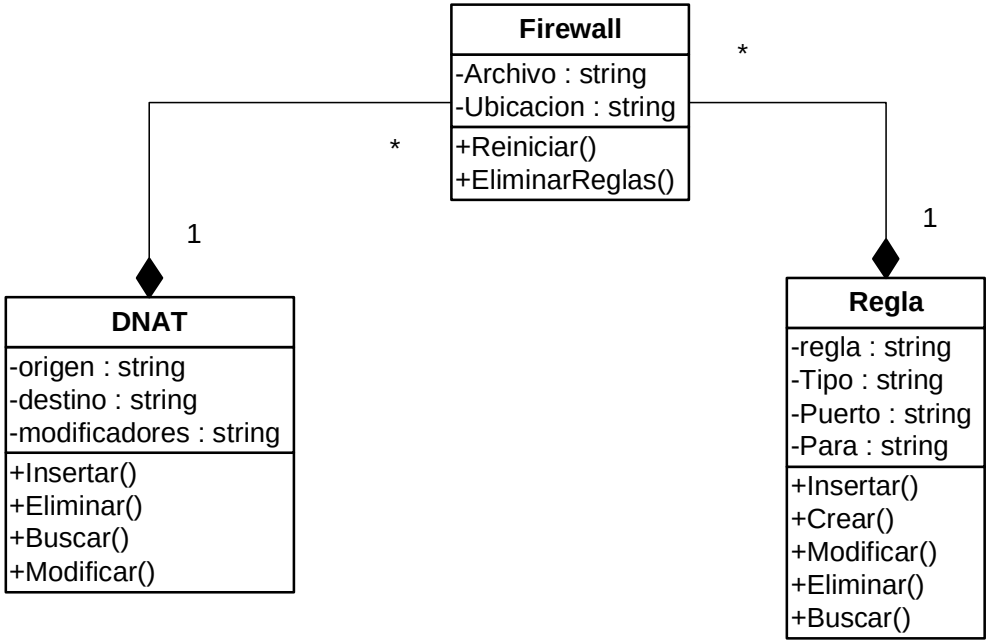
Esquema 21. Diagrama de clases control de ancho de banda.

5.8.8 Diagrama de clases administración de servidor proxy y filtro web



Esquema 22. Diagrama de clases administración de servidor proxy y filtro Web.

5.7.8 Diagrama de clases de administración de cortafuegos (firewall)



Esquema 23. Diagrama de clases de administración de cortafuegos (firewall).

6. DISEÑO ORIENTADO A OBJETOS DEL SISTEMA ANUBIS

6.1 CASOS DE USO REALES ANUBIS

6.1.1 Ingreso de usuarios

Figura 63. Ingreso al Sistema.

Pantalla Inicial

Caso de Uso: Autenticar
Actores: Administrador del sistema y usuario de correo
Propósito: Valida Información de acceso de usuarios.
Resumen: Acceso al sistema, mediante nombre de usuario y contraseña asignada.

Curso Normal de los Eventos

1. Este caso de uso comienza cuando se necesita acceder al sistema.
2. El sistema muestra la pantalla acceso al sistema como se muestra en la Figura 63.
3. El actor introduce los parámetros de acceso como: Nombre de Usuario en A, y contraseña en B, pulsa en ingresar para acceder.
4. El sistema realiza la validación de los campos de usuario y contraseña.

5. El sistema verifica el tipo de usuario que esta accediendo al sistema, Administrador o usuario Normal.
6. Se da acceso al sistema, dependiendo del tipo de usuario se muestran las opciones principales y su reporte de correo electrónico.

Cursos Alternos:

Línea 4: Si la información de acceso es incorrecta o nula, el sistema impedirá la entrada presentando nuevamente la ventana de login.

6.1.2 Correo electrónico (bandeja de entrada)

Figura 64. Bandeja de Entrada

Caso de Uso: Administrar correo electrónico (Usuario)
Actores: Administrador del sistema ó Usuario de correo
Propósito: Administrar Correo Electrónico del usuario.
Resumen: Presenta un listado y opciones de manejo del correo que posea el usuario en su bandeja de entrada o carpeta seleccionada.

Curso Normal de los Eventos

1. Este caso de uso comienza cuando se accede al sistema.
2. El sistema genera un listado detallado de los mensajes de correo, y opciones de administración de los mismos, indicando remitente G, asunto H, fecha I y tamaño J.
3. Calcula el número de Mensajes K, el espacio ocupado L y botones de control para navegar entre los mensajes M.
4. Analiza el estado de cada uno de los mensajes de correo E.

Línea 2: Si el tiempo de inactividad supera los 5 minutos, el sistema regresara a la página general de acceso.

6.1.2.1 Correo Electrónico (Redacción de Correo)

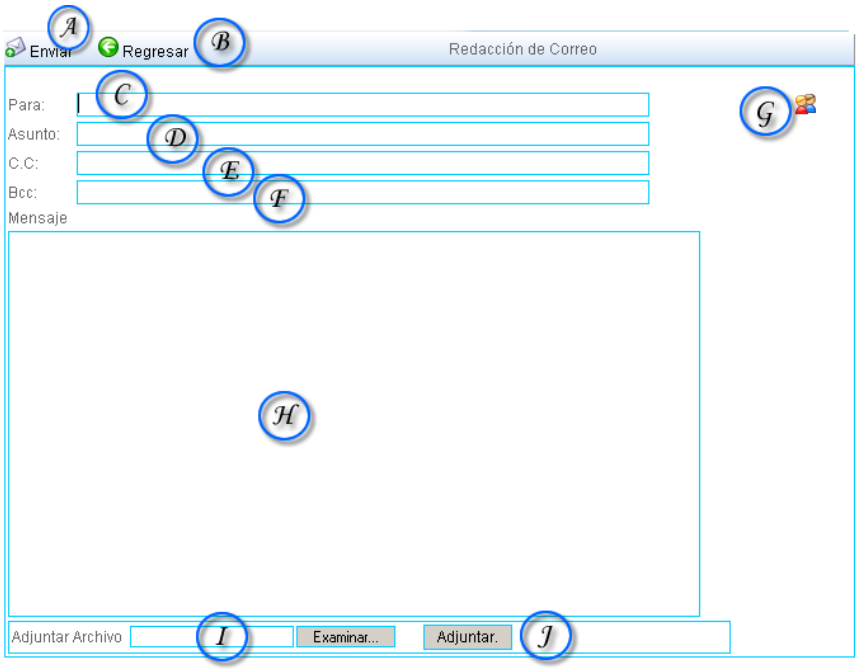


Figura 65. Envió de Mensaje de correo electrónico.

Caso de Uso: Administrar correo electrónico (Usuario) sección redactar mensaje.
Actores: Administrador del sistema ó usuario de correo
Propósito: Enviar mensaje de Correo Electrónico.

Resumen: El sistema permite la redacción de correos electrónicos, procesándolos y enviándolos al destinatario que el usuario desee, de cualquier servidor de correo.

Curso Normal de los Eventos

1. Esta sección de caso de uso comienza cuando el actor desea enviar un mensaje de correo electrónico.
2. El actor accede a la función de redacción de correos Figura 2 en la opción A.
3. El sistema genera un listado de los últimos correos enviados, y los prepara para generar una lista desplegable en C.
4. Se Muestra la pantalla como en la Figura 3, se prepara para recibir la dirección del destinatario C.
5. El actor ingresa la dirección o direcciones a las cuales desea enviar el mensaje de correo. Ingresa el Asunto D del mensaje, agrega copias E y F.
6. Si desea agregar destinatarios del libro de contactos personal, presiona G para elegirlos.

Línea 2: Si los destinatarios no existen se retorna un mensaje de error, de igual manera si los campos C o D están vacíos.

6.1.2.2 Correo Electrónico (Leer Mensaje)

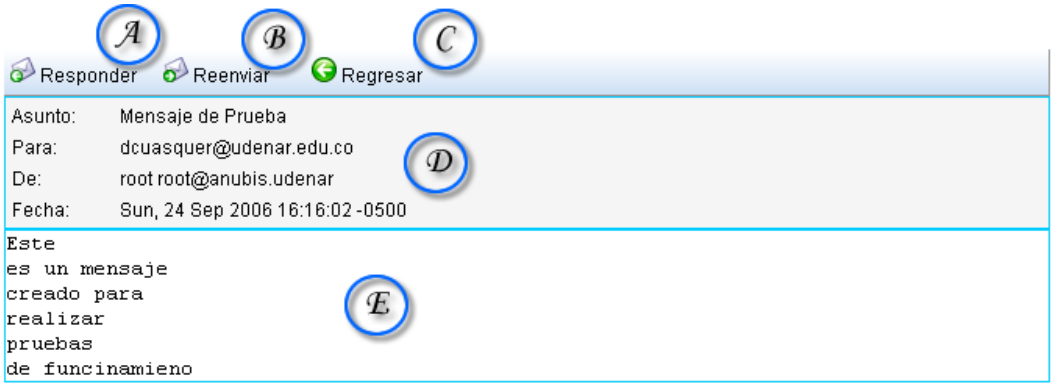


Figura 66. Lectura de mensajes de Correo.

Caso de Uso: Administrar correo electrónico (Usuario) sección leer mensaje
Actores: Administrador del sistema ó usuario de correo
Propósito: Leer mensaje de correo electrónico.
Resumen: Presenta al usuario información detallada del mensaje, el cuerpo del mensaje y accesos directos para la descarga de archivos de adjuntos al mensaje.

Curso Normal de los Eventos

1. Esta sección de caso de uso comienza cuando el actor desea conocer el contenido de un mensaje de correo electrónico mostrado en su bandeja de entrada.
2. El actor presiona sobre el Asunto del mensaje H en la Figura 64.
3. El sistema genera un informe detallado sobre la información del mensaje D Figura 66.
4. El sistema analiza las partes del mensaje determinando si posee o no archivos adjuntos que vincular.
5. En caso de ser un mensaje multiparte con archivos adjuntos, descarga una copia temporal en el servidor y genera un vínculo de descarga a este.
6. Muestra la partes del mensaje en las que se encuentre texto, convirtiéndolo a codificación UTF-8.
7. Para responder al mensaje oprime A si quiere regresar oprime C.
8. Muestra la pantalla como en la Figura 67.
9. Guarda la información sobre el remitente.
10. Redacta el mensaje a responder.
11. Oprime A para responder al mensaje.
12. Para reenviar el mensaje oprime B
13. Muestra la pantalla como en la Figura 68.
14. Guarda la información sobre el cuerpo del mensaje.
15. Digita la dirección o direcciones destinatarias.
16. Oprime A para Reenviar el mensaje

Línea 15: Si las direcciones de correo no son correctas, no se podrá reenviar el mensaje.

6.1.2.3 Correo Electrónico (Administración de Carpetas de Correo)

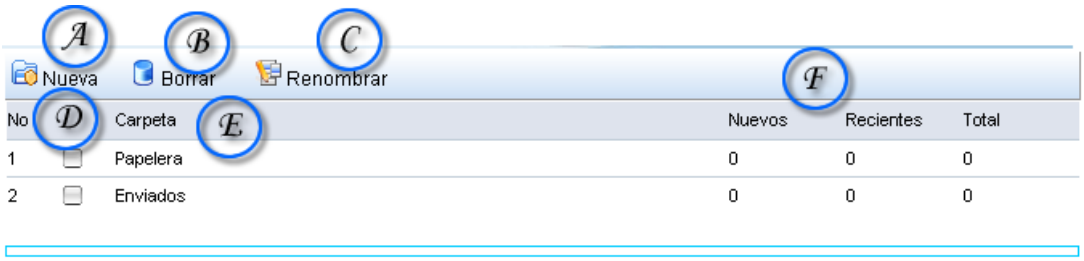


Figura 67. Carpetas de correo Electrónico.

6.1.2.4 Correo Electrónico (Crear Carpeta de Correo)

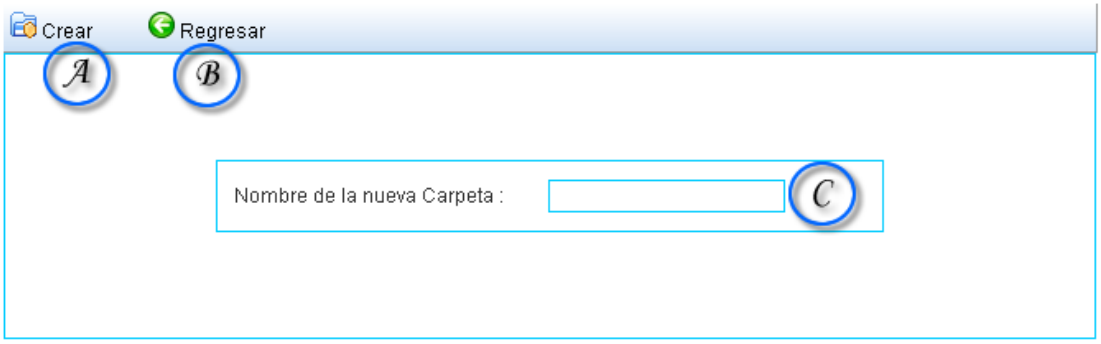


Figura 68. Crear carpeta de Correo electrónico.

6.1.2.5 Renombrar Carpeta de Correo

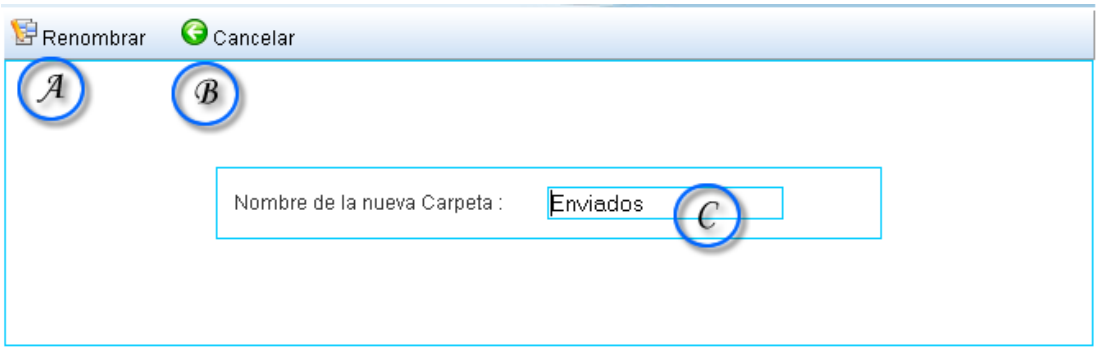


Figura 69. Modificación de nombre de carpeta de correo.

Caso de Uso: Administrar correo electrónico (Usuario) sección administración de carpetas de correo.

Actores: Administrador del sistema ó usuario de correo
Propósito: Administrar carpetas de correo electrónico.
Resumen: Brinda al usuario la posibilidad de administrar y ordenar sus mensajes en subdirectorios del buzón de correo.

Curso Normal de los Eventos

1. Esta sección del caso de uso comienza cuando el actor desea administrar sus carpetas de correo.
2. El actor presiona sobre C en la Figura 64.
3. El sistema genera un informe detallado sobre la información de las carpetas que posee el actor como en la Figura 69.
4. Tanto en D como en E y en F, el sistema brinda la información de número de la carpeta, el nombre de la carpeta, los mensajes nuevos, los mensajes recientes, y el total de mensajes respectivamente.
5. Si el usuario desea crear una carpeta adicional oprime sobre A.
6. El sistema muestra entonces la interfaz de la figura 68.
7. El sistema solicita el nombre de la nueva carpeta a ingresar en C, así como también la posibilidad de crear la nueva carpeta oprimiendo A o la opción de regresar para no efectuar ningún cambio oprimiendo en B.
8. El usuario puede renombrar una carpeta, oprimiendo C en la figura 69, una vez la haya seleccionado en la respectiva lista a través de las cajas de texto.
9. El sistema mostrará la interfaz de la figura 69.
10. El sistema solicita el nuevo nombre de la carpeta a renombrar en C, así como también la posibilidad de renombrar la carpeta oprimiendo A, y regresar sin efectuar cambios, oprimiendo en B.
11. El usuario puede borrar carpetas oprimiendo en B en a figura 67.

Línea 8, línea 10: Si el usuario no selecciona ninguna carpeta a través de las cajas de texto, el sistema no podrá continuar el proceso y mostrara una alerta informativa al respecto.

6.1.2.6 Correo Electrónico (Administración de Contactos)

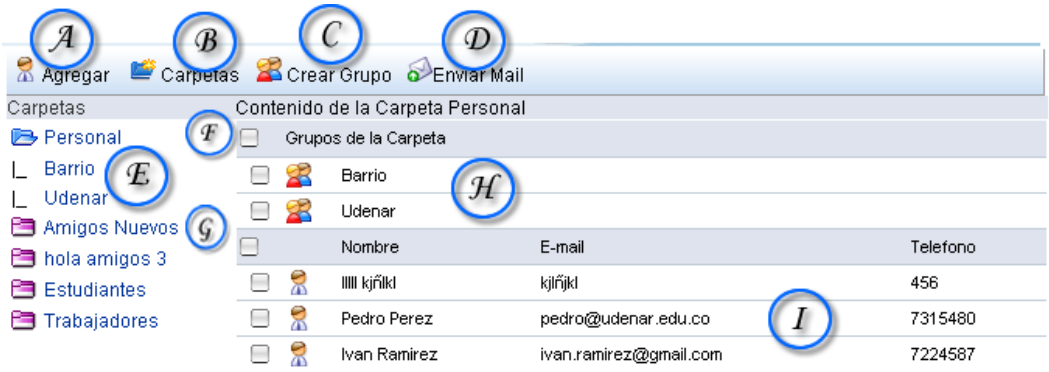


Figura 70. Administración de Contactos de Correo

Caso de Uso: Administrar Listas y grupos de correo (Contactos).

Actores: Administrador del sistema ó usuario de correo
Propósito: Administrar contactos de correo electrónico y organizarlos por carpetas o grupos.
Resumen: Brinda al usuario la posibilidad de administrar y ordenar sus contactos a través de subdirectorios, o grupos.

Curso Normal de los Eventos

1. Este caso de uso comienza cuando el actor ingresa a la sección contactos, inmediatamente después de haber iniciado sesión.
2. El actor adquiere una visión global de la jerarquía de sus carpetas de contactos, como aparece en E de la figura 70, así como también de los grupos creados y de los contactos registrados así como aparece en H y en I de la figura 70.
3. Para enviar a un mail a uno o mas contactos, o a uno o más grupos de contactos, se pueden seleccionar a través de cajas de texto así como lo señala F y G de la figura 70.
4. El sistema muestra también una breve descripción del contenido de los grupos y de los contactos registrados tal y como lo muestra H e I de la figura 10.

Línea 3: Si el usuario no selecciona ningún usuario ó grupo a través de las cajas de texto, el sistema no podrá continuar el proceso y mostrara una alerta informativa al respecto.

6.1.2.7 Correo Electrónico (Agregar Contacto)

Figura 71. Agregar contacto

Caso de Uso: Administrar Listas y grupos de correo (Contactos) sección agregar contacto.
Actores: Administrador del sistema ó usuario de correo
Propósito: Registrar nuevos contactos de correo electrónico para un mejor y más fácil acceso a los usuarios.
Resumen: Brinda al usuario la posibilidad de guardar en el sistema la información de los contactos que sean convenientes.

Curso Normal de los Eventos

1. Este caso de uso comienza cuando el actor selecciona A de la figura 70
2. El sistema solicita los datos necesarios para crear o almacenar el nuevo contacto, tales como nombre, apellido, teléfono, otro correo electrónico, tal y como lo muestra, la figura 71en E, F, G, H.
3. El nuevo contacto puede formar parte de una carpeta e incluso de un grupo, tal y como lo muestra C y D de la figura 71.
4. Para crear un contacto después de llenar la información pertinente, se presiona A.
5. Para cancelar el proceso simplemente Presionamos en B

Línea 3: Si el usuario no selecciona ninguna carpeta o grupo para el nuevo contacto, este se registrará en la carpeta y grupo por defecto.

6.1.2.8 Correo Electrónico (Crear Carpetas de Contactos)

Figura 72. Crear carpeta de contactos

Caso de Uso: Administrar Listas y grupos de correo (Contactos) sección crear carpetas de contactos.
Actores: Administrador del sistema ó usuario de correo
Propósito: Crea carpetas para ordenar contactos.
Resumen: Brinda al usuario la posibilidad de organizar a su gusto, los contactos creados a través de carpetas.

Curso Normal de los Eventos

1. Este caso de uso comienza cuando el actor selecciona B de la figura 10
2. El sistema muestra inmediatamente un listado de las carpetas creadas hasta el momento, si el usuario ingresa por primera vez solo encontrará la carpeta por defecto.
3. El sistema además muestra las carpetas con un breve resumen de los contactos o grupos que contiene cada una así como aparece en E de la figura 72.
4. El sistema brinda la posibilidad de crear nuevas carpeta, eliminar carpetas existentes, así como modificarlas, oprimiendo en A, B, C de la figura 72 respectivamente.

Línea 4: Si el usuario no selecciona ninguna carpeta a través de las cajas de texto, el sistema no podrá continuar el proceso de eliminación ó modificación de estas y mostrara una alerta informativa al respecto.

6.1.2.9 Correo Electrónico (Modificar carpeta contactos)

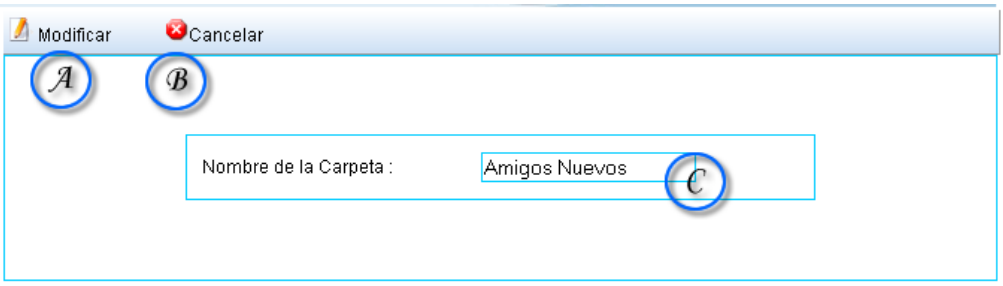


Figura 73. Modificar Carpeta Contactos

Caso de Uso: Administrar Listas y grupos de correo (Contactos) sección modificar carpetas de contactos.
Actores: Administrador del sistema ó usuario de correo
Propósito: Modificar Carpetas de contactos.
Resumen: Brinda al usuario la posibilidad de organizar a su gusto, los contactos creados a través de carpetas.

Curso Normal de los Eventos

5. Este caso de uso comienza cuando el actor selecciona C de la figura 72, una vez haya seleccionado una carpeta existente a través de las cajas de texto de esta misma.

6. El sistema presenta el nombre de la carpeta a modificar como en C de la figura 73, así como también la posibilidad de confirmar la modificación del nombre de la carpeta como de cancelar en proceso a través de A y B de la figura 73 respectivamente.

6.1.2.10 Correo electrónico (Crear grupo de contactos)

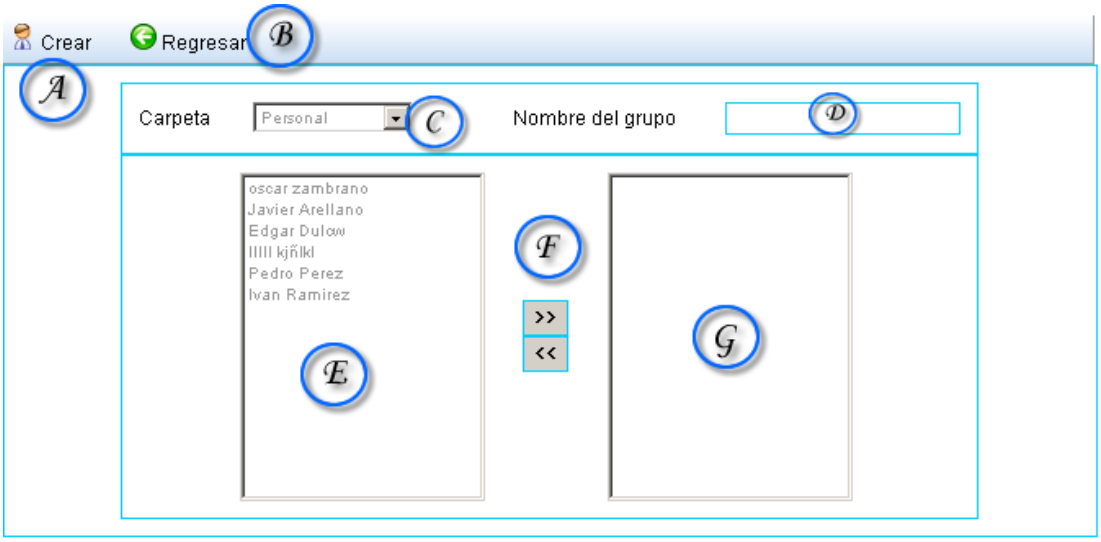


Figura 74. Crear figura contactos.

Caso de Uso: Administrar Listas y grupos de correo (Contactos) sección crear grupos de contactos
Actores: Administrador del sistema ó usuario de correo
Propósito: Crea grupos para ordenar contactos.
Resumen: Brinda al usuario la posibilidad de organizar a su gusto, los contactos creados a través de grupos específicos.

Curso Normal de los Eventos

1. Este caso de uso comienza cuando el actor selecciona C de la figura 70
2. El sistema muestra las carpetas creadas a través de una lista desplegable como lo muestra C de la figura 74, así como también los contactos inscritos a determinada carpeta tal y como lo muestra E de la misma figura.
3. El sistema permita seleccionar uno o más contactos de cualquier carpeta y vincularlos a través de un grupo, cuyo nombre en registrado en D de la figura 74, y

formado por los contactos listados en G a través de los botones de selección de F de la misma figura.

4. El usuario puede agregar a un grupo, contactos de una o más carpetas seleccionadas, y confirmar su decisión oprimiendo en A.
5. En cualquier momento, el usuario puede cancelar su operación oprimiendo en B de la figura 74.

Línea 4: Si el usuario no brinda un nombre al grupo, el sistema no podrá continuar el proceso y mostrara una alerta informativa al respecto.

6.1.3 Administrador de publicaciones web

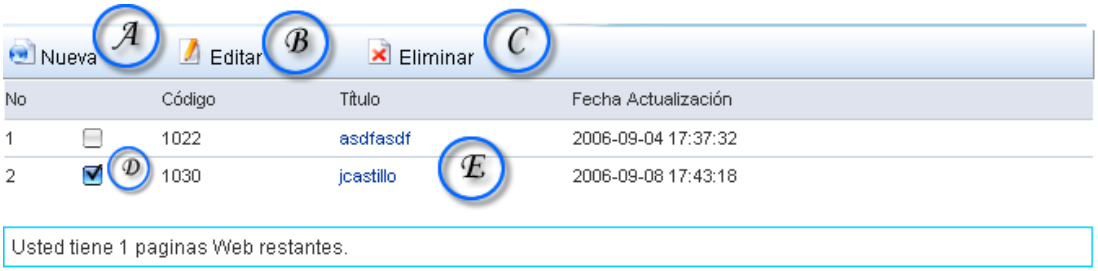


Figura 75 Administrador de Publicaciones Web

Caso de Uso: Administrar Publicaciones Web
Actores: Administrador del sistema y Usuario
Propósito: Administra las diferentes publicaciones que un usuario puede realizar, una vez figure como usuario de correo electrónico.
Resumen: Brinda al usuario la posibilidad de crear el mismo a través de un asistente en línea, sus propias páginas y publicaciones Web.

Curso Normal de los Eventos

1. Este caso de uso comienza cuando el actor selecciona Publicaciones, una vez haya ingresado al sistema después de la figura 63.
2. El sistema muestra el listado de las publicaciones Web creadas hasta el momento como E de la figura 75, respaldado por la oportunidad de modificar su contenido ó eliminar una publicación, seleccionando B ó C de la figura 75 respectivamente.
3. E muestra también el código de publicación generado por el sistema así como también el nombre de la publicación, y la fecha de publicación o ultima modificación.
4. Para cualquier modificación o eliminación de publicaciones, el usuario selecciona con anterioridad D de la figura 75 para continuar estos procesos.

5. Si el usuario no tiene publicaciones hechas, puede crear una nueva presionando A de la figura 75.
6. El sistema muestra al final de la interfaz de la figura 75, un contador de publicaciones restantes brindadas por el administrador del sistema.

Línea 2: Si el usuario no selecciona un registro a través de las cajas de texto con D de la figura 75, el sistema mostrará una alerta informativa al respecto.

6.1.3.1 Publicaciones Web (Editor de publicaciones Web)

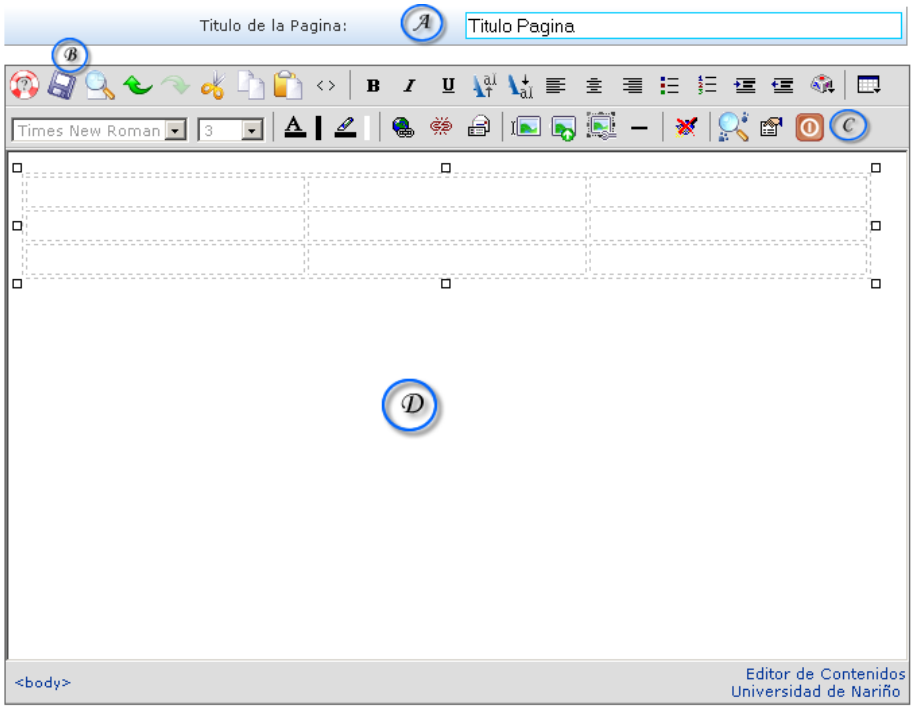


Figura 76. Editor de publicaciones Web.

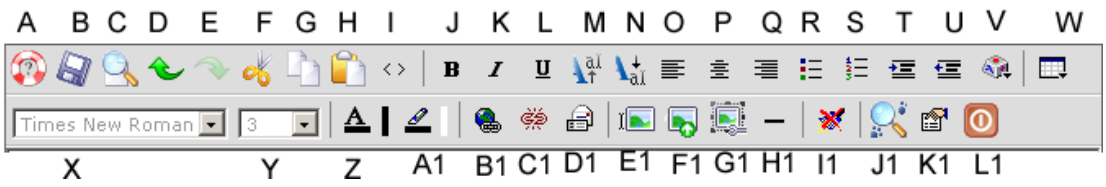


Figura 77. Barra de Control Editor de Publicaciones

Caso de Uso: Administrar Publicaciones Web (Crear Nueva Pagina Web)
Actores: Administrador del sistema y Usuario
Propósito: Crear las diferentes publicaciones que un usuario puede realizar, una vez figure como usuario de correo electrónico.
Resumen: Brinda al usuario la posibilidad de crear una publicación Web a través de un asistente en línea.

Curso Normal de los Eventos

1. Este caso de uso comienza cuando el actor selecciona Nueva Publicación en A de la figura 75.
2. El sistema muestra una completa barra de herramientas como lo muestra B en la figura 76, que facilitaran el trabajo al usuario común, sin necesidad de que este necesite conocer HTML.
3. El usuario puede dar un nombre al su página asignándoselo en A de la figura 76.
4. El usuario tiene acceso a un espacio de trabajo como lo muestra D de la figura 76. Todo lo que se realice a través de la barra de herramientas, se vera representado en el espacio de trabajo, es una aplicación de tipo (WYSIWYG "Lo que mira es lo que obtiene").
5. La barra de herramientas incluye herramientas como:

    - A: Ayuda.
    - B: Guardar.
    - C: Vista Previa.
    - D: Cancelar acción.
    - E: Reanudar acción.
    - F: Cortar.
    - G: Copiar.
    - H: Pegar.
    - I: Cambiar modo de edición.
    - J: Texto en negrilla.
    - K: Texto en cursiva.
    - L: Texto subrayado.
    - M: Superíndice.
    - N: Subíndice
    - O: Alineación izquierda
    - P: Alineación central
    - Q: Alineación derecha.
    - R: Viñetas
    - S: Numeración

- T: Sangría a la derecha.
- U: Sangría a la izquierda.
- V: Caracteres especiales.
- W: Creación de tablas.
- X: Fuente del texto.
- Y: Tamaño del texto.
- Z: Color del texto.
- B1: Agregar enlace.
- C1: Quitar enlace.
- D1: Agregar enlace de correo.
- E1: Insertar Imagen.
- F1: Subir Imagen.
- G1: Propiedades de la imagen
- H1: Insertar línea horizontal.
- I1: Borrar HTML.
- J1: Buscar y reemplazar.
- K1: Propiedades de la página.
- L1: Salir

6. El usuario una vez haya guardado su trabajo o publicación a través de la barra de herramientas, podrá salir de este ámbito presionando C de la figura 76.

Línea 6: Si el usuario no le da un nombre a la publicación, esta no podrá ser guardada, el sistema mostrará una alerta informativa al respecto.

6.1.3.2 Publicaciones Web (Insertar Tabla)

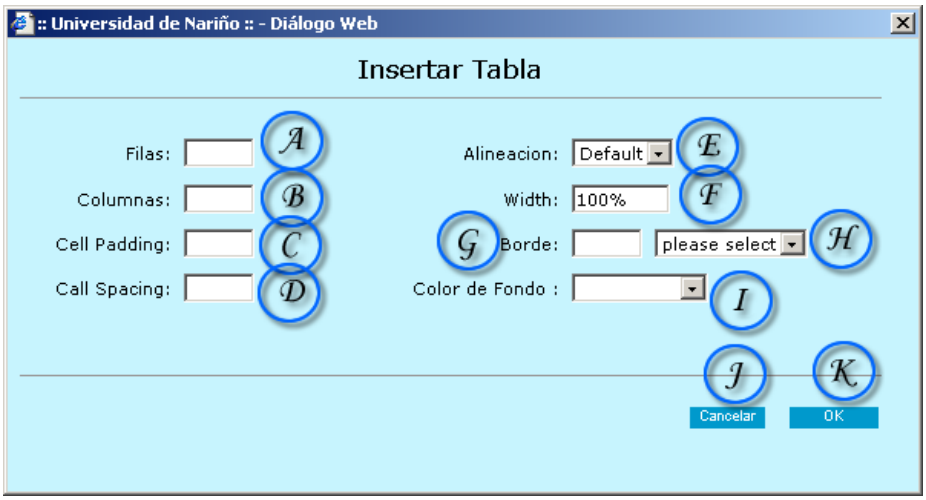


Figura 78. Insertar Tabla

Caso de Uso: Administrar Publicaciones Web (Insertar Tablas HTML)
Actores: Administrador del sistema y Usuario
Propósito: Crear fácilmente tablas en HTML.
Resumen: Brinda al usuario la posibilidad de crear tablas en HTML sin necesidad de conocer ningún tipo de lenguaje.

Curso Normal de los Eventos

1. Esta sección de caso de uso comienza cuando el actor presiona sobre W de la figura 77.
2. El sistema muestra un interfaz amigable e intuitiva que ayudara a crear fácilmente tablas HTML para su publicación Web, de llegar a necesitarlas.
3. El usuario especifica en el formulario de la figura 78 las propiedades que desea obtener en la tabla.
4. Las posibles propiedades a modificar en la figura 78 son:

    - A: Número de filas de la tabla.
    - B: Número de Columnas de la tabla.
    - C: Espacio entre contenido de celdas.
    - D: Espacio entre celdas.
    - E: Alineación de la tabla.
    - F: Ancho de la tabla.
    - G: Borde de la tabla.
    - H: Tipo de borde de la tabla.
    - I: Color de fondo de la tabla.

5. Para cancelar cualquier modificación a los parámetros de la tabla, se presiona J de la figura 78.

6. Para aceptar y aplicar los parámetros asignados por el usuario, presiona K de la figura 78.

6.1.3.3 Publicaciones Web (Propiedades de la tabla)

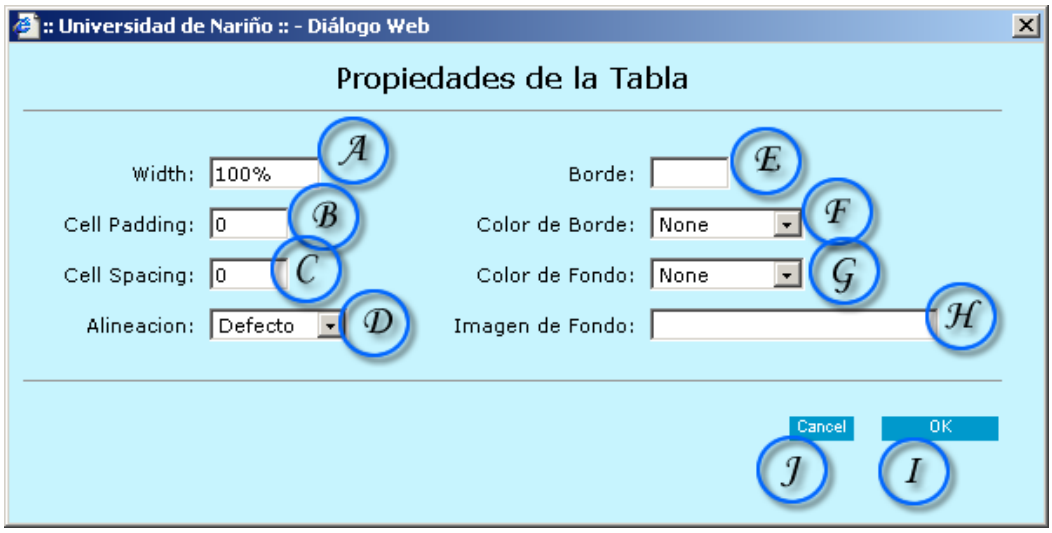


Figura 79. Propiedades de Tabla

Caso de Uso: Administrar Publicaciones Web (Modificar tabla HTML)
Actores: Administrador del sistema y Usuario
Propósito: Modificar fácilmente la propiedades de tablas en HTML.
Resumen: Brinda al usuario la posibilidad de modificar tablas en HTML sin necesidad de conocer ningún tipo de lenguaje.

Curso Normal de los Eventos

1. Esta sección de caso de uso comienza cuando el actor mantiene presionado W de la figura 77 y selecciona la herramienta de modificación.

2. El sistema muestra una interfaz amigable e intuitiva que ayudara a modificar fácilmente tablas HTML dentro del espacio de trabajo asignado.

3. El usuario especifica en el formulario de la figura 79 las propiedades que desea obtener en la tabla.

4. Las posibles propiedades a modificar en la figura 79 son:

    - A: Ancho de la Tabla.
    - B: Espacio entre contenido de celdas.

- C: Espacio entre celdas.
- D: Alineación de la tabla.
- E Borde de la tabla.
- F: Color de borde.
- G: Color de fondo.
- H: Ubicación de imagen de fondo.

5. Para cancelar cualquier modificación a las propiedades de la tabla, se presiona J de la figura 79.

6. Para aceptar y aplicar las propiedades de la tabla asignados por el usuario, presiona I de la figura 79.

6.1.3.4 Publicaciones Web (Propiedades de Celda)

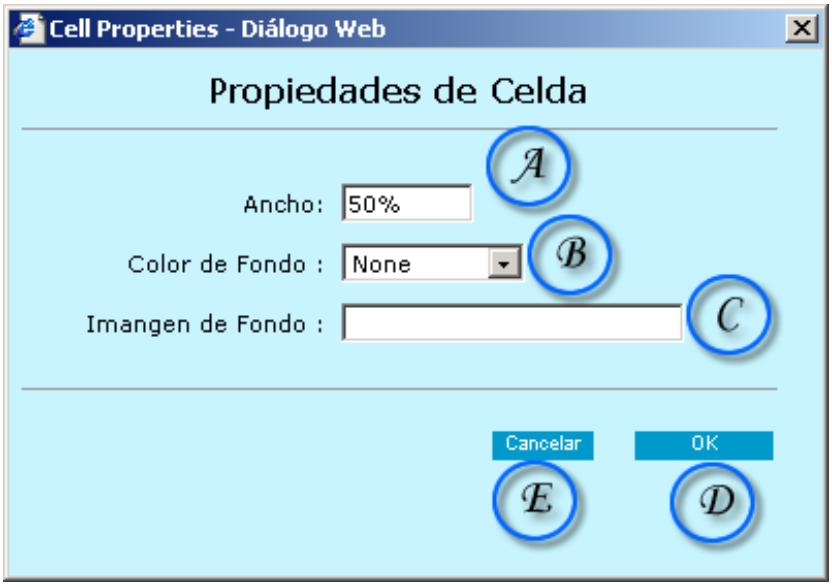


Figura 80. Propiedades de Celda.

Caso de Uso: Administrar Publicaciones Web (Propiedades de celdas HTML)
Actores: Administrador del sistema y Usuario
Propósito: Modificar fácilmente la propiedades de Celdas en HTML.
Resumen: Brinda al usuario la posibilidad de modificar celdas de tablas en HTML sin necesidad de conocer ningún tipo de lenguaje.

Curso Normal de los Eventos

1. Esta sección de caso de uso comienza cuando el actor mantiene presionado W de la figura 77 y selecciona la herramienta de propiedades de Celda.

2. El sistema muestra una interfaz amigable e intuitiva que ayudara a modificar fácilmente las celdas de las tablas HTML dentro del espacio de trabajo asignado.

3. El usuario especifica en el formulario de la figura 80 las propiedades que desea obtener en la celda seleccionada.

4. Las posibles propiedades a modificar en la figura 80 son:

   - A: Ancho de la celda.
   - B: Color de fondo de la celda.
   - C: Imagen de fondo de la celda.

5. Para cancelar cualquier modificación a las propiedades de la celda, se presiona E de la figura 80.

6. Para aceptar y aplicar las propiedades de la celda asignados por el usuario, presiona D de la figura 80.

6.1.3.5 Publicaciones Web (Agregar enlace Web)

Figura 81. Agregar Enlace

Caso de Uso: Administrar Publicaciones Web (Agregar enlace o hipervínculo)
Actores: Administrador del sistema y Usuario
Propósito: Implementar fácilmente vínculos HTML.
Resumen: Brinda al usuario la posibilidad de ingresar vínculos en HTML sin necesidad de conocer ningún tipo de lenguaje.

Curso Normal de los Eventos

1. Esta sección de caso de uso comienza cuando el actor presiona B1 de la figura 77.

2. El sistema muestra una interfaz amigable e intuitiva que ayudara al usuario a crear hipervínculos HTML dentro del espacio de trabajo asignado en D de la figura 76.

3. El usuario especifica en el formulario de la figura 81 los parámetros necesarios para crear un hipervínculo.

4. Las posibles propiedades a modificar en la figura 81 son:

    - URL: Universal Resource Locator.
    - Titulo: Titulo del hipervínculo.
    - Target: Nombre del Frame o cuadro por defecto en donde se abrirá el vínculo.
    - Color de Link: Color del Enlace.
    - Estilo de Link: Estilo del Enlace.

5. Para cancelar cualquier modificación a las propiedades de la tabla, el usuario presiona CANCELAR de la figura 81.

6. Para quitar un vínculo antes realizado, el usuario presiona QUITAR VINCULO de la figura 81.

7. Para aceptar y aplicar las propiedades del hipervínculo creado por el usuario, presiona OK de la figura 81.

Línea 6: El usuario también puede quitar un Hipervínculo, presionando C1 de la figura 77.

6.1.3.6 Publicaciones Web (Agregar enlace Web)

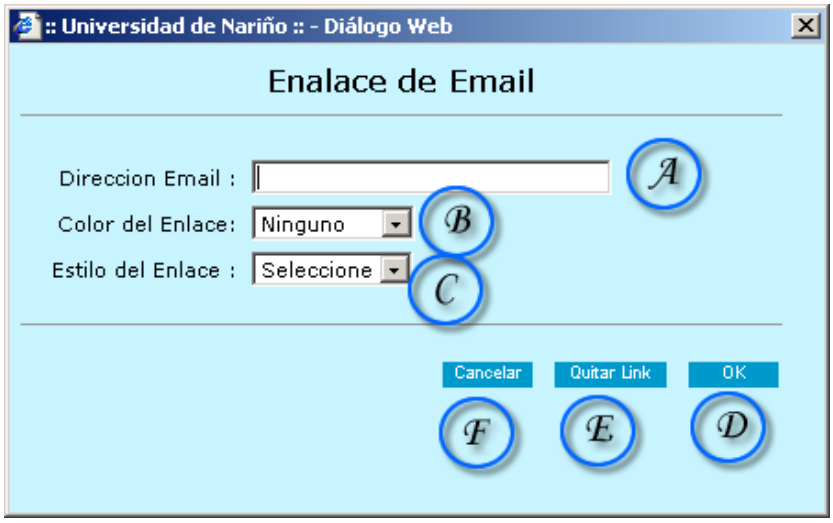


Figura 82. Agregar Enlace a email

Caso de Uso: Administrar Publicaciones Web (Agregar enlace de email)
Actores: Administrador del sistema y Usuario
Propósito: Implementar fácilmente enlaces email en HTML.
Resumen: Brinda al usuario la posibilidad de crear enlaces email en HTML sin necesidad de conocer ningún tipo de lenguaje.

Curso Normal de los Eventos

1. Esta sección de caso de uso comienza cuando el actor presiona D1 de la figura 77.
2. El sistema muestra una interfaz amigable e intuitiva que ayudara al usuario a crear enlaces email en HTML dentro del espacio de trabajo asignado en D de la figura 76.
3. El usuario especifica en el formulario de la figura 82 los parámetros necesarios para crear un enlace email.

4. Las posibles propiedades a modificar en la figura 82 son:

   - A: Dirección de correo electrónico
   - B: Color del enlace email.
   - C: Estilo del enlace email.
   - D: Confirmar creación de enlace email.

- E: Quitar enlace email.
- F: Cancelar Operación

5. Para cancelar la creación del enlace de email, el usuario presiona F de la figura 82.
6. Para quitar un enlace email antes realizado, el usuario presiona E en la figura 82.
7. Para aceptar y aplicar las propiedades enlace mail creado por el usuario, presiona D de la figura 82.

6.1.3.7 Publicaciones Web (Insertar imagen)

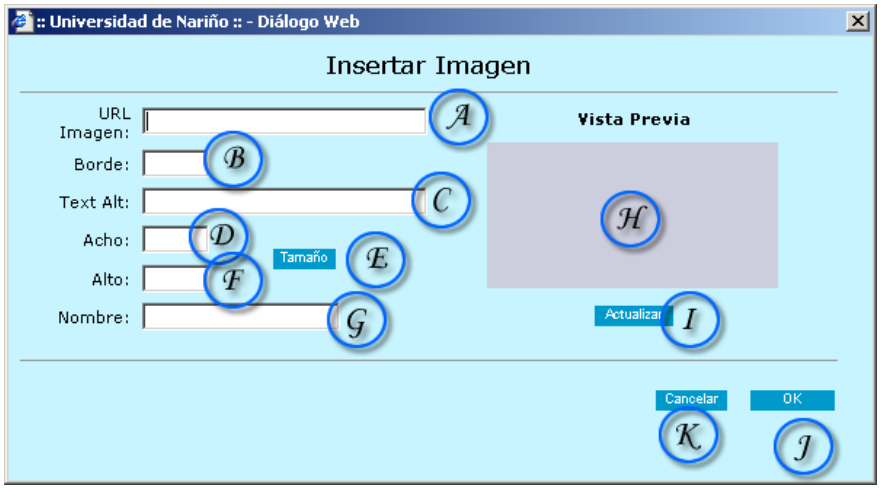


Figura 83. Insertar Imagen

Caso de Uso: Administrar Publicaciones Web (Insertar Imagen)
Actores: Administrador del sistema y Usuario
Propósito: Insertar Imágenes en el documento HTML.
Resumen: Brinda al usuario la posibilidad de ingresar imágenes en el documento HTML.

Curso Normal de los Eventos

1. Esta sección de caso de uso comienza cuando el actor presiona E1 de la figura 77.
2. El sistema muestra una interfaz que ayudará al usuario a implementar imágenes dentro del espacio de trabajo asignado en D de la figura 76.
3. El usuario especifica en el formulario de la figura 83 los parámetros necesarios para introducir una imagen al documento HTML.

4. Las posibles propiedades a modificar en la figura 83 son:
    - A: URL, o dirección electrónica de la imagen.
    - B: Borde de la imagen.
    - C: Texto informativo de la imagen.
    - D: Ancho de la imagen.
    - E: Alto de la imagen.
    - F: Adquirir tamaño de la imagen.
    - G: Nombre de la imagen.
    - H: Vista previa de la imagen.
    - I: Actualizar vista previa de la imagen.

5. Para cancelar cualquier inserción de imágenes al documento HTML, el usuario presiona K de la figura 83.

6. Para aceptar y aplicar la inserción de la imagen al documento HTML, el usuario presiona J de la figura 83.

Línea 4: Presionando en E, se obtiene automáticamente el ancho y alto de la imagen.

6.1.3.8 Publicaciones Web (Insertar línea horizontal)

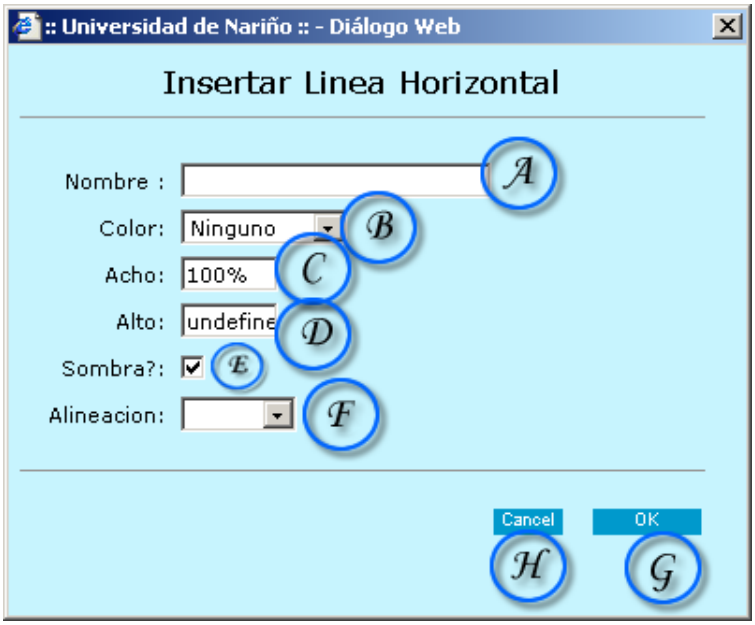


Figura 84. Insertar División HR

Caso de Uso: Administrar Publicaciones Web (Insertar línea horizontal)
Actores: Administrador del sistema y Usuario
Propósito: Insertar líneas horizontales en el documento HTML.
Resumen: Brinda al usuario la posibilidad de líneas horizontales en el documento HTML.

Curso Normal de los Eventos

1. Esta sección de caso de uso comienza cuando el actor presiona H1 de la figura 77.
2. El sistema muestra una interfaz que ayudará al usuario a implementar líneas horizontales confines de ordenamiento de información, en el espacio de trabajo asignado en D de la figura 76.
3. El usuario especifica en el formulario de la figura 84 los parámetros necesarios para la creación del la línea horizontal.

4. Las posibles propiedades a modificar en la figura 84 son:

    - A: Nombre o texto que ira sobre la línea horizontal
    - B: Color de la línea horizontal.
    - C: Ancho de la línea horizontal.
    - D: Alto de la línea horizontal.
    - E: Activar Sobra en la línea horizontal
    - F: Alineación de la línea horizontal

5. Para cancelar cualquier inserción de líneas horizontales en el documento HTML, el usuario presiona H de la figura 84.

6. Para aceptar y aplicar la inserción de la línea horizontal en el documento HTML, el usuario presiona G de la figura 84.

6.1.3.9 Publicaciones Web (Insertar texto scroll).

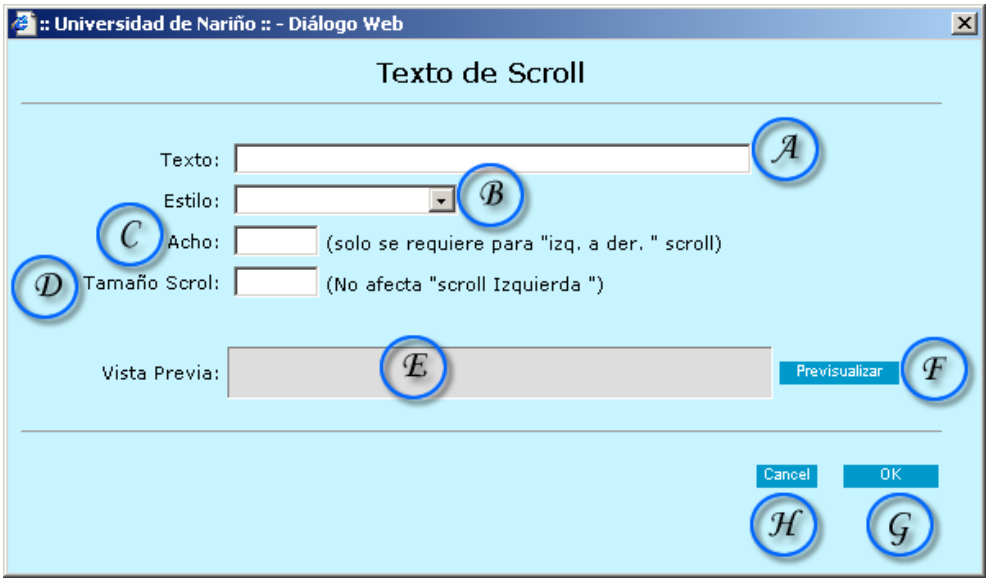


Figura 85. Insertar Texto Scroll

Caso de Uso: Administrar Publicaciones Web (Insertar Texto Scroll)
Actores: Administrador del sistema y Usuario
Propósito: Insertar Texto scroll en el documento HTML.
Resumen: Brinda al usuario la posibilidad de ingresar texto scroll en el documento HTML.

Curso Normal de los Eventos

1. Esta sección de caso de uso comienza cuando el actor presiona V de la figura 77 y selecciona texto scroll.
2. El sistema muestra una interfaz que ayudará al usuario a implementar texto de tipo Scroll dentro del espacio de trabajo asignado en D de la figura 76.
3. El usuario especifica en el formulario de la figura 85 los parámetros necesarios para introducir texto scroll al documento HTML.

4. Las posibles propiedades a modificar en la figura 83, son:

   - A: Texto a introducir.
   - B: Estilo del texto.
   - C: Ancho del scroll.

- D: Tamaño de scroll.
- E: Vista previa del texto scroll.
- F: Pre visualizar texto scroll.

5. Para cancelar cualquier inserción de texto scroll al documento HTML, el usuario presiona H de la figura 85.

6. Para aceptar y aplicar la inserción de texto scroll al documento HTML, el usuario presiona G de la figura 85.

Línea 4: Presionando en F de la figura 85, se obtiene automáticamente la pre visualización en E.

6.1.3.10 Publicaciones Web (Buscar y reemplazar)

Figura 86. Buscar y Reemplazar.

Caso de Uso: Administrar Publicaciones Web (Buscar y reemplazar texto)
Actores: Administrador del sistema y Usuario
Propósito: Busca y/o reemplaza texto en el documento HTML.
Resumen: Brinda al usuario la posibilidad de buscar y reemplazar texto en el documento HTML.

Curso Normal de los Eventos

1. Esta sección de caso de uso comienza cuando el actor presiona J1 de la figura 77.
2. El sistema muestra una interfaz que ayudará al usuario a buscar y/o reemplazar texto dentro del documento HTML.

3. El usuario especifica en el formulario de la figura 86 los parámetros necesarios para buscar y/o reemplazar texto en el documento HTML.

4. Las posibles propiedades del formulario de la figura 86 son:

   - A: Texto a buscar.
   - B: Texto a reemplazar por el texto buscado.
   - C: reemplazar o buscar coincidiendo completamente el texto ingresado por el usuario.
   - D: Distinguir entre mayúsculas y minúsculas.
   - E: Reemplaza todo el texto en A por el texto en B.

5. Para cancelar la búsqueda o reemplazo de texto en el documento o publicación Web, el usuario presiona F de la figura 86.

6.1.3.11 Publicaciones Web (Propiedades de la página)

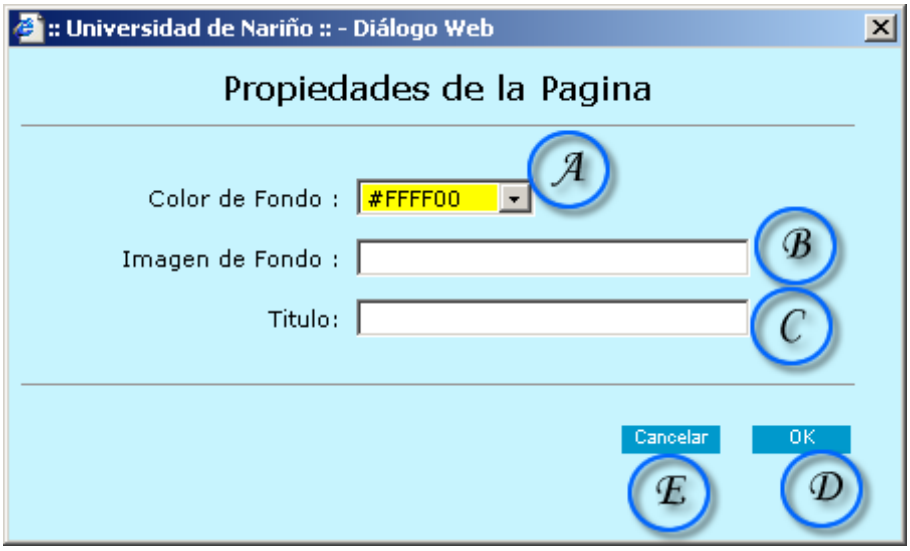


Figura 87. Propiedades de la Publicación

Caso de Uso: Administrar Publicaciones Web (Propiedades de la publicación Web)
Actores: Administrador del sistema y Usuario
Propósito: Aplicar propiedades generales del documento HTML.

Resumen: Brinda al usuario la posibilidad de configurar las propiedades generales del documento HTML.

Curso Normal de los Eventos

1. Esta sección de caso de uso comienza cuando el actor presiona K1 de la figura 77.
2. El sistema muestra una interfaz que ayudará al usuario a configurar propiedades de la página HTML.
3. El usuario especifica en el formulario de la figura 87 los parámetros necesarios para la configuración de la publicación Web.

4. Las posibles propiedades del formulario de la figura 86 son:
   - A: Color de fondo del documento HTML.
   - B: Imagen de fondo del documento HTML.
   - C: Titulo del documento o publicación Web.

5. Para cancelar la configuración de la publicación Web, el usuario presiona E de la figura 87.
6. Para aplicar los cambios el usuario presiona D de la figura 87.

6.1.4 Actualizar información personal

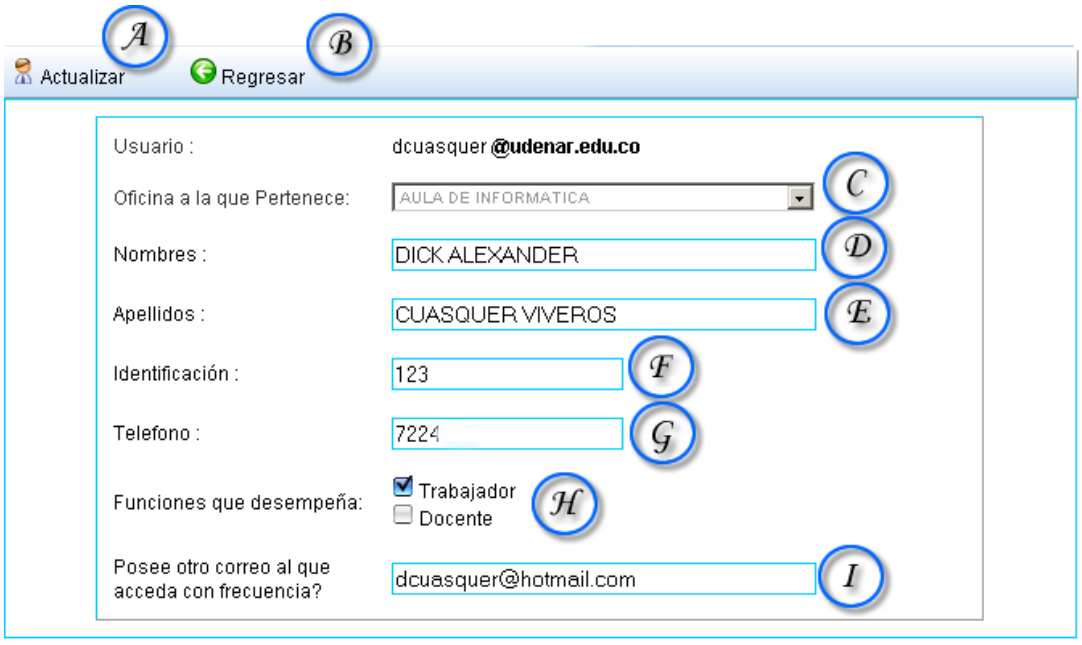


Figura 88. Actualizar Información Personal

Caso de Uso: Para todos los servicios (Actualización de datos personales).
Actores: Usuario
Propósito: Actualiza datos personales para cualquier tipo de servicio.
Resumen: Brinda al usuario la posibilidad de actualizar sus datos personales en cualquier momento sin necesidad del administrador del sistema.

Curso Normal de los Eventos

1. Esta sección de caso de uso comienza cuando el actor entra a la sección de información personal de la página principal del sistema.
2. El sistema muestra una interfaz que ayudará al usuario a actualizar sus datos personales.
3. El usuario muestra en el formulario de la figura 88 la ultima información personal registrada y brinda la posibilidad de cambiarla.
4. Para cambiar la oficina a la que pertenece presiona C de la figura 88.
5. Para cambiar sus nombres o apellidos el usuario edita D y E de la figura 88 respectivamente.
6. Para cambiar su identificación o teléfono, el usuario edita F y G de la figura 88 respectivamente.
7. Para cambiar la función que desempeña el usuario, el usuario selecciona en H de la figura 88, una de las opciones.
8. Para cambiar la referencia de alguna otra dirección electrónica, el usuario presiona I de la figura 88.
9. Para confirmar los cambios realizados, el usuario presiona A o bien B de la figura 88 para cancelar cualquier novedad.

6.1.5 Cambiar contraseña de acceso

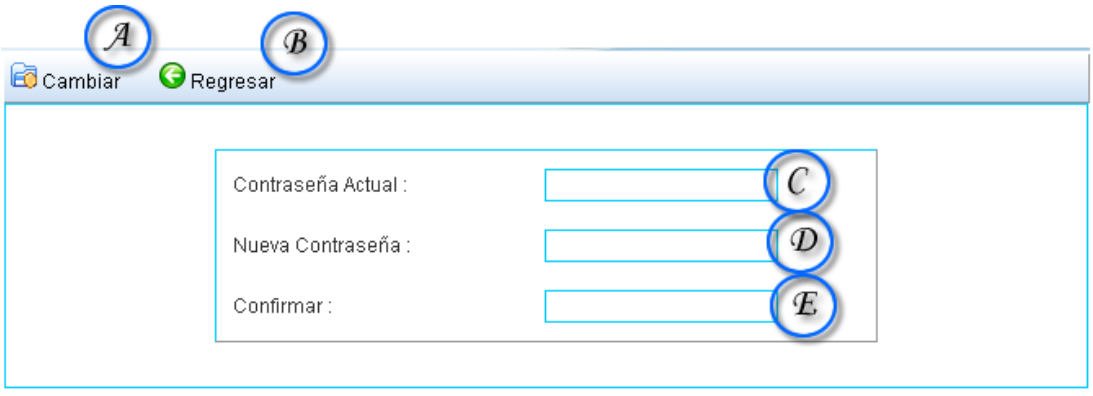


Figura 89. Cambiar Contraseña de Acceso

Caso de Uso: Para todos los servicios (Cambio de contraseña).
Actores: Usuario
Propósito: Cambiar la contraseña de acceso al sistema.
Resumen: Brinda al usuario la posibilidad de cambiar su contraseña de acceso, lo cual le brindará mayor seguridad en el inicio de su sesión de todos los servicios que este reciba.

Curso Normal de los Eventos

1. Esta sección de caso de uso comienza cuando el actor entra a la sección "información personal" y luego a la sección "cambio de contraseña" de la página principal del sistema.
2. El sistema muestra una interfaz que ayudará al usuario a cambiar fácilmente la contraseña de acceso al sistema.
3. Para cambiar la contraseña de acceso por una nueva, el usuario ingresa su antigua contraseña en C, luego escribe su nueva contraseña en D y la confirma en E de la figura 89 respectivamente.
4. Para aceptar los cambios, el usuario presiona A de la figura 89.
5. Para cancelar cualquier operación, el usuario presiona B de la figura 89.

Línea 3: Si la nueva contraseña y la confirmación de esta no coinciden, el sistema mostrará una alerta informativa al respecto.

6.1.6 Administración usuarios de correo (administrador)

Figura 90. Administración de Usuarios de Correo.

Caso de Uso: Administración de cuentas de correo (Solo Administrador).
Actores: Administrador del sistema
Propósito: Controla las cuentas de correo electrónico de la institución.
Resumen: Brinda al administrador la posibilidad de controlar fácilmente las cuentas de correo de sus usuarios.

Curso Normal de los Eventos

1. Esta sección de caso de uso comienza cuando el actor entra a la sección "Administración" y luego a la sección "Administración de correo" de la página principal del sistema.
2. El sistema muestra una interfaz que ayudará al administrador a controlar fácilmente las cuentas de correo electrónico de todos los usuarios adscritos a sistema.
3. El sistema hace un listado de los usuarios registrados, en donde aparece el nombre del usuario y la oficina al que pertenece, todos organizados por login de usuario así como lo muestra G de la figura 90.
4. Para listas usuarios por orden alfabético se utiliza la barra de acceso H de la figura 90.
5. Para edita un usuario, este debe ser seleccionado a través de F de la figura 90, y luego presionar B de la figura 90 respectivamente.
6. Para eliminar un usuario, este debe ser seleccionado a través de F de la figura 90, y luego presionar C de la figura 90 respectivamente.
7. El administrador puede buscar usuarios ingresando todo o parte de la información disponible, ya sea nombre o login en la caja de texto D, y posteriormente presionar E para iniciar su búsqueda.
8. Para crear un nuevo usuario, el administrador presiona A de la figura 90.

6.1.7 Creación de usuario de correo (administrador)

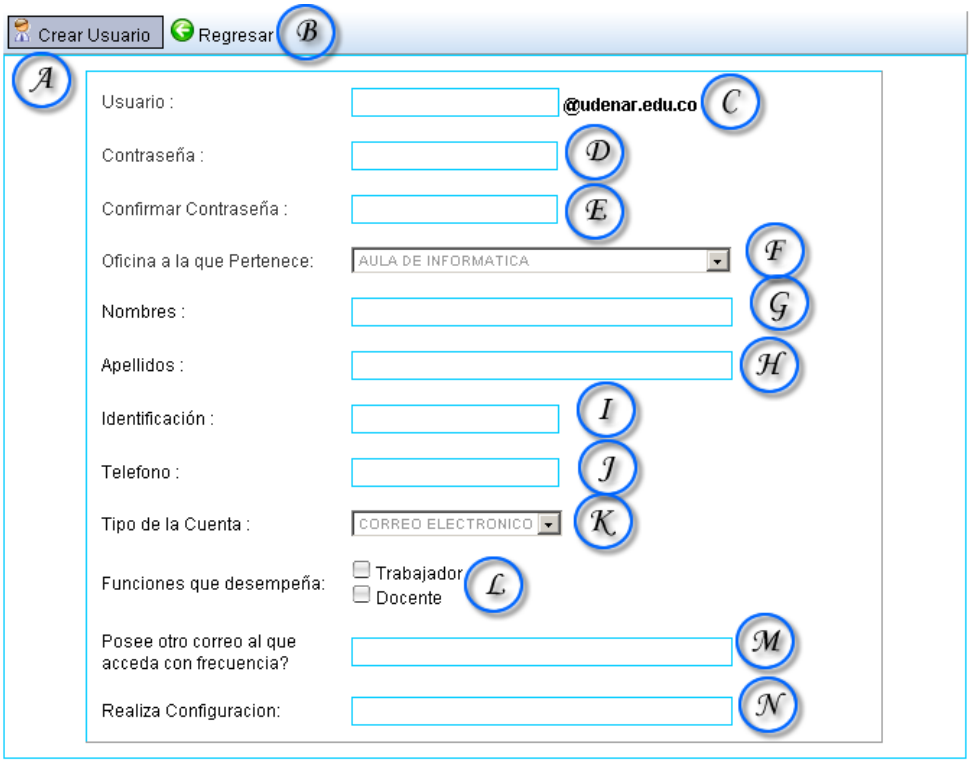


Figura 91. Creación de Usuario de correo.

Caso de Uso: Administración de cuentas de correo (Creación de Usuarios de Correo).
Actores: Administrador del sistema
Propósito: Crea nuevas cuentas de usuario de correo.
Resumen: Brinda al administrador la posibilidad de crear fácilmente nuevas cuentas de usuario de correo electrónico.

Curso Normal de los Eventos

1. Esta sección de caso de uso comienza cuando el actor presiona A de la figura 90.
2. El sistema muestra una interfaz que ayudará al administrador a controlar fácilmente a crear nuevas cuentas de correo electrónico.

3. El sistema muestra el formulario correspondiente a la creación de nuevos usuarios de correo, compuesto por los siguientes campos:

    - C: Dirección electrónica deseada.
    - D: Contraseña de la cuenta.
    - E: Confirmación de contraseña de la cuenta.
    - F: Oficina a la que pertenece el usuario.
    - G: Nombres del nuevo usuario de correo.
    - H: Apellidos del nuevo usuario de correo.
    - I: Identificación (Cedula ó cedula de extranjería).
    - J: Teléfono de contacto del usuario.
    - K: Tipo de cuenta de usuario (Correo electrónico).
    - L: Funciones que desempeña el nuevo usuario si es docente o trabajador.
    - M: Correo alternativo de contacto
    - N: Campo para crear nuevos administradores valores (SI ó NO)

4. Si el administrador desea confirmar la creación del nuevo usuario, presiona A de la figura 91.
5. Para cancelar la creación del nuevo usuario, el usuario presiona B de la figura 91.

Línea 4: El sistema validará la información ingresada por el administrador en caso de haber duplicidad de campos.

6.1.8 Editar información de usuario (administrador)

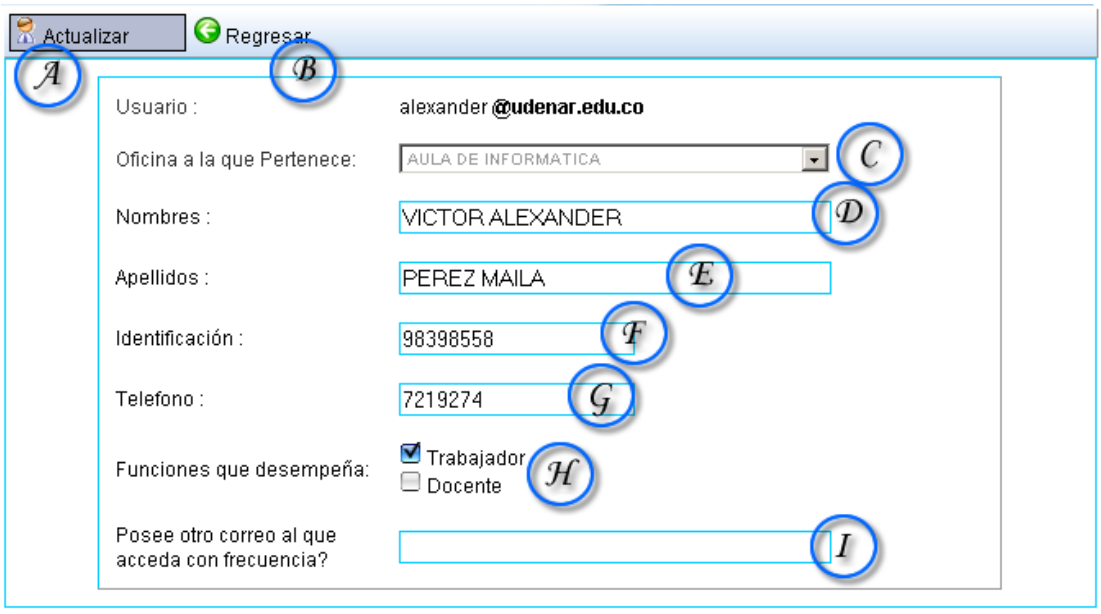


Figura 92. Editar Información de usuario.

Caso de Uso: Administración de cuentas de correo (Edición de Usuarios de Correo).
Actores: Administrador del sistema
Propósito: Modifica cuentas de usuario de correo existentes.
Resumen: Brinda al administrador la posibilidad de modificar información de contacto de cualquier cuenta de usuario de correo electrónico.

Curso Normal de los Eventos

1. Esta sección de caso de uso comienza cuando el actor presiona B de la figura 90, una vez haya utilizado F de la figura 90 para seleccionar el usuario a editar.
2. El sistema muestra una interfaz que ayudará al administrador a actualizar fácilmente la información de contacto del usuario seleccionado de correo electrónico como lo muestra la figura 92.
3. El sistema muestra el formulario correspondiente a la modificación de información de contacto del usuario de correo seleccionado anteriormente, compuesto por los siguientes campos:

    - C: Para cambiar la oficina a la que pertenece.
    - D: Para modificar los nombres del usuario.
    - E: Para modificar los apellidos del usuario.
    - F: Para modificar el número de identificación del usuario.
    - G: Para modificar el número telefónico de contacto.
    - H: Para modificar funciones que desempeña el usuario.
    - I: Para modificar el correo electrónico alternativo de contacto.

4. Si el administrador desea confirmar la modificaron de la cuenta de correo del usuario, presiona A de la figura 92.
5. Para cancelar la modificación de los datos, el administrador presiona B de la figura 92.

Línea 4: El sistema validará la información ingresada por el administrador en caso de haber duplicidad de campos.

6.1.9 Eliminar usuario de correo (administrador)

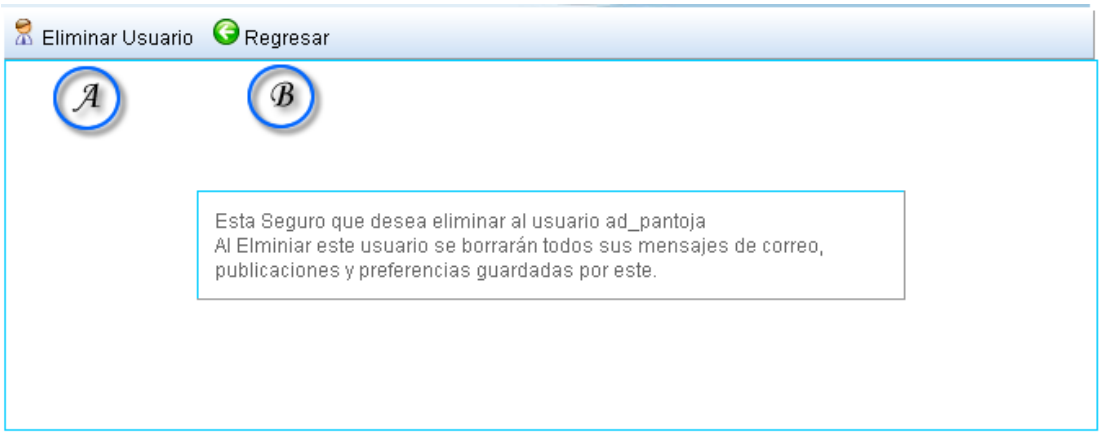


Figura 93. Eliminar Usuario de correo

Caso de Uso: Administración de cuentas de correo (Eliminar Usuarios de Correo).
Actores: Administrador del sistema
Propósito: Elimina cuentas de usuario de correo existentes.
Resumen: Brinda al administrador la posibilidad de eliminar cualquier cuenta de usuario de correo electrónico.

Curso Normal de los Eventos

1. Esta sección de caso de uso comienza cuando el actor presiona C de la figura 90, una vez haya utilizado F de la figura 90 para seleccionar el usuario a editar.
2. El sistema muestra una interfaz que permite al administrador confirmar la eliminación del usuario de correo o cancelar la operación así como lo muestra la figura 93.
3. Para confirmar la eliminación del usuario, el administrador presiona A de la figura 93.
4. Para cancelar la eliminación del usuario, el administrador presiona B de la figura 93.

Línea 3: El sistema eliminará de forma permanente el usuario seleccionado por el administrador.

6.1.10 Administración de nodos

6.1.10.1 Administración de Usuarios de Red

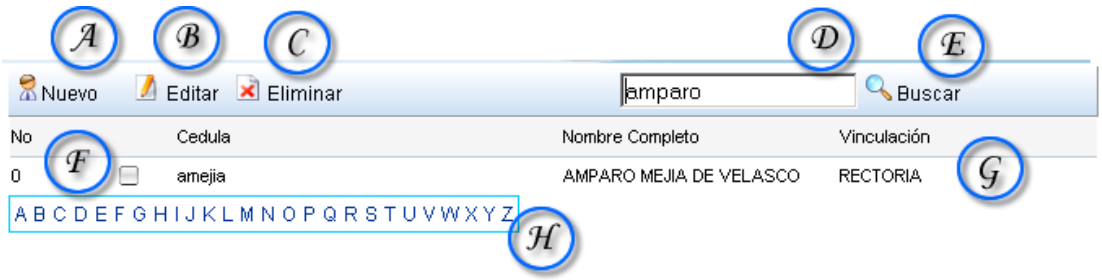


Figura 94. Administración de Usuarios de Red

Caso de Uso: Administración de nodos de Red (Administración de Usuarios de Red).
Actores: Administrador del sistema
Propósito: Administra las cuentas de usuarios de red.
Resumen: Brinda al administrador la posibilidad de manejar fácilmente las cuentas de usuario de red.

Curso Normal de los Eventos

1. Esta sección de caso de uso comienza cuando el actor entra en la sección "Administración" de la página principal, y luego a la sección "Administración de nodos o puntos de red".
2. El sistema muestra una interfaz que ayudará al administrador a manejar de una forma más eficiente los usuarios registrados a la red LAN, así como lo muestra la figura 94.
3. La figura 94 muestra un resumen en listado de los usuarios registrados a la red, así como también el tipo de vinculación a la institución así como lo muestra G de la figura 94.
4. El sistema permite seleccionar un determinado, a través F de la figura 94, para luego editar o eliminar el registro seleccionado a través de B y C de la figura 94 respectivamente.
5. El sistema permite buscar un usuario específico, bien utilizando el listado por orden alfabético a través de H o bien usando D y E para buscar una cadena de texto específica.
6. Para crear un nuevo usuario de red, el administrador presiona A de la figura 94.

Línea 4: Si el usuario no es seleccionado a través de la caja de texto F de la figura 85, no se podrá realizar ninguna modificación o eliminación del mismo. El sistema mostrará un error informativo al respecto.

6.1.10.2 Crear Usuarios de red

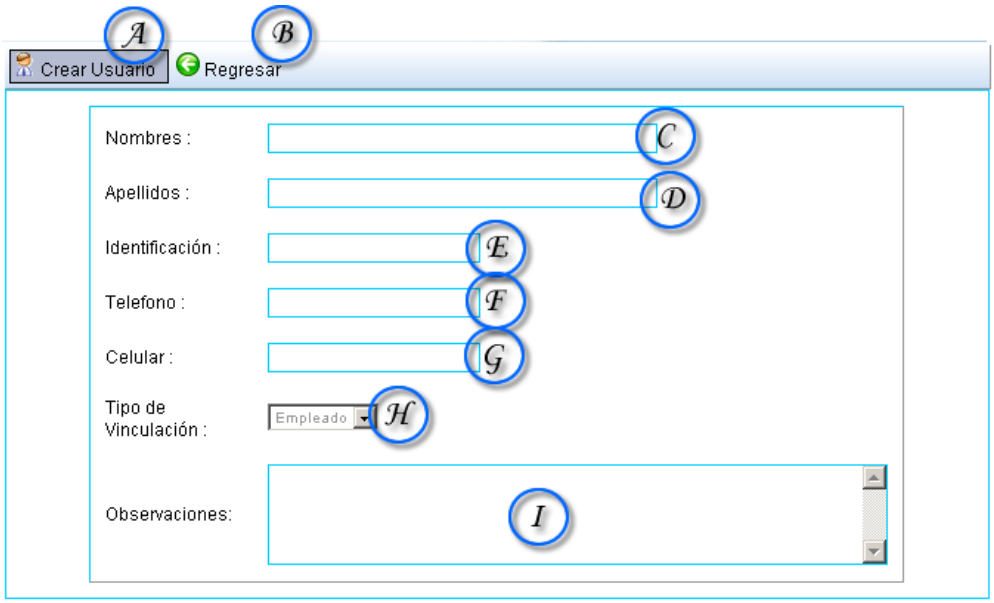


Figura 95. Crear usuarios de red

Caso de Uso: Administración de nodos de red (Creación de Usuarios de red).
Actores: Administrador del sistema
Propósito: Crea nuevos usuarios de red responsables de algún equipo conectado a la LAN.
Resumen: Brinda al administrador la posibilidad de tener un completo control de los usuarios adscritos a la red local, con el fin hacerlos responsables por los equipos que estos conecten a la LAN.

Curso Normal de los Eventos

1. Esta sección de caso de uso comienza cuando el actor presiona A de la figura 94.
2. El sistema muestra una interfaz que ayudará al administrador a ingresar los datos pertinentes del nuevo usuario, así como lo muestra la figura 95.
3. El sistema muestra el formulario correspondiente a la creación de un nuevo usuario de red, compuesto por los siguientes campos:

- C: Nombres del usuario.
- D: Apellidos del usuario.
- E: Identificación del usuario (cedula ó carné).
- F: Teléfono fijo de contacto del usuario.
- G: Celular de contacto del usuario.
- H: Tipo de vinculación a la institución.
- I: Observaciones especiales (Opcional).

4. Si el administrador desea confirmar la creación del nuevo usuario de red, presiona A de la figura 95.
5. Para cancelar la operación descrita, el administrador presiona B de la figura 95.

Línea 4: El sistema validará la información ingresada por el administrador en caso de haber duplicidad de campos.

6.1.10.3 Modificar Usuarios de red

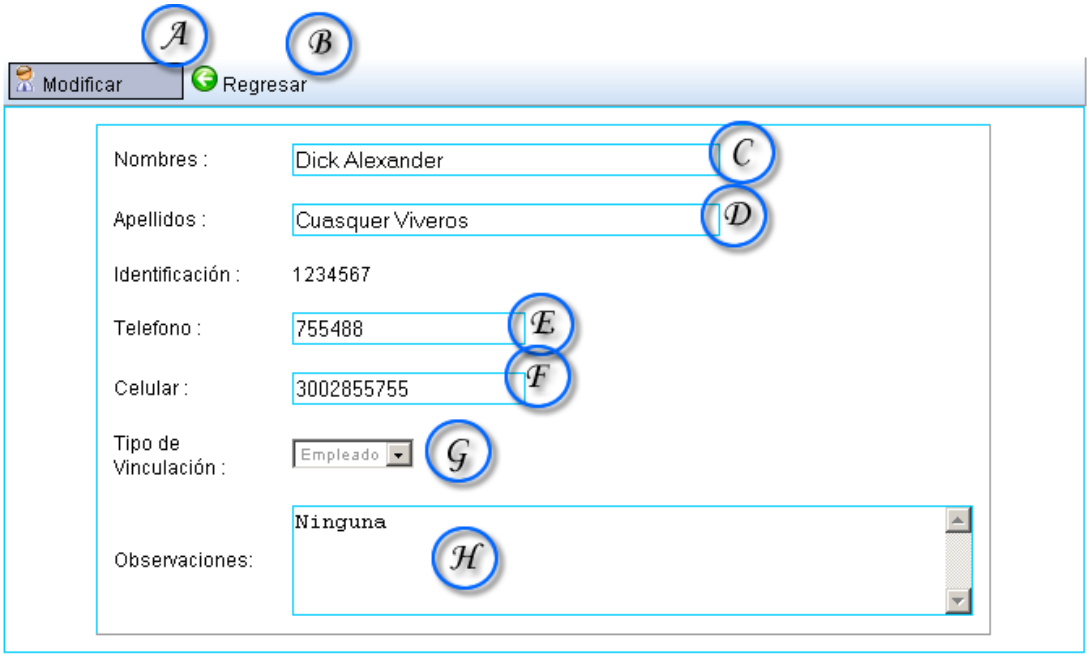


Figura 96. Modificar usuarios de red.

Caso de Uso: Administración de nodos de red (Modificar Usuarios de red).
Actores: Administrador del sistema
Propósito: Modifica usuarios de red existentes responsables de algún o algunos equipos conectados a la LAN.
Resumen: Brinda al administrador la posibilidad de tener un completo control de los usuarios adscritos a la red local, y modificar sus datos según sea conveniente.

Curso Normal de los Eventos

1. Esta sección de caso de uso comienza cuando el actor presiona B de la figura 94, luego de haber seleccionado al usuario a modificar, a través de las cajas de texto en F de la misma figura.
2. El sistema muestra una interfaz que ayudará al administrador a modificar los datos del usuario seleccionado, así como lo muestra la figura 96.
3. El sistema muestra el formulario correspondiente a la modificación de usuarios de red, compuesto por los siguientes campos:

    - C: Para modificar nombres del usuario.
    - D: Para modificar apellidos del usuario.
    - E: Para modificar teléfono fijo de contacto del usuario.
    - F: Para modificar celular de contacto del usuario.
    - G: Para modificar tipo de vinculación a la institución.
    - H: Para modificar observaciones especiales (Opcional).

4. Si el administrador desea confirmar la modificación del usuario de red, presiona sobre A de la figura 96.
5. Para cancelar la operación descrita, el administrador presiona B de la figura 96.

Línea 4: El sistema validará la información ingresada por el administrador en caso de haber duplicidad de campos.
Administración de Infraestructura

6.1.11 Administración de Sedes

Figura 97. Administración de Sedes

Caso de Uso: Administración de nodos de Red (Administración de infraestructura).
Actores: Administrador del sistema
Propósito: Manejar la infraestructura física de la institución a través de sedes, para dar un mejor orden a la red LAN.
Resumen: Brinda al administrador la posibilidad de manejar fácilmente la infraestructura de la institución a través de grandes entes como lo son las sedes de una institución si es que existen.

Curso Normal de los Eventos

1. Esta sección de caso de uso comienza cuando el actor entra en la sección "Administración" de la página principal, y luego a la sección "Administración de nodos o puntos de red" seguido por la sección "Administración de infraestructura física".
2. El sistema muestra una interfaz que ayudará al administrador a manejar de una forma más eficiente la red LAN teniendo en cuenta la distribución física de los equipos de red como se ve en la figura 97.
3. La figura 97 muestra un resumen en listado de las sedes registradas, así como también la fecha de registro de la sede así como lo muestra F de la figura 97.
4. El sistema permite seleccionar una sede determinada, a través F de la figura 97, para luego editar o eliminar el registro seleccionado a través de B y C de la figura 97 respectivamente.
5. Para crear una nueva sede, el administrador presiona A de la figura 97.
6. Para cancelar el registro y regresar, el administrador presiona D.

Línea 4: Si la sede no es seleccionada a través de la caja de texto F de la figura 97, no se podrá realizar ninguna modificación o eliminación sobre la misma. El sistema mostrará un error informativo al respecto.

6.1.11.1 Crear nueva Sede

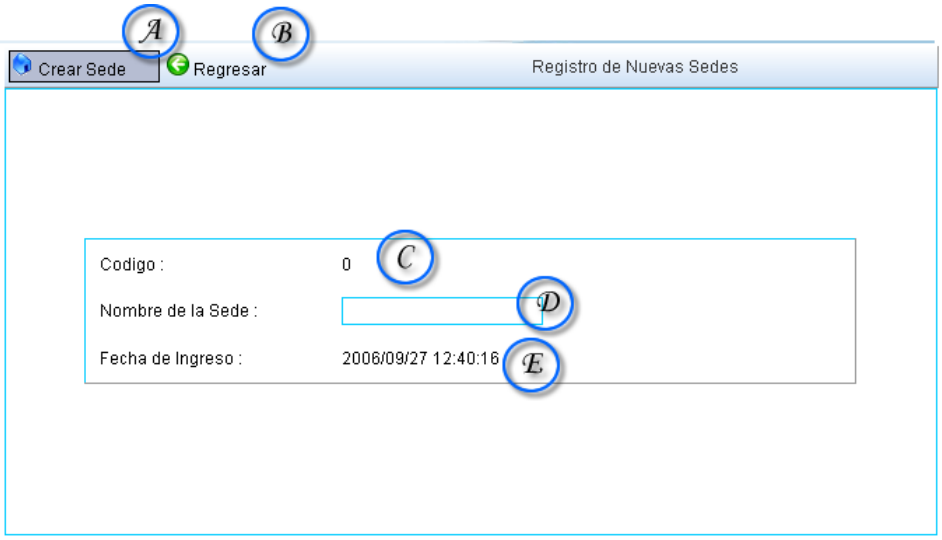


Figura 98. Crear nueva Sede

Caso de Uso: Administración Infraestructura física (Crear nueva Sede).
Actores: Administrador del sistema
Propósito: Crear nuevas sedes como elementos principales de la institución.
Resumen: Brinda al administrador la posibilidad de crear nuevas sedes cuando la expansión de la red LAN lo amerite.

Curso Normal de los Eventos

1. Esta sección de caso de uso comienza cuando el actor presiona A de la figura 97.
2. El sistema muestra una interfaz que ayudará al administrador a crear nuevas sedes en la empresa o institución así como lo muestra la figura 97.
3. El sistema muestra el formulario correspondiente a la creación de nuevas sede, compuesto por los siguientes campos:

    - C: Un código dado automáticamente por el sistema.
    - D: Un campo de texto para ingresar el nombre de la sede.
    - E: La fecha actual dada por el sistema al momento de crear la sede.

4. Si el administrador desea confirmar la creación de la nueva sede, presiona sobre A de la figura 97.
5. Para cancelar la operación descrita, el administrador presiona B de la figura 97.

6.1.11.2 Modificar Sede

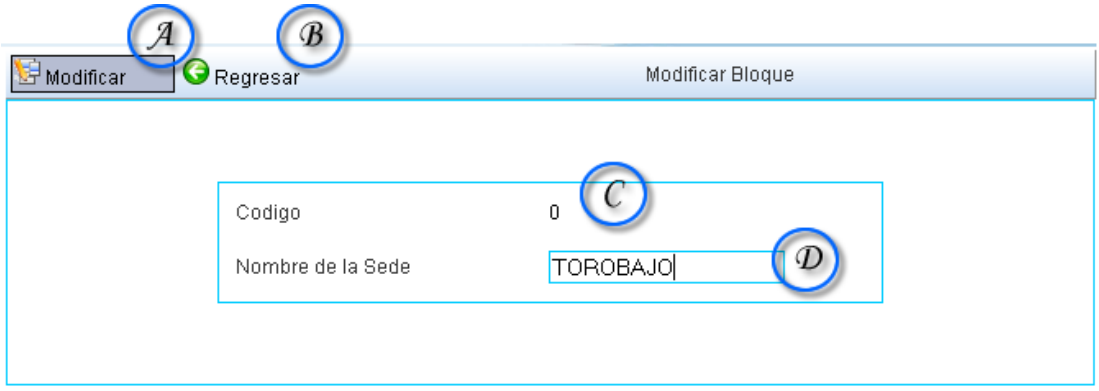


Figura 99. Modificar Sede

Caso de Uso: Administración Infraestructura física (Modificar Sede).
Actores: Administrador del sistema
Propósito: Modifica sedes existentes como elementos principales de la institución.
Resumen: Brinda al administrador la posibilidad de modificar las sedes existentes en el momento que se necesite.

Curso Normal de los Eventos

1. Esta sección de caso de uso comienza cuando el actor presiona B de la figura 97.
2. El sistema muestra una interfaz que ayudará al administrador a modificar el nombre de las sedes registradas así como lo muestra la figura 99.
3. El sistema muestra el formulario, compuesto por los siguientes campos:

    - C: El código dado automáticamente por el sistema que no es modificable.
    - D: Un campo de texto para modificar el nombre de la sede.

4. Si el administrador desea confirmar la modificación de la sede, presiona sobre A de la figura 99.
5. Para cancelar la operación descrita, el administrador presiona B de la figura 99.

6.1.13 Administración de Bloques

Figura 100. Administración de Bloques

Caso de Uso: Administración de nodos de red (Administración de infraestructura).
Actores: Administrador del sistema
Propósito: Manejar la infraestructura física de la institución a través de bloques dentro de sedes, para dar un mejor orden a la red LAN.
Resumen: Brinda al administrador la posibilidad de manejar fácilmente la infraestructura de la institución a través de entidades más pequeñas o bloques ubicadas dentro de la sedes anteriormente descritas.
Curso Normal de los Eventos

1. Esta sección de caso de uso comienza cuando el actor entra en la sección "Administración" de la página principal, y luego a la sección "Administración de nodos o puntos de red" seguido por la sección "Administración de infraestructura física - manejo de bloques".
2. El sistema muestra una interfaz que ayudará al administrador a manejar de una forma más eficiente la red LAN teniendo en cuenta la distribución física de los equipos de red como se ve en la figura 100.
3. La figura 100 muestra un resumen en listado de los bloques registrados, así como también la fecha de registro del bloque así como lo muestra F de la figura 100.
4. El sistema permite seleccionar un registro determinado, a través de F de la figura 100, para luego editar o eliminar el registro seleccionado a través de B y C de la figura 100 respectivamente.

Línea 4: Si el bloque no es seleccionado a través de la caja de texto E de la figura 100, no se podrá realizar ninguna modificación o eliminación del mismo. El sistema mostrará un error informativo al respecto.

6.1.13.1 Crear Nuevo Bloque

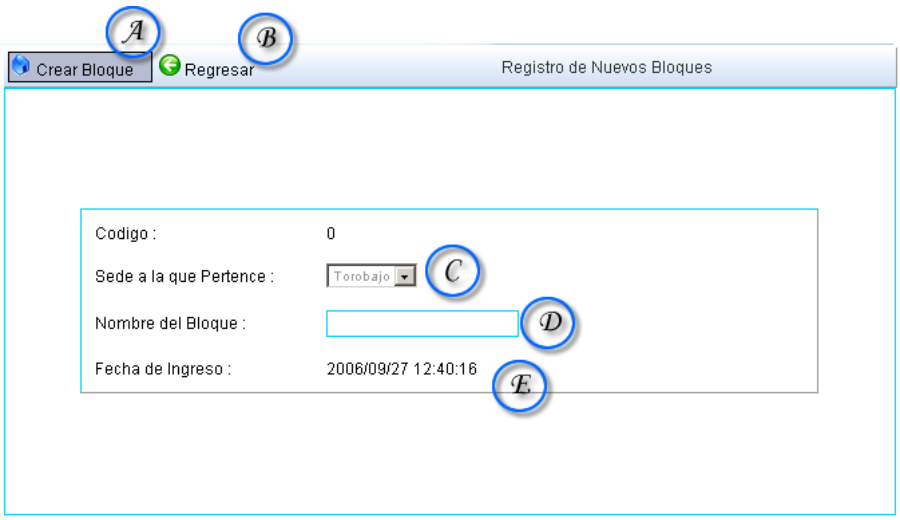


Figura 101. Crear Nuevo Bloque.

Caso de Uso: Administración Infraestructura física (Crear nuevo bloque).
Actores: Administrador del sistema
Propósito: Crear nuevos bloques como elementos secundarios en la infraestructura de la institución.
Resumen: Brinda al administrador la posibilidad de crear nuevos bloques cuando la expansión de la red LAN lo amerite.

Curso Normal de los Eventos

1. Esta sección de caso de uso comienza cuando el actor presiona A de la figura 101.
2. El sistema muestra una interfaz que ayudará al administrador a crear nuevos bloques en la empresa o institución así como lo muestra la figura 101.
3. El sistema muestra el formulario correspondiente a la creación de nuevos bloques, compuesto por los siguientes campos:

   - C: Sede al que pertenece el nuevo bloque.
   - D: Un campo de texto para ingresar el nombre del bloque.
   - E: La fecha actual dada por el sistema al momento de crear el bloque.

4. Si el administrador desea confirmar la creación del nuevo bloque, presiona sobre A de la figura 101.
5. Para cancelar la operación descrita, el administrador presiona B de la figura 101.

Línea 3: El código del nuevo bloque, es dado automáticamente por el sistema.

6.1.13.2 Modificar Bloque

Figura 102. Modificar Bloque

Caso de Uso: Administración Infraestructura física (Modificar Bloque).
Actores: Administrador del sistema
Propósito: Modifica bloques existentes como elementos secundarios de la institución.
Resumen: Brinda al administrador la posibilidad de modificar los bloques existentes en el momento que se necesite.

Curso Normal de los Eventos

1. Esta sección de caso de uso comienza cuando el actor presiona B de la figura 100, una vez se haya seleccionad con F de la figura 100 uno de los registros hechos con anterioridad.
2. El sistema muestra una interfaz que ayudará al administrador a modificar el nombre de los bloques registradas así como lo muestra la figura 102.
3. El sistema muestra el formulario, compuesto por los siguientes campos:

    - C: La sede actual a la que pertenece el bloque seleccionado.
    - D: Un campo de texto para modificar el nombre del bloque.

4. Si el administrador desea confirmar la modificación del bloque, presiona sobre A de la figura 102.
5. Para cancelar la operación descrita, el administrador presiona B de la figura 102.

6.1.14 Administración de oficinas

Figura 103. Administrar Oficinas

Caso de Uso: Administración de nodos de red (Administración de infraestructura).
Actores: Administrador del sistema
Propósito: Manejar la infraestructura física de la institución a través de oficinas dentro de bloques, para dar un mejor orden a la red LAN.
Resumen: Brinda al administrador la posibilidad de manejar fácilmente la infraestructura de la institución a través de entidades más pequeñas como oficinas ubicadas dentro de los bloque anteriormente descritos.
Curso Normal de los Eventos

1. Esta sección de caso de uso comienza cuando el actor entra en la sección "Administración" de la página principal, y luego a la sección "Administración de nodos o puntos de red" seguido por la sección "Administración de infraestructura física - manejo de oficinas".
2. El sistema muestra una interfaz que ayudará al administrador a manejar de una forma más eficiente la red LAN teniendo en cuenta la distribución física de los equipos de red como se ve en la figura 103.
3. La figura 103 muestra un resumen en listado de las oficinas registradas, así como también la fecha de registro de las oficinas tal y como lo muestra F de la figura 103.
4. El sistema permite seleccionar un registro determinado, a través de E de la figura 103, para luego editar o eliminar el registro seleccionado a través de B y C de la figura 103 respectivamente.

Línea 4: Si el bloque no es seleccionado a través de la caja de texto E de la figura 103, no se podrá realizar ninguna modificación o eliminación del mismo. El sistema mostrará un error informativo al respecto.

6.1.14.1 Crear Nueva Oficina

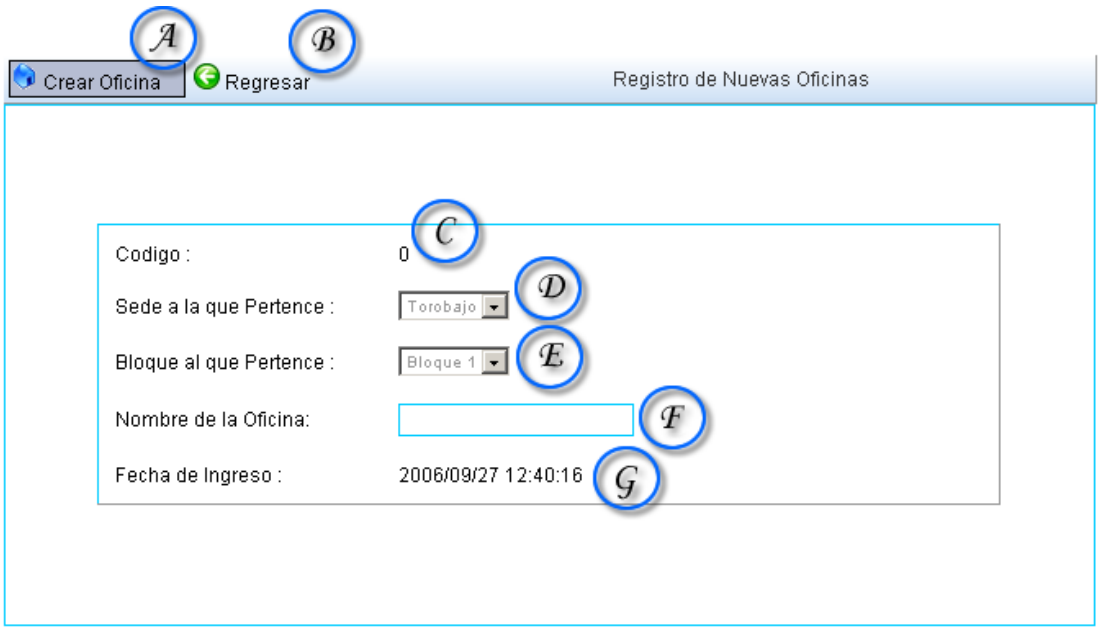


Figura 104. Crear nuevas oficinas

Caso de Uso: Administración Infraestructura física (Crear nueva oficina).

Actores: Administrador del sistema
Propósito: Crear nuevas oficinas como los elementos más pequeños en la infraestructura de la institución.
Resumen: Brinda al administrador la posibilidad de crear nuevas oficinas cuando la expansión de la red LAN lo amerite.

Curso Normal de los Eventos

1. Esta sección de caso de uso comienza cuando el actor presiona A de la figura 103.
2. El sistema muestra una interfaz que ayudará al administrador a crear nuevas oficinas en la empresa o institución así como lo muestra la figura 103.
3. El sistema muestra el formulario correspondiente a la creación de nuevas oficinas, compuesta por los siguientes campos:

    - C: Código de la oficina asignado automáticamente por el sistema.
    - D: Sede a la que pertenece la oficina.

- E: Bloque al que pertenece la oficina.
- F: Nombre de la oficina.
- G: Fecha de registro de la oficina, asignada por el sistema al momento de crearla.

4. Si el administrador desea confirmar la creación del nuevo bloque, presiona sobre A de la figura 103.
5. Para cancelar la operación descrita, el administrador presiona B de la figura 103.

Línea 3: El código de la nueva oficina, es dado automáticamente por el sistema, y la fecha no podrá ser modificable para mayor veracidad en la información.

6.1.14.2 Modificar Oficina

Figura 105. Modificar Oficinas

Caso de Uso: Administración Infraestructura física (Modificar Oficina).
Actores: Administrador del sistema
Propósito: Modifica oficinas existentes como elementos secundarios de la institución.
Resumen: Brinda al administrador la posibilidad de modificar las oficinas existentes en el momento que se necesite.

Curso Normal de los Eventos

1. Esta sección de caso de uso comienza cuando el actor presiona B de la figura 103, una vez se haya seleccionado F de la figura 103, uno de los registros hechos con anterioridad.
2. El sistema muestra una interfaz que ayudará al administrador a modificar el nombre de las oficinas registradas así como lo muestra la figura 105.

3. El sistema muestra el formulario, compuesto por los siguientes campos:

    - C: La sede actual a la que pertenece la oficina seleccionada.
    - D: El bloque actual al cual pertenece la oficina seleccionada.
    - E: El nuevo nombre de la oficina a modificar.

4. Si el administrador desea confirmar la modificación de la oficina, presiona sobre A de la figura 105.
5. Para cancelar la operación descrita, el administrador presiona B de la figura 105.

6.1.15 Administrar equipos

Figura 106. Administrar Equipos

Caso de Uso: Administración de nodos de red (Administración de Equipos).
Actores: Administrador del sistema
Propósito: Ayuda a controlar un registro de los equipos conectados a la red.
Resumen: Brinda al administrador la posibilidad de controlar fácilmente los equipos conectados a la red con sus principales características.

Curso Normal de los Eventos

1. Esta sección de caso de uso comienza cuando el actor entra en la sección "Administración" de la página principal, y luego a la sección "Administración de nodos o puntos de red" seguido por la sección "Administración de Equipos".
2. El sistema muestra una interfaz que ayudará al administrador controlar los equipos que hacen parte de la red local o LAN de la institución como lo muestra la figura 106.
3. La figura 106 muestra un resumen en listado de los equipos registrados, así como también el usuario responsable de este, la oficina a la cual pertenece el equipo y obviamente la dirección física asignada.

4. El sistema permite seleccionar un registro determinado, a través de E de la figura 106, para luego editar o eliminar el registro seleccionado a través de B y C de la figura 106 respectivamente.

Línea 4: Si el equipo no es seleccionado a través de la caja de texto E de la figura 106, no se podrá realizar ninguna modificación o eliminación del mismo. El sistema mostrará un error informativo al respecto.

6.1.15.1 Agregar Equipo

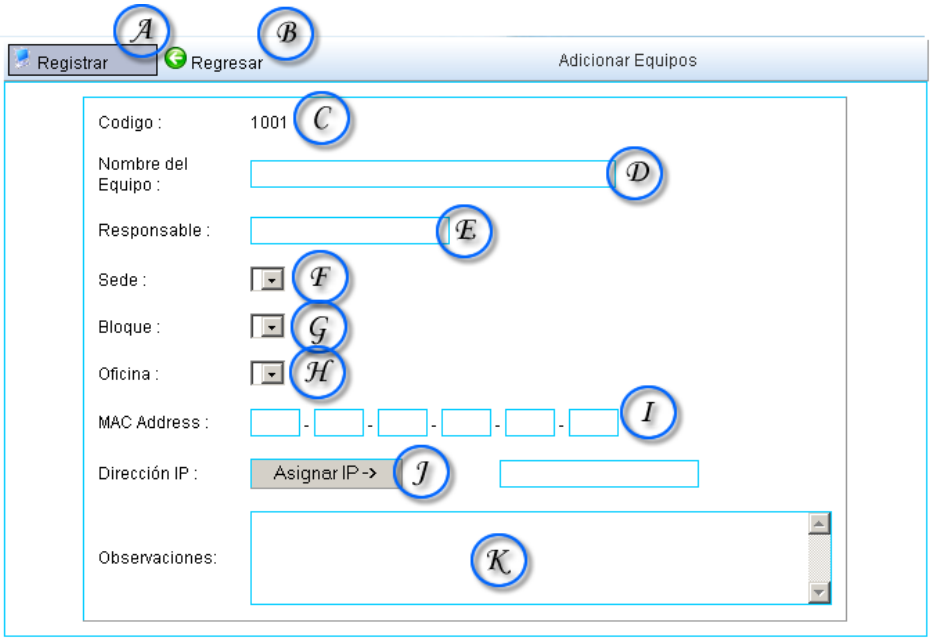


Figura 107. Agregar Equipos

Caso de Uso: Administración de Nodos de red (Crear nueva equipo).
Actores: Administrador del sistema
Propósito: Registrar nuevos equipos de computo a la red local.
Resumen: Brinda al administrador la posibilidad de ingresar fácilmente, nuevos equipos de computo a la red LAN cuando se requiera.

Curso Normal de los Eventos

1. Esta sección de caso de uso comienza cuando el actor presiona A de la figura 106.

2. El sistema muestra una interfaz que ayudará al administrador a registrar nuevos equipos en la empresa o institución así como lo muestra la figura 107.
3. El sistema muestra el formulario correspondiente al registro de nuevos equipos de computo a la red, compuesta por los siguientes campos:

    - C: Código del equipo asignado automáticamente por el sistema.
    - D: Nombre del Equipo.
    - E: Usuario de red, responsable del equipo.
    - F: Sede a la cual pertenece el equipo.
    - G: Bloque a la cual pertenece el equipo.
    - H: Oficina a la cual pertenece el equipo.
    - I: Dirección física del equipo a registrar. (MAC address).
    - J: Botón de asignación automática de dirección IP.
    - K: Observaciones adicionales del equipo.

4. Si el administrador desea confirmar el registro del nuevo equipo, presiona sobre A de la figura 107.
5. Para cancelar la operación descrita, el administrador presiona B de la figura 107.

Línea 3: El código del nuevo equipo, es dado automáticamente por el sistema.

6.1.15.2 Modificar Equipos

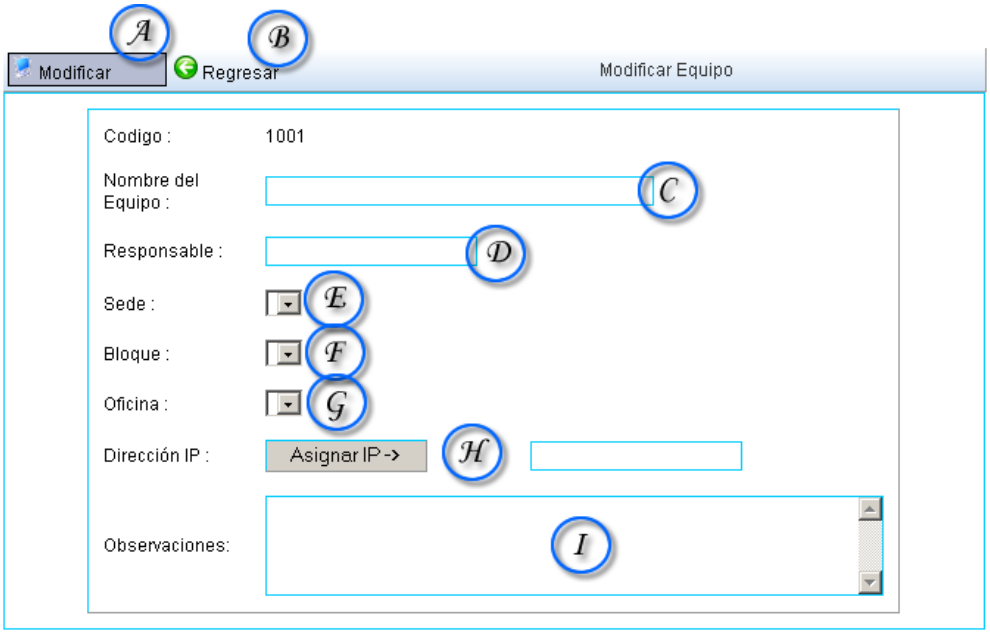


Figura 108. Modificar Equipos

Caso de Uso: Administración de Nodos de red (Crear nueva equipo).
Actores: Administrador del sistema
Propósito: Registrar equipos de computo existentes en la red local.
Resumen: Brinda al administrador la posibilidad de modificar fácilmente, equipos de computo existentes en la red LAN cuando se requiera.

Curso Normal de los Eventos

1. Esta sección de caso de uso comienza cuando el actor presiona B de la figura 106.
2. El sistema muestra una interfaz que ayudará al administrador a modificar la información de los equipos conectados a la red en la empresa o institución así como lo muestra la figura 108.
3. El sistema muestra el formulario correspondiente al registro de nuevos equipos de computo a la red, compuesta por los siguientes campos:

    - C: Nombre del Equipo a modificar.
    - E: Usuario de red, responsable del equipo a modificar.
    - F: Sede a la cual pertenece el equipo a modificar.
    - G: Bloque a la cual pertenece el equipo a modificar.
    - H: Oficina a la cual pertenece el equipo a modificar.
    - I: Dirección física del equipo a registrar. (MAC address) a modificar.
    - J: Botón de asignación automática de dirección IP a modificar.
    - K: Observaciones adicionales del equipo a modificar.

4. Si el administrador desea confirmar el registro del nuevo equipo, presiona sobre A de la figura 108.
5. Para cancelar la operación descrita, el administrador presiona B de la figura 108.

Línea 3: El código del nuevo equipo, es dado automáticamente por el sistema y no es modificable.

6.1.15.3 Ver Estado de Equipos

Figura 109. Ver estado de Equipos

Caso de Uso: Administración de Nodos de red (Crear nueva equipo).
Actores: Administrador del sistema
Propósito: Monitoriza los quipos de computo conectados a la red local.
Resumen: Brinda al administrador la posibilidad de monitorizar fácilmente los equipos de computo conectados a la red LAN cuando se requiera.

Curso Normal de los Eventos

1. Esta sección de caso de uso comienza cuando el actor presiona D de la figura 106, luego de haber seleccionado un equipo registrado anteriormente mediante E de la misma figura.
2. El sistema muestra una interfaz que ayudará al administrador a monitorizar el estado, y las características principales del equipo seleccionado, así como lo muestra B en la figura 109.
3. Si el administrador desea regresar, presiona sobre A de la figura 109.

6.1.16 Administrar de ancho de banda

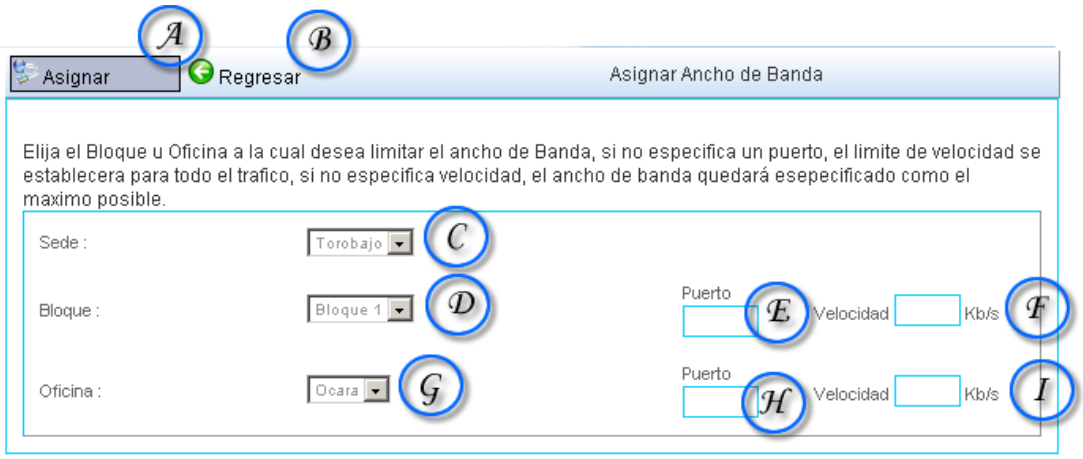


Figura 110. Administrar Ancho de Banda

Caso de Uso: Administrar ancho de banda.
Actores: Administrador del sistema.
Propósito: Brinda un ancho de banda específico a un bloque u oficina.
Resumen: Brinda al administrador la posibilidad de brindar un ancho de banda específico a un bloque u oficina para cualquier eventualidad.

Curso Normal de los Eventos

1. Esta sección de caso de uso comienza cuando el actor entra a la sección Administrador de la página principal a la sección de “Administración de ancho de banda”.
2. El sistema muestra una interfaz que ayudará al administrador a asignar un ancho de banda específico, seleccionando un bloque o una oficina registrada previamente en el sistema.
3. Para seleccionar una sede específica el actor utiliza la lista en D de la figura 110.
4. Para seleccionar un bloque específico el actor utiliza la lista en E de la figura 110.
5. Para seleccionar una oficina específica el actor utiliza la lista en G de la figura 110.
6. Para gestionar el tráfico de un bloque en un puerto específico se utiliza E. junto con F para especificar la velocidad.
7. Para gestionar el tráfico de una oficina en un puerto específico se utiliza H de la figura 110, junto con I para especificar la velocidad.
8. Para asignar los datos ingresados, el actor presiona sobre A de la figura 110.
9. Para cancelar cualquier cambio de la figura 110, el actor presiona en B de la figura 110.

6.1.17 Administrador servidor proxy

6.1.17.1 Control de Subredes

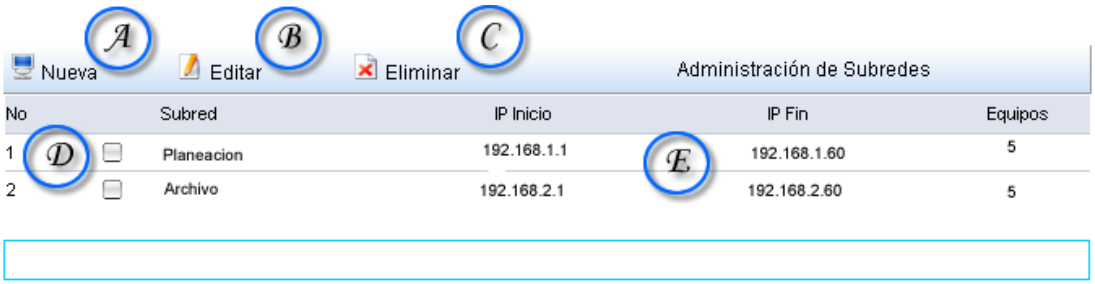


Figura 111. Control de Subredes

Caso de Uso: Control de Subredes Proxy.

Actores: Administrador del sistema.
Propósito: Controla el acceso a las subredes que tendrán acceso ó salida a Internet a través del servidor Proxy.
Resumen: Brinda al administrador la posibilidad de controlar todas y cada una de la subredes que tendrán acceso o salida a Internet a través del Proxy.

Curso Normal de los Eventos

1. Esta sección de caso de uso comienza cuando el actor entra a la sección Administración de la página principal en la sección de "Administración de servidor Proxy", en "control y manejo de subredes Proxy".
2. El sistema muestra una interfaz que ayudará al administrador a manejar las subredes que estén registradas para que posean acceso a Internet a través del Proxy transparente.
3. Para seleccionar adiciona una nueva subred al Proxy, se selecciona o presiona A de la figura 111
4. Para editar una de las subredes ya registradas, se presiona B de la figura 111, después de haber seleccionado un registro a través de D de la misma figura.
5. Para eliminar una de las subredes ya registradas, se presiona C de la figura 111, después de haber seleccionado un registro a través de D de la misma figura
6. La interfaz también muestra información sobre el nombre de las subredes, su equipo de inicio, su equipo de fin, así como lo muestra E de la figura 111.

Línea 4-5: Si el equipo no es seleccionado a través de la caja de texto D de la figura 111, no se podrá realizar ninguna modificación o eliminación del mismo. El sistema mostrará un error informativo al respecto.

6.1.17.2 Crear Subred Proxy

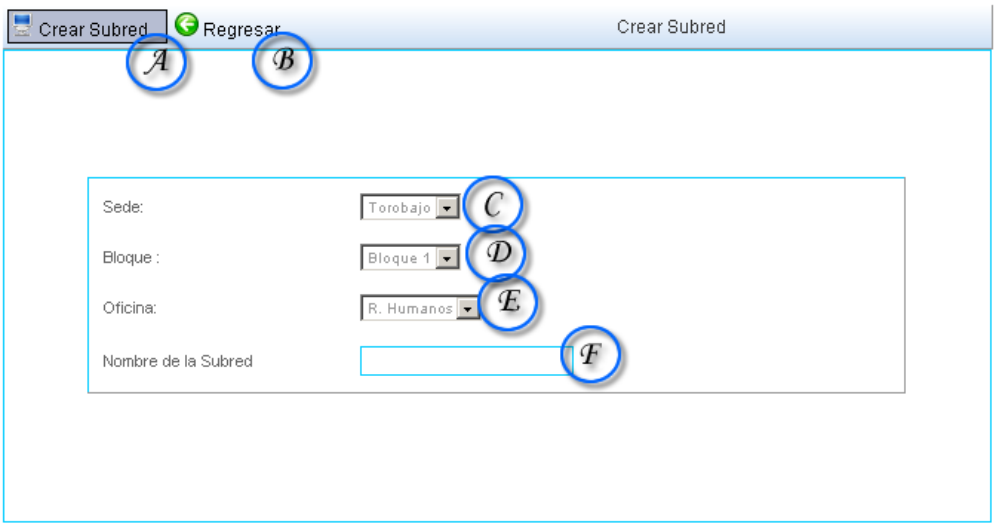


Figura 112. Crear Subred Proxy.

Caso de Uso: Administración de Subredes Proxy (Crear Subred).
Actores: Administrador del sistema.
Propósito: Crea subredes de acceso al servidor Proxy.
Resumen: Brinda al administrador la posibilidad de crear nuevas subredes para que estas tengan acceso a Internet a través de Proxy.

Curso Normal de los Eventos

1. Esta sección de caso de uso comienza cuando el actor presiona A de la figura 111
2. El sistema muestra una interfaz que ayudará al administrador a crear subredes Proxy a partir de subredes ya creadas en el momento de administrar infraestructura o equipos de red.
3. Para adicionar una sede, el actor se guía a través de la ubicación de la misma, a través de las listas C, D, E de la figura 112.
4. La subred aparecerá automáticamente en F de la figura 112.
5. Para dar acceso de Proxy a esa subred el actor presiona A de la figura 112.
6. Para descartar cualquier cambio presiona B de la figura 112.

6.1.17.3 Modificar Subred Proxy

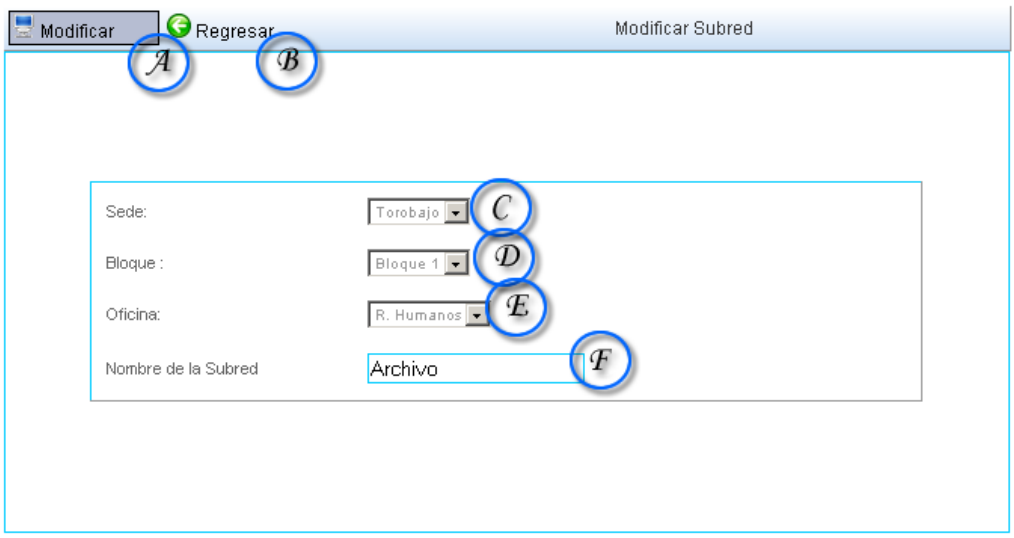


Figura 113. Modificar subred Proxy.

Caso de Uso: Administración de Subredes Proxy (Crear Subred).
Actores: Administrador del sistema.
Propósito: Modifica subredes de acceso al servidor Proxy.
Resumen: Brinda al administrador la posibilidad de modificar subredes para que estas tengan acceso a Internet a través de Proxy.

Curso Normal de los Eventos

1. Esta sección de caso de uso comienza cuando el actor presiona B de la figura 111
2. El sistema muestra una interfaz que ayudará al administrador a modificar subredes Proxy a partir de subredes ya creadas en el momento de administrar infraestructura o equipos de red.
3. Para modificar una sede, el actor se guía a través de la ubicación de la misma, a través de las listas C, D, E de la figura 113.
4. La subred aparecerá automáticamente en F de la figura 113.
5. Para dar acceso de Proxy a esa subred el actor presiona A de la figura 113.
6. Para descartar cualquier cambio presiona B de la figura 113.

6.1.17.4 Administrar tipos de archivos

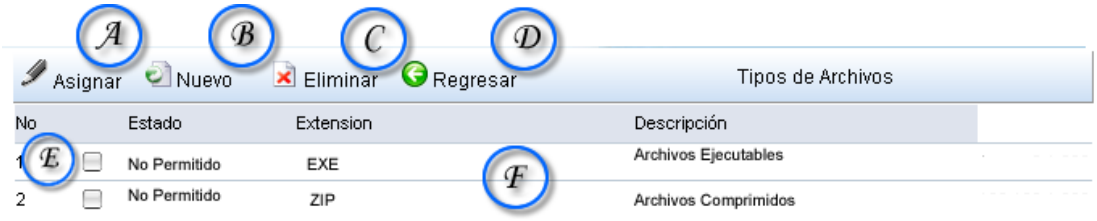


Figura 114. Administrar Tipos de Archivo.

Caso de Uso: Administrar Tipos de archivos.
Actores: Administrador del sistema.
Propósito: Controla el acceso a ciertos tipos de archivo.
Resumen: Brinda al administrador la posibilidad de controlar el acceso o descarga de ciertos tipos de archivos con el fin de evitar congestiones de tráfico.

Curso Normal de los Eventos

1. Esta sección de caso de uso comienza cuando el actor entra a la sección Administración de la página principal en la sección de "Administración de servidor Proxy", en "Administración de tipos de archivo".
2. El sistema muestra una interfaz que ayudará al administrador a manejar los tipos de archivo dentro de la red local, y controla su acceso.
3. Para adicionar un nuevo tipo de archivo presiona B de la figura 114.
4. Para restringir una extensión ya registrada en el sistema, el actor presiona A de la figura 114 una vez haya seleccionado a través de E de la figura 114, el registro de la extensión.
5. Para eliminar una extensión ya registrada en el sistema, el actor presiona C de la figura 114 una vez haya seleccionado a través de E de la figura 114, el registro de la extensión.
6. Para regresar sin hacer ningún cambio, se presiona D de la figura 114.
7. La interfaz también muestra información sobre las extensiones registradas en el sistema, y una breve descripción de su funcionamiento, al igual de su estado, activado o desactivado, tal y como lo muestra F en la figura 114.

Línea 4-5: Si el equipo no es seleccionado a través de la caja de texto D de la figura 114, no se podrá realizar ninguna asignación o eliminación de la extensión. El sistema mostrará un error informativo al respecto.

6.1.17.5 Agregar Tipos de Archivos

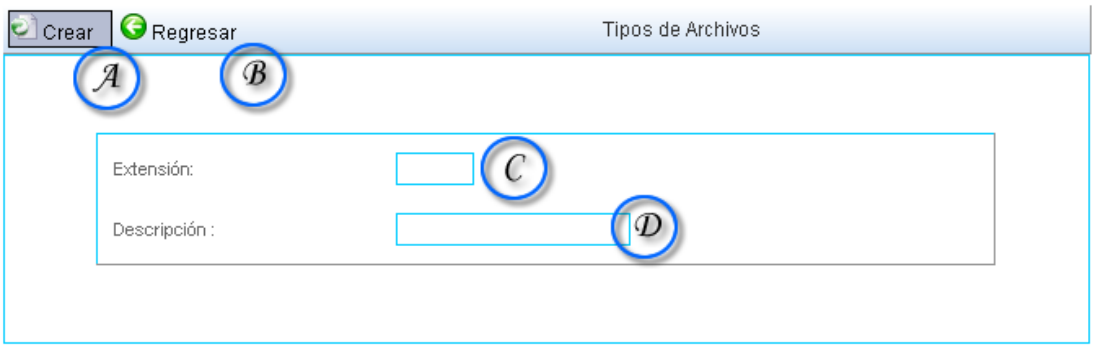


Figura 115. Agregar tipos de archivo

Caso de Uso: Administración de tipos de archivos (Agregar tipos de archivo).
Actores: Administrador del sistema.
Propósito: Registra tipos de archivo a restringir.
Resumen: Brinda al administrador la posibilidad de agregar nuevos tipos o extensiones de archivo al sistema para que este pueda en un momento dado restringido.

Curso Normal de los Eventos

1. Esta sección de caso de uso comienza cuando el actor presiona B de la figura 114
2. El sistema muestra una interfaz que ayudará al administrador a registrar nuevos tipos o extensiones de archivos para ser restringidos.
3. Para registrar una extensión se utiliza el campo C de la figura 115.
4. para registrar una descripción de la nueva extensión de utiliza el campo D de la figura 115.
5. Para cancelar cualquier operación, se presiona B de la figura 115.
6. Para confirmar el registro de la nueva extensión, el actor presiona A de la figura 115.

6.1.17.6 Administrar de Caché

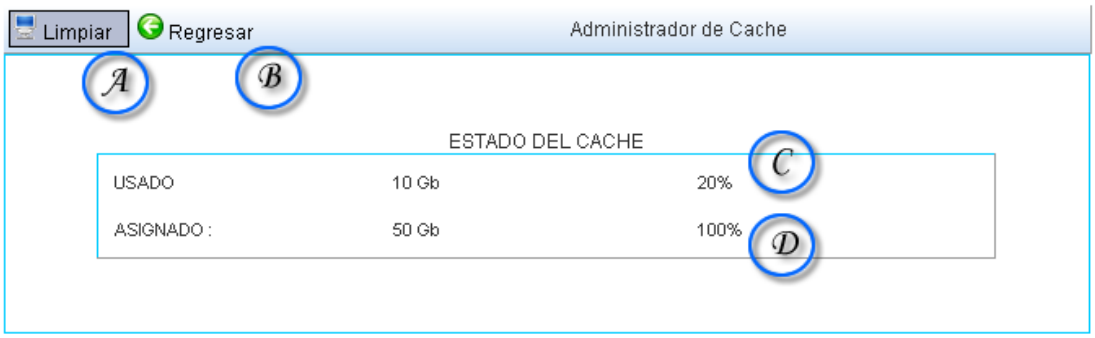


Figura 116. Administrar Caché.

Caso de Uso: Administración de servidor Proxy (Administrar Caché).
Actores: Administrador del sistema.
Propósito: Monitoriza y Limpia el Espacio de Caché ocupado.
Resumen: Brinda al administrador la posibilidad de Monitorizar el espacio de caché ocupado en el servidor, y limpiarlo de ser necesario.

Curso Normal de los Eventos

1. Esta sección de caso de uso comienza cuando el actor ingresa a Administración de Servidor Proxy, en la sección de "Administración de caché de Proxy".
2. El sistema muestra una interfaz que ayudará al administrador realizar el monitoreo pertinente.
3. Para observar el estado de caché, el actor se guía a través de C y D de la Figura 116.
4. Para limpiar el caché actual, el actor presiona A de la figura 116.
5. Para cancelar cualquier operación y regresar, se presiona B de la figura 116.

6.1.18 Administrar filtro web

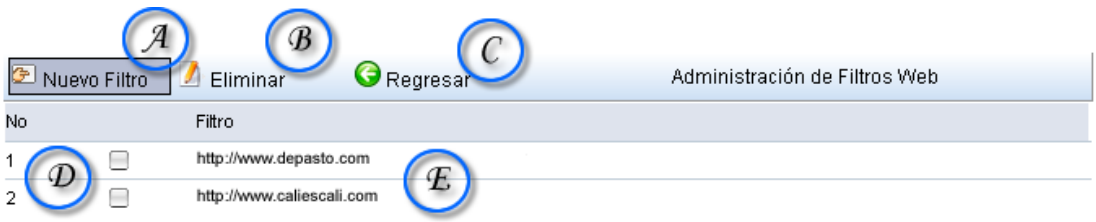


Figura 117. Administrar Filtro Web

Caso de Uso: Control de Subredes Proxy.
Actores: Administrador del sistema.
Propósito: Controla ciertas URLS y palabras no aptas en una red local.
Resumen: Brinda al administrador la posibilidad de restringir URLS y palabras separadas, con el fin de evitar una mala utilización de la red local (Pornografía, Drogas, Piratería, etc.).

Curso Normal de los Eventos

1. Esta sección de caso de uso comienza cuando el actor entra a la sección Administración de la página principal en la sección de "Administración de servidor Proxy", en "Administrar Filtro Web".
2. El sistema muestra una interfaz que ayudará al administrador a controlar y restringir URLS y palabras dentro del tráfico de Internet de los usuarios.
3. Para adicionar una nueva URL ó palabra a ser restringida, de presiona sobre A de la figura 117.
4. Para observar las URLS o palabras actualmente restringidas, el actor de apoya en E de la figura 117.
5. Para eliminar alguna URL ó palabra, se presiona sobre B de la figura 117 una vez el registro a eliminar haya sido seleccionado a través de D de la misma figura.
6. Para cancelar cualquier cambio o modificación, se presiona C de la figura 117.

Línea 5: Si el equipo no es seleccionado a través de la caja de texto D de la figura 117, no se podrá realizar ninguna eliminación del mismo. El sistema mostrará un error informativo al respecto.

6.1.18.1 Agregar Filtro Web

Figura 118. Agregar Filtro Web

Caso de Uso: Administración de filtro Web (Agregar filtro Web).
Actores: Administrador del sistema.
Propósito: Registra URLS o palabras a restringir.
Resumen: Brinda al administrador la posibilidad de registrar URLS o palabras maliciosas con el fin de optimizar una mayor utilidad a la red LAN.

Curso Normal de los Eventos

1. Esta sección de caso de uso comienza cuando el actor presiona A de la figura 117.
2. El sistema muestra una interfaz que ayudará al administrador a registrar URLS o palabras maliciosas.
3. Para registrar una URLS, el actor escribe sobre C de la figura 118.
4. Para registrar una palabra, el actor escribe sobre D de la figura 118.
5. Para confirmar el registro, el actor presiona sobre A de la figura 118.
6. Para cancelar cualquier cambio, el actor presiona sobre B de la figura 118.

6.1.19 Administración de firewall (cortafuegos)

6.1.19.1 Administración de puertos y servicios básicos de red

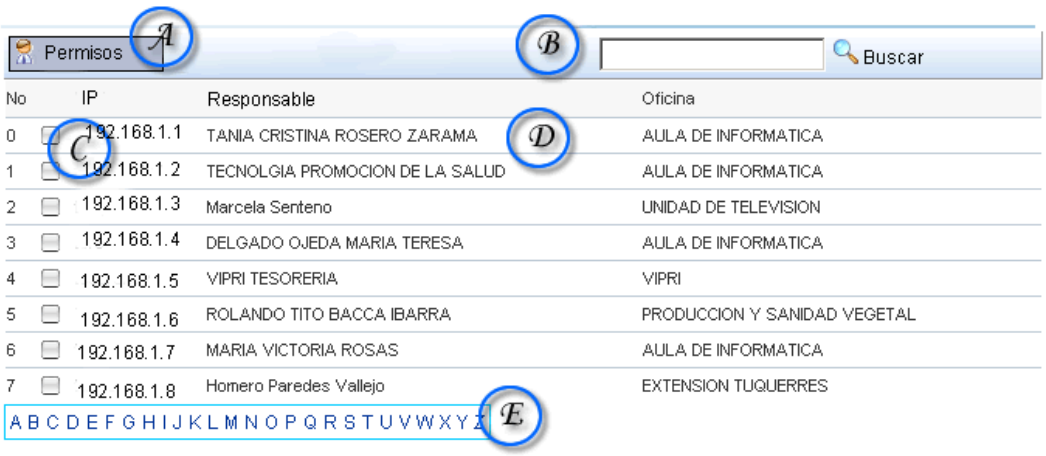


Figura 119. Administración de puertos y servicios básicos de red.

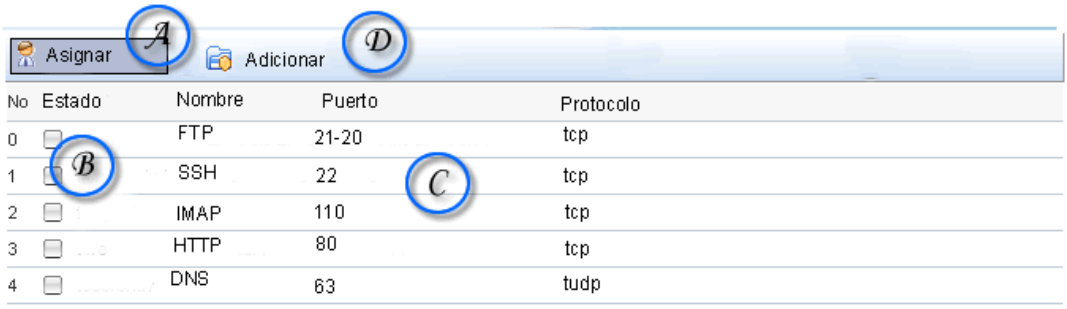


Figura 120 Administración de servicios específicos.

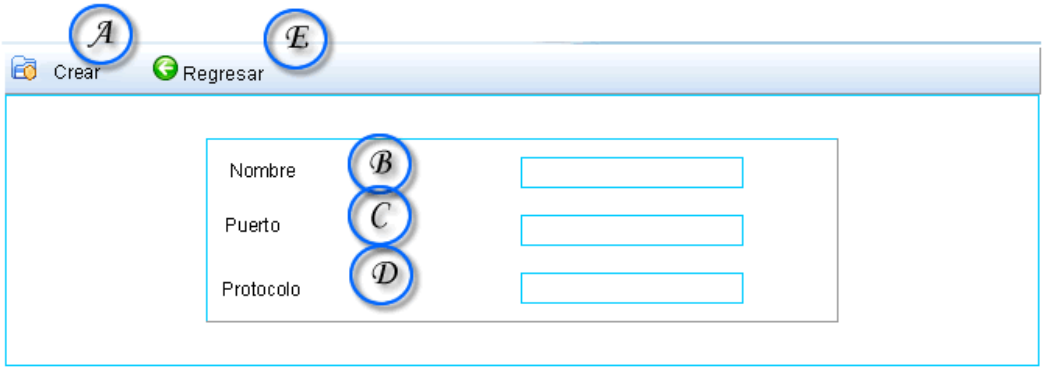


Figura 121 Asignación de servicios específicos.

Caso de Uso: Administración de Puertos y servicios básicos de red.
Actores: Administrador del sistema.
Propósito: Controla los accesos a puertos de red a los equipos conectados a esta.
Resumen: Brinda al administrador la posibilidad de tener un completo control tanto de la red como tal como del acceso de sus usuarios, a través de la gestión de los puertos de red ya sean TCP ó UDP en el servidor principal de internet o Proxy.

Curso Normal de los Eventos

1. Esta sección de caso de uso comienza cuando el actor entra a la sección Administración de la página principal en la sección de “Administración de Firewall”, en “Administración de puertos y servicios básicos de red”.
2. Para visualizar los permisos de red de algún usuario en particular, se selecciona primero el usuario del cual se necesite la información a través de C de la figura 119, y luego se presiona A de la figura 119.
3. Para buscar un equipo en particular se utiliza la barra de búsqueda de B de la figura 119, o bien utilizando la barra alfabética ubicada en E de la figura 119.
4. La información sobre los equipos, sus responsables y las oficinas a las cuales pertenecen están dadas en D de la figura 119.
5. Para adicionar un nuevo puerto que representa un servicio determinado, se presiona D de la figura 120.
6. Para asignar un nuevo puerto de red se presiona A de la figura 120 después de haber seleccionado el servicio respectivo mediante B de la figura 120.
7. La información de los servicios se lista en C de la figura 120.
8. Para adicionar el control de un nuevo puerto de red al sistema se utiliza la interfaz de la figura 121 luego de presionar D de la figura 120.
9. Se escribe el Nombre del Servicio, Puerto de red respectivo y protocolo de res en B, C, D respectivamente.

Línea 2: Si el equipo no es seleccionado a través de la caja de texto C de la figura 119, no se podrá realizar ninguna visualización de sus propiedades. El sistema mostrará un error informativo al respecto.

Línea 6: Si el equipo no es seleccionado a través de la caja de texto B de la figura 120, no se podrá realizar modificación en sus servicios de red. El sistema mostrará un error informativo al respecto.

6.1.19.2 Administración de Servicios Especiales NAT y DNAT.

Figura 122. Administración de Servicios Especiales NAT y DNAT.

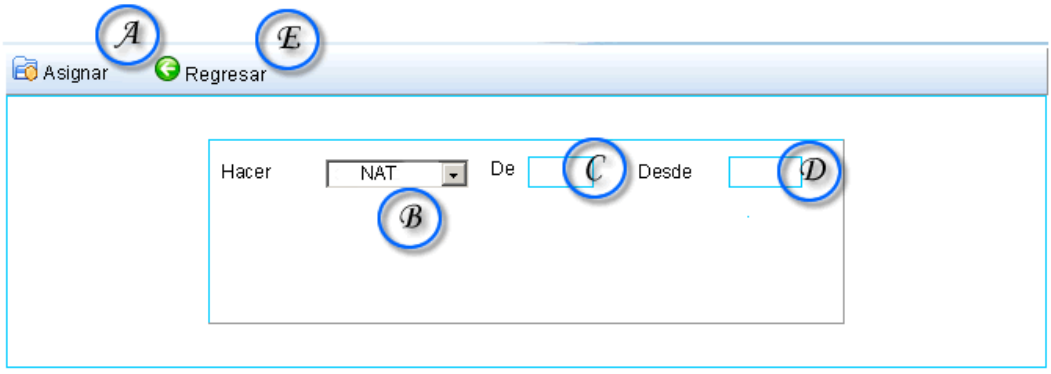


Figura. 123 Interfaz de creación de servicios avanzados de red.

Caso de Uso: Administración de servicios especiales de NAT y DNAT.
Actores: Administrador del sistema.
Propósito: Controla servicios más avanzados de red como son el NAT y el DNAT.
Resumen: Brinda al administrador la posibilidad de brindar servicios que permitan a los equipos de la red interna ser vistos desde internet o que un equipo de la red interna pueda salir directamente a internet sin necesidad de un servidor proxy.

Curso Normal de los Eventos

1. Esta sección de caso de uso comienza cuando el actor entra a la sección Administración de la página principal en la sección de “Administración firewall”, en “Administrar de servicios especiales de red NAT y DNAT”.
2. Para visualizar los permisos de red especiales de algún usuario en particular, se selecciona primero el usuario del cual se necesite la información a través de C de la figura 122, y luego se presiona A de la figura 122.
3. Para buscar un equipo en particular se utiliza la barra de búsqueda de B de la figura 122, o bien utilizando la barra alfabética ubicada en E de la figura 122.
4. La información sobre los equipos, sus responsables y las oficinas a las cuales pertenecen están dadas en D de la figura 122.
5. Para adicionar un nuevo servicio avanzado se utiliza la interfaz de la figura 123.
6. Se utiliza B de la figura 123 para determinar si el servicio va a ser un servicio NAT o un DNAT, se escribe la dirección IP en C del equipo el cual va a ser afectado, y se escribe en D la dirección IP, por lo general una IP publica la cual va a permitir en servicio.
7. En cualquier momento se presiona E para regresar al menú de la figura 122.

Línea 2: Si el equipo no es seleccionado a través de la caja de texto C de la figura 122, no se podrá realizar ninguna modificación en los servicios de red. El sistema mostrará un error informativo al respecto.

6.1.19.3 Suspensión del servicio

Figura 124. Suspensión del servicio.

Caso de Uso: Suspensión del servicio.
Actores: Administrador del sistema.
Propósito: Suspende el servicio de red a equipos maliciosos.
Resumen: Brinda al administrador la posibilidad de suspender temporal o definitivamente el servicio de red a equipos maliciosos que utilizan de forma inadecuada el servicio ya sea de Internet o Intranet.

Curso Normal de los Eventos

1. Esta sección de caso de uso comienza cuando el actor entra a la sección Administración de la página principal en la sección de “Administración firewall”, en “Suspensión de equipos”.
2. Para suspender la actividad de red de algún usuario en particular, se selecciona primero el usuario a través de C de la figura 124, y luego se presiona A de la figura 124.
3. Para buscar un equipo en particular se utiliza la barra de búsqueda de B de la figura 124, o bien utilizando la barra alfabética ubicada en E de la figura 124.
4. La información sobre los equipos, sus responsables y las oficinas a las cuales pertenecen están dadas en D de la figura 124.

Línea 2: Si el equipo no es seleccionado a través de la caja de texto C de la figura 124, no se podrá realizar ninguna suspensión de los servicios de red. El sistema mostrará un error informativo al respecto.

7. GLOSARIO

TERMINO	CATEGORIA	COMENTARIO
CGI	Concepto	Common Gateway Interface (en castellano «Interfaz Común de Pasarela», abreviado CGI) es una importante tecnología de la World Wide Web que permite a un cliente (explorador web) solicitar datos de un programa ejecutado en un servidor web. CGI especifica un estándar para transferir datos entre el cliente y el programa. Es un mecanismo de comunicación entre el servidor web y una aplicación externa.
DEMONIO	Concepto	Un demonio, daemon ó dæmon es un tipo especial de proceso informático que se ejecuta en segundo plano en vez de ser controlado directamente por el usuario (es un proceso no interactivo e infinito).
DHCP	Concepto	DHCP (sigla en inglés de Dynamic Host Configuration Protocol) es un protocolo de red que permite a los nodos de una red IP obtener sus parámetros de configuración automáticamente.
DNS	Concepto	El Domain Name System (DNS) es una base de datos distribuida y jerárquica que almacena información asociada a nombres de dominio en redes como Internet.
IMAP	Concepto	Es un protocolo de red de acceso a mensajes electrónicos almacenados en un servidor.
Inetd	Concepto	Inetd es un demonio presente en la mayoría de sistemas tipo Unix, conocido como el "Super Servidor de Internet".
IPCHAINS	Concepto	ipchains es un cortafuegos libre para Linux. Es el código reescrito del código fuente del cortafuegos IPv4 anterior de Linux, ipfwadm anterior a iptables para kernel 2.2 o más antiguos.
IPTABLES	Concepto	iptables es el nombre de la herramienta del espacio de usuario por medio de la cual el administrador crea reglas para filtrado de paquetes y para hacer NAT.
LAN	Concepto	Red de area local.
MAN	Concepto	Red de area metropolitana.

NETFILTER	Concepto	Netfilter es el conjunto de aplicaciones dentro del núcleo Linux que interceptan y manipulan paquetes de red.
P2P	Concepto	Una red informática entre iguales (en inglés peer-to-peer -que se traduciría de par a par- o de punto a punto, y más conocida como P2P [pedospe] se refiere a una red que no tiene clientes ni servidores fijos, sino una serie de nodos que se comportan simultáneamente como clientes y como servidores de los demás nodos de la red.
PERL	Concepto	Perl, Lenguaje Práctico para la Extracción e Informes. Es un lenguaje de programación diseñado por Larry Wall creado en 1987. Estructuralmente, Perl está basado en un estilo de bloques como los del C o AWK, y fue ampliamente adoptado por su destreza en el procesado de texto y no tener ninguna de las limitaciones de los otros lenguajes de script.
PHP	Concepto	PHP es un lenguaje de programación usado para la creación de contenido de sitios web. PHP es un acrónimo recurrente que significa "PHP Hypertext Pre-processor" (inicialmente PHP Tools, o, Personal Home Page Tools), y se trata de un lenguaje interpretado usado para la creación de aplicaciones para servidores, o creación de contenido dinámico para sitios web.
POP	Concepto	Post Office Protocol (Protocolo de Oficina de Correos).
PUERTO	Concepto	En computación, un puerto es una forma genérica de denominar a una interfaz por la cual diferentes tipos de datos pueden ser enviados y recibidos. Dicha interfaz puede ser física, o puede ser a nivel software (por ej: los puertos que permiten la transmisión de datos entre diferentes computadores).
SENDMAIL	Concepto	Sendmail es un popular "agente de transporte de correo" (MTA - Mail Transport Agent) en Internet, cuya tarea consiste en "encaminar" los mensajes correos de forma que estos lleguen a su destino
SERVICIO	Concepto	Una aplicación informática o programa que realiza algunas tareas en beneficio de otras aplicaciones llamadas clientes.

SERVIDOR DE APLICACIONES	Concepto	En informática se denomina servidor de aplicaciones a un servidor en una red de computadores que ejecuta ciertas aplicaciones de software. Usualmente se trata de un dispositivo de software que proporciona servicios de aplicación a los computadores cliente.
SERVIDOR DE CORREO	Concepto	Un servidor de correo es una aplicación que permite enviar mensajes (correos) de unos usuarios a otros, con independencia de la red que dichos usuarios estén utilizando.
SERVIDOR FTP	Concepto	El término servidor FTP puede significar dos cosas: un ordenador que sirve cualquier tipo de fichero, a través del Protocolo de Transferencia de Ficheros a clientes FTP o a navegadores web que lo soporten, ó un programa que implementa el protocolo FTP y trabaja como demonio sirviendo ficheros.
SERVIDOR WEB	Concepto	Un servidor web es un programa que implementa el protocolo HTTP (hypertext transfer protocol). Este protocolo está diseñado para transferir lo que llamamos hipertextos, páginas web o páginas HTML (hypertext markup language): textos complejos con enlaces, figuras, formularios, botones y objetos incrustados como animaciones o reproductores de sonidos.
SGBD	Concepto	Los Sistemas de gestión de base de datos son un tipo de software muy específico, dedicado a servir de interfaz entre la base de datos, el usuario y las aplicaciones que la utilizan.
SMTP	Concepto	Simple Mail Transfer Protocol (SMTP), o protocolo simple de transferencia de correo electrónico. Protocolo de red basado en texto utilizado para el intercambio de mensajes de correo electrónico entre computadores o distintos dispositivos (PDA's, teléfonos móviles, etc.).
SSH	Concepto	SSH (Secure SHell) es el nombre de un protocolo y del programa que lo implementa, y sirve para acceder a máquinas remotas a través de una red. Permite manejar por completo el ordenador mediante un intérprete de comandos, y también puede redirigir el tráfico de X para poder ejecutar

		programas gráficos si tenemos un Servidor X arrancado.
TCP	Concepto	El Protocolo de Control de Transmisión TCP en sus siglas en inglés, Transmission Control Protocol. El protocolo garantiza que los datos serán entregados en su destino sin errores y en el mismo orden en que se transmitieron. También proporciona un mecanismo para distinguir distintas aplicaciones dentro de una misma máquina, a través del concepto de puerto.
TFTP	Concepto	TFTP son las siglas de Trivial File Transfer Protocol (Protocolo de transferencia de archivos trivial). Es un protocolo de transferencia muy simple semejante a una versión básica de FTP. TFTP a menudo se utiliza para transferir pequeños archivos entre ordenadores en una red, como cuando un terminal X Window o cualquier otro cliente ligero arrancan desde un servidor de red.
UDP	Concepto	User Datagram Protocol (UDP) es un protocolo del nivel de transporte basado en el intercambio de datagramas. Permite el envío de datagramas a través de la red sin que se haya establecido previamente una conexión.
WAN	Concepto	Red de area extensa.

Tabla 2. Glosario de Términos Comunes.

8. BASE DE DATOS DE ANUBIS SUITE DE APLICACIONES DESTINADAS A LA ADMINSITRACION DE SERVICIOS DE REDES DE AREA LOCAL TIPO IP

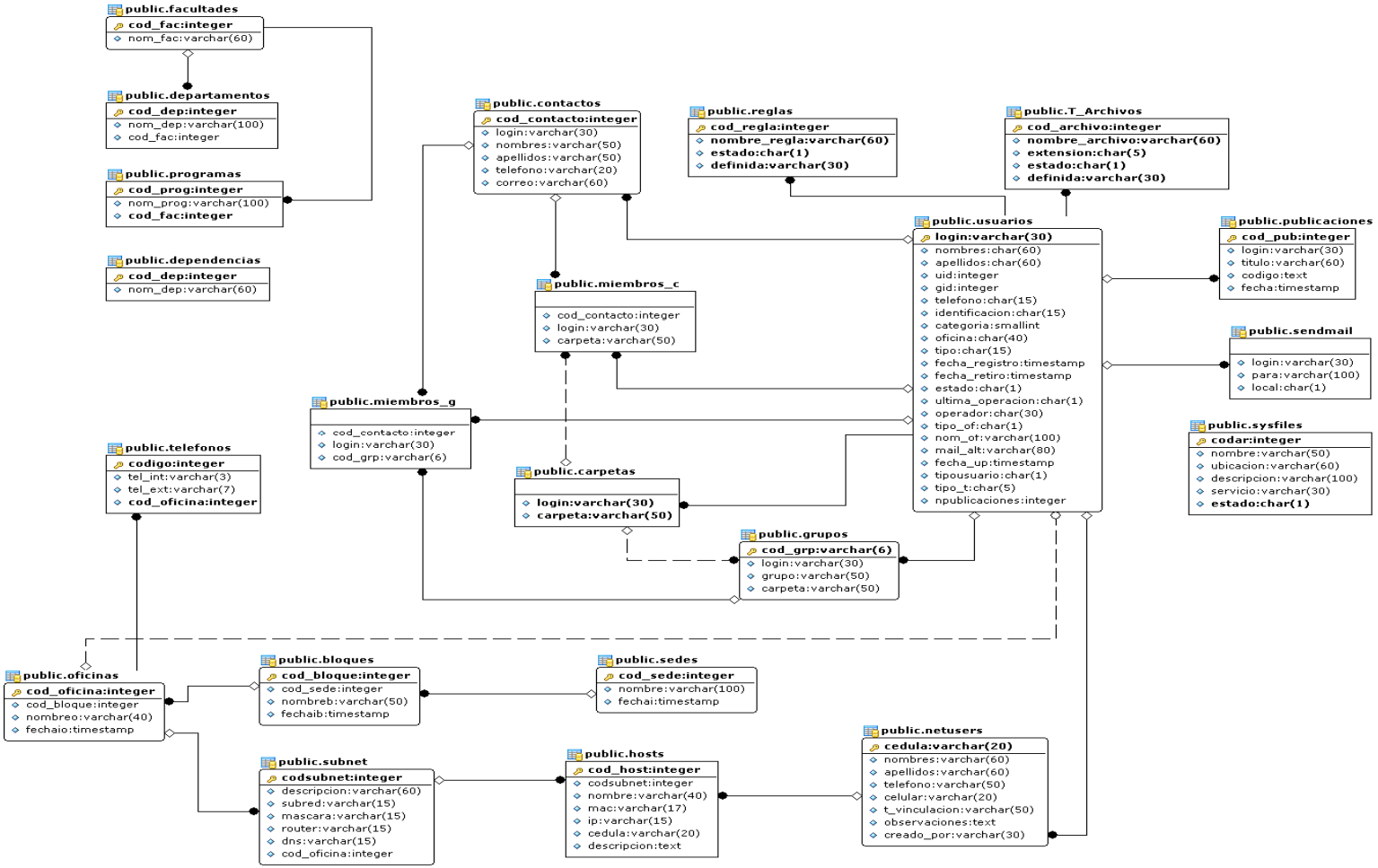


Figura 125. Diseño de Datos

8.1 LISTA DE TABLAS

TABLA	DESCRIPCION
Facultades	Almacena el nombre y código de las facultades de la institución.
Departamentos	Almacena información de los departamentos adscritos a las facultades.
Programas	Almacena los programas académicos que forman parte de cada facultad.
Dependencias	Almacena información sobre organismos más pequeños como son las dependencias.
Teléfonos	Almacena los teléfonos de las oficinas de la organización teniendo en cuenta al responsable de cada número telefónico.
Oficinas	Almacena la información de las oficinas así como también la fecha en la cual ésta es conectada a la red por primera vez.
Bloques	Almacena información sobre los bloques, edificios, o edificaciones interiores de una sede ya sea principal o secundaria.
Sedes	Almacena información sobre las sedes de la institución. Físicamente la entidad más grande que alberga bloques, los cuales albergan oficinas las cuales albergan equipos de cómputo.
Subnet	Almacena información sobre las subredes de la red de datos las cuales representan directamente a las oficinas, es decir una subred por oficina.
Hosts	Almacena la información correspondiente a los equipos de cómputo o nodos conectados a la red y los cuales hacen parte de una subred.
Netusers	Almacena la información correspondiente a los usuarios conectados a la red ya sea en Intranet o Internet, dentro de la organización.
Usuarios	Almacena información correspondiente a los usuarios inscritos

	en el servicio de correo electrónico.
Sysfiles	Almacena las rutas de los archivos de configuración del sistema operativo, lo cual es pieza fundamental para el funcionamiento del sistema.
Sendmail	Almacena la información concerniente al login de inicio de sesión, y a los remitentes del mensaje en el servicio de correo electrónico.
Publicaciones	Almacena la información concerniente al control de publicaciones Web de los usuarios.
T_Archivos	Almacena la información concerniente al control y de acceso a diferentes extensiones de archivo.
Reglas	Almacena la información concerniente a las reglas que definen el acceso a ciertas direcciones Web o URLS o palabras restringidas.
Contactos	Almacena información personal sobre los contactos de correo electrónico del usuario.
Miembros_C	Almacena información de los contactos organizados por carpetas o directorios.
Miembros_G	Almacena información de los contactos organizados por grupos.
Carpetas	Almacena información concerniente a la creación de carpetas de cada usuario de correo.
Grupos	Almacena información concerniente a la creación de los grupos de cada usuario de correo.

Tabla 3. Base de datos ANUBIS.

8.2 DESCRIPCION DE TABLAS

TABLA T_Archivos					
Campos	**Descripción**	**Tipo**	**Nulo**	**Llave primaria**	**Llave foránea**
cod_archivo	**Identificador de los archivos restringidos.**	**Entero**	**NO**	**SI**	**NO**
nombre_archivo	**Nombre de los archivos restringidos**	**Cadena**	**NO**	**NO**	**NO**
extension	**Extensión de los archivos restringidos**	**Cadena**	**NO**	**NO**	**NO**
Estado	**Estado de actividad de la restricción del archivo.**	**Carácter**	**NO**	**NO**	**NO**
definida	**Código sobre quien definió determinada política.**	**Cadena**	**NO**	**NO**	**SI (usuarios)**

Tabla 4. Descripción tabla T_Archivos.

TABLA bloques					
Campos	**Descripción**	**Tipo**	**Nulo**	**Llave primaria**	**Llave foránea**
cod_bloque	**Identificador de bloques o edificios de la institución**	**Entero**	**NO**	**SI**	**NO**
cod_sede	**Nombre de las sedes de la organización**	**Entero**	**NO**	**NO**	**SI (sedes)**
nombreb	**Nombre de los bloques o edificios interno de la organización.**	**Cadena**	**NO**	**NO**	**NO**
fechaib	**Fecha de registro del bloque**	**Fecha**	**NO**	**NO**	**NO**

Tabla 5. Descripción tabla bloques.

TABLA Carpetas					
Campos	**Descripción**	**Tipo**	**Nulo**	**Llave primaria**	**Llave foránea**
Login	**Identificador del usuario que crea la carpeta**	**Cadena**	**NO**	**SI**	**SI (usuarios)**
Carpeta	**Nombre de la carpeta dada por el usuario**	**Cadena**	**NO**	**SI**	**NO**

Tabla 6. Descripción tabla carpetas.

TABLA contactos					
Campos	**Descripción**	**Tipo**	**Nulo**	**Llave primaria**	**Llave foránea**
cod_contacto	**Identificador de contactos de correo.**	**Entero**	**NO**	**SI**	**NO**
login	**Identificador del usuario quien realiza el contacto de correo.**	**Cadena**	**NO**	**NO**	**SI (usuarios)**
nombres	**Nombre del contacto dado por el usuario.**	**Cadena**	**NO**	**NO**	**NO**
apellidos	**Apellidos de contacto dados por el usuario.**	**Cadena**	**SI**	**NO**	**NO**
telefono	**Teléfono del contacto dado por el usuario.**	**Cadena**	**SI**	**NO**	**NO**
correo	**Dirección electrónica del contacto.**	**Cadena**	**NO**	**NO**	**NO**

Tabla 7. Descripción tabla contactos.

TABLA departamentos					
Campos	**Descripción**	**Tipo**	**Nulo**	**Llave primaria**	**Llave foránea**
cod_dep	**Identificador de departamentos académicos**	**Entero**	**NO**	**SI**	**NO**
nom_dep	**Nombre del departamento**	**Cadena**	**NO**	**NO**	**NO**
cod_fac	**Código de la facultad a la cual hace parte el departamento.**	**Entero**	**NO**	**NO**	**SI (facultades)**

Tabla 8. Descripción tabla departamentos.

TABLA dependencias					
Campos	**Descripción**	**Tipo**	**Nulo**	**Llave primaria**	**Llave foránea**
cod_dep	**Identificador de dependencias administrativas**	**Entero**	**NO**	**SI**	**NO**
nom_dep	**Nombre de la dependencia**	**Cadena**	**NO**	**NO**	**NO**

Tabla 9. Descripción tabla dependencias.

TABLA facultades					
Campos	**Descripción**	**Tipo**	**Nulo**	**Llave primaria**	**Llave foránea**
cod_fac	**Identificador de facultades**	**Entero**	**NO**	**SI**	**NO**
nom_fac	**Nombre de la facultad en cuestion**	**Cadena**	**NO**	**NO**	**NO**

Tabla 10. Descripción tabla facultades.

TABLA grupos					
Campos	**Descripción**	**Tipo**	**Nulo**	**Llave primaria**	**Llave foránea**
cod_grp	**Identificador de grupos de correo**	**Cadena**	**NO**	**SI**	**NO**
login	**Identificador del usuario quien realiza el grupo de correo.**	**Cadena**	**NO**	**NO**	**SI (usuarios)**
grupo	**Nombre del grupo de correo**	**Cadena**	**NO**	**NO**	**NO**
carpeta	**Nombre de la carpeta de grupos de correo.**	**Cadena**	**NO**	**NO**	**SI(carpetas)**

Tabla 11. Descripción tabla grupos.

TABLA hosts					
Campos	**Descripción**	**Tipo**	**Nulo**	**Llave primaria**	**Llave foránea**
cod_host	**Identificador de cliente de red**	**Entero**	**NO**	**SI**	**NO**
codsubnet	**Identificador de la subred a la cual pertenece el equipo**	**Entero**	**NO**	**NO**	**SI (subnet)**
nombre	**Nombre del equipo conectado a la red.**	**Cadena**	**NO**	**NO**	**NO**
mac	**Dirección Física de la interfaz de red del equipo.**	**Cadena**	**NO**	**NO**	**NO**
ip	**Dirección lógica del equipo conectado a la red.**	**Cadena**	**NO**	**NO**	**NO**
cedula	**Identificador del responsable del equipo conectado a la red.**	**Cadena**	**NO**	**NO**	**SI(netusers)**
descripción	**Características del equipo**	**Texto**	**SI**	**NO**	**NO**

Tabla 12. Descripción tabla hosts.

TABLA miembros_C					
Campos	**Descripción**	**Tipo**	**Nulo**	**Llave primaria**	**Llave foránea**
cod_contacto	**Identificador del contacto hecho por el usuario de correo**	**Entero**	**NO**	**NO**	**SI(contactos)**
login	**Identificador del usuario quien realiza el contacto de correo.**	**Cadena**	**NO**	**NO**	**SI (usuarios)**
carpeta	**Nombre de la carpeta de contactos**	**Cadena**	**NO**	**NO**	**SI(carpetas)**

Tabla 13. Descripción tabla miembros_C.

TABLA niembros_G					
Campos	**Descripción**	**Tipo**	**Nulo**	**Llave primaria**	**Llave foránea**
cod_contacto	**Identificador del contacto hecho por el usuario de correo**	**Entero**	**NO**	**NO**	**SI(contactos)**
login	**Identificador del usuario quien realiza el contacto de correo.**	**Cadena**	**NO**	**NO**	**SI (usuarios)**
cod_grp	**Código del grupo de contactos de correo**	**Cadena**	**NO**	**NO**	**SI(grupos)**

Tabla 14. Descripción tabla miembros_G.

TABLA netusers					
Campos	**Descripción**	**Tipo**	**Nulo**	**Llave primaria**	**Llave foránea**
cedula	**Identificador del usuario de red**	**Cadena**	**NO**	**SI**	**NO**
nombres	**Nombre del usuario de red**	**Cadena**	**NO**	**NO**	**NO**
apellidos	**Apellidos del usuario de red**	**Cadena**	**NO**	**NO**	**NO**
telefono	**Teléfono del usuario de red**	**Cadena**	**NO**	**NO**	**NO**
celular	**Celular del usuario de red**	**Cadena**	**SI**	**NO**	**NO**
t_vinculacion	**Tipo de vinculación del usuario de red**	**Cadena**	**NO**	**NO**	**NO**
observaciones	**Observaciones sobre el usuario**	**Texto**	**SI**	**NO**	**NO**
creado_por	**Responsable del registro del usuario**	**Cadena**	**NO**	**NO**	**SI(usuarios)**

Tabla 15. Descripción tabla netusers.

TABLA oficinas					
Campos	**Descripción**	**Tipo**	**Nulo**	**Llave primaria**	**Llave foránea**
cod_oficina	**Identificador de la oficina**	**Entero**	**NO**	**SI**	**NO**
cod_bloque	**Identificador del bloque al cual pertenece la oficina**	**Entero**	**NO**	**NO**	**SI (bloques)**
nombreo	**Nombre de la oficina**	**Cadena**	**NO**	**NO**	**NO**
fechaio	**Fecha de ingreso al sistema de la oficina**	**Fecha**	**NO**	**NO**	**NO**

Tabla 16. Descripción tabla oficinas.

TABLA programas					
Campos	**Descripción**	**Tipo**	**Nulo**	**Llave primaria**	**Llave foránea**
cod_prog	**Identificador del programa académico**	**Entero**	**NO**	**SI**	**NO**
nom_prog	**Nombre del programa académico**	**Cadena**	**NO**	**NO**	**NO**
cod_fac	**Código de la facultad a la cual pertenece el programa**	**Entero**	**NO**	**NO**	**SI(facultades)**

Tabla 17. Descripción tabla programas.

TABLA publicaciones					
Campos	**Descripción**	**Tipo**	**Nulo**	**Llave primaria**	**Llave foránea**
cod_pub	**Identificador de la publicación Web**	**Entero**	**NO**	**SI**	**NO**
login	**Identificador del usuario autor de la publicación.**	**Cadena**	**NO**	**NO**	**SI (usuarios)**
titulo	**Titulo de la publicación.**	**Cadena**	**NO**	**NO**	**NO**
código	**Código fuente HTML de la publicación.**	**Texto**	**NO**	**NO**	**NO**
fecha	**Fecha de creación y publicación del documento Web.**	**Fecha**	**NO**	**NO**	**NO**

Tabla 18. Descripción tabla publicaciones.

TABLA reglas					
Campos	**Descripción**	**Tipo**	**Nulo**	**Llave primaria**	**Llave foránea**
cod_regla	**Identificador de la regla de filtrado Web**	**Entero**	**NO**	**SI**	**NO**
nom_regla	**Nombre de la regla de filtrado Web**	**Cadena**	**NO**	**NO**	**NO**
estado	**Estado de la regla de filtrado**	**Carácter**	**NO**	**NO**	**NO**
definida	**Identificador del creador de la regla de filtrado**	**Cadena**	**NO**	**NO**	**SI(usuarios)**

Tabla 19. Descripción tabla reglas.

TABLA sedes					
Campos	**Descripción**	**Tipo**	**Nulo**	**Llave primaria**	**Llave foránea**
cod_sede	**Identificador de la sede de la organización**	**Entero**	**NO**	**SI**	**NO**
nom_sede	**Nombre de las sedes de la organización**	**Cadena**	**NO**	**NO**	**NO**
fechai	**Fecha de ingreso al sistema de la sede**	**Fecha**	**NO**	**NO**	**NO**

Tabla 20. Descripción tabla sedes.

TABLA sendmail					
Campos	**Descripción**	**Tipo**	**Nulo**	**Llave primaria**	**Llave foránea**
login	**Identificador del usuario de correo electrónico.**	**Cadena**	**NO**	**NO**	**SI(usuarios)**
para	**Direcciones de los destinatarios de correo**	**Cadena**	**NO**	**NO**	**NO**
local	**Mandar un auto correo**	**Carácter**	**NO**	**NO**	**NO**

Tabla 21. Descripción tabla sendmail.

TABLA subnet					
Campos	**Descripción**	**Tipo**	**Nulo**	**Llave primaria**	**Llave foránea**
codsubnet	**Identificador de subred de nodos.**	**Entero**	**NO**	**SI**	**NO**
descripción	**Breve descripción sobre las características de la subred**	**Cadena**	**NO**	**NO**	**NO**
subred	**Dirección IP de la subred.**	**Cadena**	**NO**	**NO**	**NO**
máscara	**Máscara de Subred de la subred.**	**Cadena**	**NO**	**NO**	**NO**
router	**Puerta de enlace de la**	**Cadena**	**NO**	**NO**	**NO**

	subred.				
dns	**Resolución de nombres de la subred**	**Cadena**	**NO**	**NO**	**NO**
cod_oficina	**Código de la oficina a la cual pertenece.**	**Entero**	**NO**	**NO**	**SI (oficinas)**

Tabla 22. Descripción tabla subnet.

TABLA sysfiles					
Campos	**Descripción**	**Tipo**	**Nulo**	**Llave primaria**	**Llave foránea**
codar	**Identificador del archivo de configuración del sistema operativo**	**Entero**	**NO**	**SI**	**NO**
nombre_ar	**Nombre del archivo de configuración del sistema operativo**	**Cadena**	**NO**	**NO**	**NO**
ubicación	**Ubicación física del archivo**	**Cadena**	**NO**	**NO**	**NO**
descripción	**Breve descripción del archivo de configuración**	**Cadena**	**NO**	**NO**	**NO**
servicio	**Servicio al cual hace referencia el archivo de configuración.**	**Cadena**	**NO**	**NO**	**NO**
estado	**Estado del servicio de red.**	**Carácter**	**NO**	**NO**	**NO**

Tabla 23. Descripción tabla sysfiles.

TABLA telefonos					
Campos	**Descripción**	**Tipo**	**Nulo**	**Llave primaria**	**Llave foránea**
codigo	**Identificador de número telefónico organizacional**	**Entero**	**NO**	**SI**	**NO**
tel_int	**Número telefónico interno de la organización**	**Cadena**	**NO**	**NO**	**NO**
tel_ext	**Número externo o de sedes de la organización.**	**Cadena**	**NO**	**NO**	**NO**
cod_oficina	**Código de la oficina a la cual hace referencia el número telefónico.**	**Entero**	**NO**	**NO**	**SI(oficina)**

Tabla 24. Descripción tabla telefonos.

TABLA usuarios					
Campos	**Descripción**	**Tipo**	**Nulo**	**Llave**	**Llave foránea**

				primaria	
login	**Identificador de usuario**	**Cadena**	**NO**	**SI**	**NO**
nombres	**Nombre del usuario**	**Cadena**	**NO**	**NO**	**NO**
apellidos	**Apellidos del usuario**	**Cadena**	**NO**	**NO**	**NO**
uid	**Identificador de usuario del sistema operativo**	**Entero**	**NO**	**NO**	**NO**
gid	**Grupo de usuario del sistema operativo**	**Entero**	**NO**	**NO**	**NO**
teléfono	**Teléfono del usuario**	**Cadena**	**NO**	**NO**	**NO**
identificación	**Cedula o carné de vinculación**	**Cadena**	**NO**	**NO**	**NO**
categoría	**Categoría de integración a la organización.**	**Entero**	**NO**	**NO**	**NO**
oficina	**Oficina en la cual trabaja y/o estudia el usuario.**	**Cadena**	**NO**	**NO**	**SI(oficinas)**
tipo	**Tipo de usuario (administrador o no)**	**Cadena**	**NO**	**NO**	**NO**
fecha_registro	**Fecha de registro al sistema**	**Fecha**	**NO**	**NO**	**NO**
fecha_retiro	**Fecha de retiro del sistema**	**Fecha**	**SI**	**NO**	**NO**
estado	**Estado de actividad del usuario**	**Carácter**	**NO**	**NO**	**NO**
ultima_operacion	**Fecha de último acceso al sistema.**	**Fecha**	**SI**	**NO**	**NO**
operador	**Responsable de la creación de la cuenta de correo.**	**Cadena**	**NO**	**NO**	**NO**
tipo_of	**Tipo de la oficina (departamento)**	**Carácter**	**NO**	**NO**	**NO**
oficina	**Código de la oficina del usuario.**	**Entero**	**NO**	**NO**	**NO**
mail_alt	**Dirección electrónica alternativa al sistema.**	**Cadena**	**NO**	**NO**	**NO**
fecha_up	**Fecha de ingreso al sistema**	**Fecha**	**NO**	**NO**	**NO**
tipousuario	**Tipo de vinculación a la institución.**	**Carácter**	**NO**	**NO**	**NO**
tipo_t	**Tipo de trabajador**	**Carácter**	**NO**	**NO**	**NO**
npublicaciones	**Número de publicaciones**	**Entero**	**NO**	**NO**	**NO**

Tabla 25. Descripción tabla usuarios.

CONCLUSIONES

El sistema ANUBIS suite de aplicaciones destinadas a la administración de servicios de red de área local tipo IP. En este se realizó el análisis, diseño, codificación e implementación con el fin de demostrar que es posible sistematizar todos los procesos, comandos, servicios y programas desarrollados para el sistema operativo GNU/Linux, y llevarlos a la Web, lo que significaría crear un sistema administrable remotamente y de forma mucho más segura, fácil y rápida, que actuales maneras como escritorio remoto, VNC ó TELNET.

La filosofía del sistema está en adoptar los archivos de configuración de cualquier aplicación ya sea propia del sistema operativo o instalado o compilado posteriormente, para luego ser analizados e interpretados por el Sistema. Así, es posible llevar a la Web la administración de dicha aplicación o servicio de una manera mucho más simple al usuario, con lo cual se obtendría un sinnúmero de nuevos clientes que podrían administrar todo un conjunto de servicios sin necesidad de conocer la tediosa manipulación de los archivos de configuración ya que cada aplicación tiene su propia forma de configurarse o administrarse.

El lenguaje de modelado UML junto con herramientas como rational rose, facilitan en gran parte el análisis y diseño del sistema. Así mismo, los nuevos diagramas de dominio, secuencia y colaboración que UML 2.0 ofrece, brindan al lector la posibilidad de comprender más el comportamiento del sistema y no adentrarse con complejos esquemas, tablas o referencias obsoletas actualmente que no hacen más que hacer más compleja la lectura del documento tanto para el lector como para los desarrolladores.

Este proyecto permitió afianzar y generar nuevo conocimiento en cuanto a desarrollo de Software, UML 2.0, así como también entender con más profundidad en funcionamiento de los servicios en un sistema orientado a UNIX como lo es GNU/Linux. El mundo de las telecomunicaciones es el futuro de nuestra sociedad no solo regional, sino también mundial, aquí se entrega un grano de arena a la Universidad de Nariño y al mundo entero para que el conocimiento y la investigación sigan en búsqueda de la verdad.

RECOMENDACIONES

Incentivar a los estudiantes de ingeniería de sistemas por medio de este tipo de proyectos. Los sistemas de gestión de procesos son pieza clave en el buen funcionamiento de la organización.

Promover más la investigación en la rama de las Telemáticas. Las oportunidades laborales son mayores que en cualquier otra rama de la ingeniería. El futuro de la computación esta en el mundo de las redes de datos, ya sean cableadas, inalámbricas ó móviles.

ANEXOS

REDES Y SUBREDES IP

Direccionamiento

Las direcciones de Internet pueden ser simbólicas o numéricas. La forma simbólica es más fácil de leer, por ejemplo: minombre@tcpip.com. La forma numérica es un número binario sin signo de 32 bits, habitualmente expresado en forma de números decimales separados por puntos. Por ejemplo, 9.167.5.8 es una dirección de Internet válida. La forma numérica es usada por el software de IP. La función de mapeo entre los dos la realiza el ***DNS (Domain Name System***. Primeramente se examinará la forma numérica, denominada dirección IP.

La dirección IP

Los estándares para las direcciones IP se describen en ***RFC 1166 -- Números de Internet***.

Para ser capaz de identificar una máquina en Internet, a cada interfaz de red de la máquina o host se le asigna una dirección, la ***dirección IP***, o ***dirección de Internet***. Cuando la máquina está conectada a más de una red se le denomina ***"multi-homed"*** y tendrá una dirección IP por cada interfaz de red. La dirección IP consiste en un par de números:

IP dirección = <número de red<número de interfaz de red

La parte de la dirección IP correspondiente al ***número de red*** está administrada centralmente por el InterNIC(Internet Network Information Center)y es única en toda la Internet.

Las direcciones IP son números de 32 bits representados habitualmente ***en formato decimal*** (la representación decimal de cuatro valores binarios de 8 bits concatenados por puntos). Por ejemplo***128.2.7.9*** es una dirección IP, donde 128.2 es el número de red y 7.9 el de la interfaz de red. Las reglas usadas para dividir una dirección de IP en su parte de red y de interfaz de red se explican abajo.

El formato binario para la dirección IP 128.2.7.9 es:

10000000 00000010 00000111 00001001

Las direcciones IP son usadas por el protocolo IP para definir únicamente un host en la red.

Los datagramas IP(los paquetes de datos elementales intercambiados entre máquinas) se transmiten a través de alguna red física conectada a la interfaz de la máquina y cada uno de ellos contiene la ***dirección IP de origen*** y ***la dirección IP de destino***. Para enviar un datagrama a una dirección IP de destino determinada la dirección de destino de ser traducida o mapeada a una dirección física. Esto puede requerir transmisiones en la red para encontrar la dirección física de destino (por ejemplo, en LANs el ARP ("Adress Resolution Protocol", el cual se usa para traducir las direcciones IP a direcciones físicas MAC).

Los primeros bits de las direcciones IP especifican como el resto de las direcciones deberían separarse en sus partes de red y de interfaz.

Hay cinco clases de direcciones IP. Se muestran en la siguiente figura:

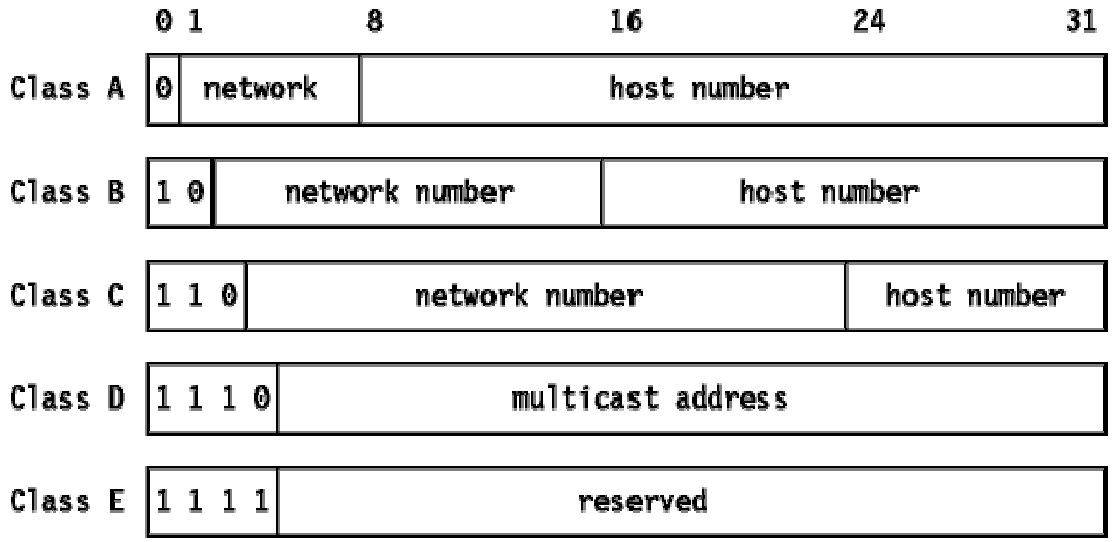


Figura 126. Clases asignadas de direcciones de Internet.

Nota: Dos de los números de red de cada una de las clases A, B y C, y dos de los números de host de cada red están pre asignados: los que tienen todos los bits a 0 y los que tienen todos los bits a 1. Son estudiados luego en Direcciones IP especiales.

- Las direcciones de clase A usan 7 bits para el número de red permitiendo 126 posibles redes (veremos posteriormente que de cada par de direcciones de red y de host, dos tienen un significado especial). Los restantes 24 bits se emplean para el número de host, de modo que cada red puede tener hasta 16,777,214 hosts.

- Las direcciones de clase B usan 14 bits para el número de red, y 16 bits para el de host, lo que supone 16382 redes de hasta 65534 hosts cada una.
- Las direcciones de clase C usan 21 bits para el número de red y 8 para el de host, lo que supone 2,097,150 redes de hasta 254 hosts cada una.
- Las direcciones de clase D se reservan para multicasting o multidifusión, usada para direccionar grupos de hosts en un área limitada. Las direcciones de clase E se reservan para usos en el futuro

Es obvio que una dirección de clase A sólo se asignará a redes con un elevado número de hosts, y que las direcciones de clase C son adecuadas para redes con pocos hosts. Sin embargo, esto significa que las redes de tamaño medio (aquellas con más de 254 hosts o en las que se espera que en el futuro haya más de 254 hosts) deben usar direcciones de clase IP.

El número de redes de tamaño pequeño y medio ha ido creciendo muy rápidamente en los últimos años y se temía que de haber permitido que se mantuviera este crecimiento, todas las direcciones de clase B se habrían usado para mediados de los '90. Esto es lo que se conoce como el problema del agotamiento de las direcciones IP. Este problema y cómo está siendo tratado es analizado con nuevas tecnología como lo es Ipv6 ó IP versión 6.

Un hecho a señalar en la división de la dirección IP en dos partes es que esta división a su vez divide en dos partes la responsabilidad de elegir una dirección IP. El número de red es asignado por el InterNIC y el de host por la autoridad que controla la red. Como veremos en la siguiente sección, el número de host puede dividirse aún más: esta división también es controlada por la autoridad propietaria de la red, y ***no*** por el InterNIC.

SUBREDES

Debido al crecimiento explosivo de Internet, el uso de direcciones IP asignadas se volvió demasiado rígido para permitir cambiar con facilidad la configuración de redes locales. Estos cambios podían ser necesarios cuando:

- Se instala una nueva red física.
- El crecimiento del número de hosts requiere dividir la red local en dos o más redes.

Para evitar tener que solicitar direcciones IP adicionales en estos casos, se introdujo el concepto de ***subred***.

El número de host de la dirección IP se subdivide de nuevo en un número de red y uno de host. Esta segunda red se denomina ***subred***. La red principal consiste ahora en un conjunto de subredes y la dirección IP se interpreta como

<número de red < número de subred < número de host

La combinación del número de subred y del host suele denominarse "dirección local" o parte local". La creación de subredes se implementa de forma que es transparente a redes remotas. Un host dentro de una red con subredes es consciente de la existencia de estas, pero un host de una red distinta no lo es; sigue considerando la parte local de la dirección IP como un número de host.

La división de la parte local de la dirección IP en números de subred y de host queda a libre elección del administrador local; cualquier serie de bits de la parte local se puede tomar para la subred requerida. La división se efectúa empleando una ***máscara de subred*** que es un número de 32 bits. Los bits a cero en esta máscara indican posiciones de bits correspondientes al número de host, y los que están a uno, posiciones de bits correspondientes al número de subred. Las posiciones de la máscara pertenecientes al número de red se ponen a uno pero no se usan. Al igual que las direcciones IP, las máscaras de red suelen expresarse en formato decimal.

El tratamiento especial de "todos los bits a cero" y "todos los bits a uno" se aplica a cada una de las tres partes de dirección IP con subredes del mismo modo que a una dirección IP que no las tiene, como las IP especiales. Por ejemplo, una red de clase B con subredes, que tiene un parte local de 16 bits, podría hacer uso de uno de los siguientes esquemas:

- El primer byte es el número de subred, el segundo el de host. Esto proporciona 254(256 menos dos, al estar los valores 0 y 255 reservados) posibles subredes, de 254 hosts cada una. La máscara de subred es 255.255.255.0.
- Los primeros 12 bits se usan para el número de subred, y los 4 últimos para el de host. Esto proporciona 4094 posibles subredes (4096 menos 2), pero sólo 14 host por subred. La máscara de subred es 255.25.255.240. Hay muchas otras posibilidades.

Mientras el administrador es totalmente libre de asignar la parte de subred a la dirección local de cualquier forma legal, el objetivo es asignar un ***número*** de bits al número de subred y el resto a la dirección local. Por tanto, es corriente usar un bloque de bits contiguos al comienzo de la parte local para el número de subred ya que así las direcciones son más legibles (esto es particularmente cierto cuando la subred ocupa 8 o 16 bits). Con este enfoque, cualquiera de las máscaras anteriores es buena, pero no máscaras como 255.255.252.252 o 255.255.255.15.

Ejemplo de subredes

Asumiendo que a la red en cuestión, se le ha asignado el número de red IP de clase B 129.112. se debe implementar múltiples redes físicas en la red. Por tanto se tendrá que

elegir una máscara de subred para la totalidad de la red. Se tiene una dirección local de 16 bits para la red y se debe dividirla correctamente en dos partes. Por el momento, no se preverá tener más de 254 redes físicas, ni más de 254 hosts por red, de tal forma que una máscara de subred aceptable sería 255.255.255.0 (que además tiene la ventaja de ser legible). Esta decisión debe tomarse cuidadosamente, ya que será difícil cambiarla posteriormente. Si el número de redes o de hosts crece por encima de las previsiones hechas, seguramente se presentaran muchos problemas.

Una configuración de subred muestra un ejemplo de implementación con tres subredes.

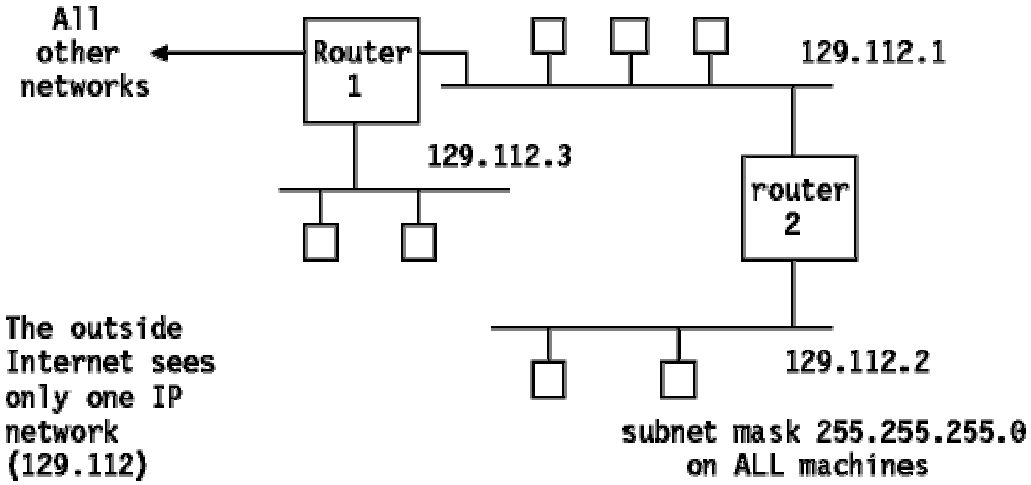
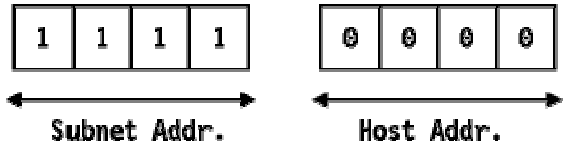


Figura 127. Una configuración de subred

Tres redes físicas forman una sola red IP. Los dos "routers" realizan tareas ligeramente diferentes. El "router" 1 actúa como "router" entre las subredes 1 y 3 así como para toda nuestra red y el resto de Internet. El "router" 2 actúa sólo como "router" entre las redes 1 y 2.

Se Considera ahora una máscara de subred diferente: 255.255.255.240. El cuarto octeto se ha dividido por tanto en dos partes:



La siguiente tabla contiene las posibles subredes que usarían esta máscara:

Hexadecimal value	Subnet number
0000	0
0001	16
0010	32
0011	48
0100	64
0101	80
0110	96
0111	112
1000	128
1001	144
1010	160
1011	176
1100	192
1101	208
1110	224
1111	240

Tabla 26. Valores de subredes para la máscara de subred 255.255.255.240

Para cada uno de estos valores de subred, sólo 14 direcciones (de la 1 a la 14) de hosts están disponibles, ya que sólo la parte derecha del octeto se puede usar y porque las direcciones 0 y 15 tienen un significado especial tal como se describe en la sección de ***Direcciones IP especiales***.

De este modo, el número de subred 9.67.32.16 contendrá a los hosts cuyas direcciones IP estén en el rango de 9.67.32.17 a 9.67.32.30, y el número de subred 9.67.32.32 a los hosts cuyas direcciones IP estén en el rango de 9.67.32.33 a 9.67.32.46, etc.

Direcciones IP especiales

Como se ha señalado anteriormente, cualquier componente de una dirección IP con todos sus bits a 1 o a 0 tiene un significado especial.

Todos los bits a 0

Significa "este": "este" host (direcciones IP con < número de host = 0) o "esta" red (direcciones IP con <número de red=0) y sólo se usa cuando el valor real no se conoce. Esta forma de expresar direcciones se utiliza con direcciones IP fuente, cuando el host trata

de determinar sus direcciones IP por medio de un servidor remoto. El host puede incluir su número de host, si lo conoce, pero no su número de red o subred.

Todos los bits a 1

Significa "todos": "todas" las redes o "todos" los hosts. Por ejemplo, 128.2.255.255 (una dirección de clase B con número de host 255.255) significa "todos los host de la red 128.2". Esta forma de expresar direcciones se emplea en mensajes de broadcast, como se describe más abajo.

Hay otra dirección de especial importancia: el número de red de clase A con todos los bits a 1, 127, se reserva para la ***dirección de loopback***. Todo lo que se envíe a una dirección con 127 como valor del byte de mayor orden, por ejemplo 127.0.0.1, no debe encaminarse a través de la red, sino directamente del controlador de salida al de entrada.

Unicasting, broadcasting

La mayoría de las direcciones IP se refieren a un sólo destinatario: se denomina direcciones de ***unicast***. Sin embargo, como se ha señalado anteriormente, hay dos tipos especiales de direcciones IP que se utilizan para direccionar a múltiples destinatarios: las direcciones de broadcast y de multicast. Cualquier protocolo ***no orientado a conexión*** puede enviar mensajes de broadcast o de multicast, además de los unicast. Un protocolo ***orientado a conexión*** sólo puede usar direcciones de unicast porque la conexión existe entre un par específico de hosts.

Broadcasting

Hay una serie de direcciones que se usan para el broadcast en IP: todas manejan el convenio de que "todos los bits a 1" indica "todos". Las direcciones de broadcast nunca son válidas como direcciones fuente, sólo como direcciones de destino. Los diferentes tipos de broadcast se listan aquí:

Direcciones de broadcast limitado

La dirección 255.255.255.255 (todos los bits a 1 en toda la dirección IP) se usa en redes que soportan broadcast, como por ejemplo redes en anillo, y se refiere a todos los host de la subred. No requiere que el host tenga conocimiento alguno de la configuración IP. Todos los host de la red local reconocerán la dirección, pero los "router" nunca enviarán el mensaje. Esta regla tiene una excepción, llamada ***retransmisión BOOTP***. El protocolo BOOTP emplea el broadcast limitado para permitir a estaciones de trabajo sin disco contactar con un servidor BOOTP. La retransmisión BOOTP es una opción de configuración disponible en algunos "routers". Sin esta posibilidad, haría falta un servidor

BOOTP en cada subred. Sin embargo, no se trata de una simple retransmisión, ya que el "router" también interviene en el desarrollo del protocolo BOOTP.

Direcciones de broadcast dirigidas a red

Si el número de red es un válido, la red no se subdivide en subredes y el número de host referencia todos los hosts de la red especificada, (por ejemplo, 128.2.255.255). Los "router" deberían enviar estos mensajes de broadcast a menos que están configurados para no hacerlo. Este tipo de broadcast se utiliza en solicitudes ARP.

Direcciones de broadcast dirigidas a subred

Si el número de red y el de subred son válidos, y el de host tiene todos sus bits a 1, entonces la dirección referencia a todos los host de la subred especificada. Ya que la subred fuente y la de destino pueden tener distintas máscaras de subred, la fuente debe resolver de algún modo la máscara usada en la subred de destino. El broadcast lo efectúa realmente el "router" de subred que recibe el datagrama.

Direcciones de broadcast dirigidas a todas las subredes

Si el número de red es válido, la red se subdivide en subredes y la parte local de la dirección tiene todos los bits a 1(por ejemplo, 128.2.255.255), y la dirección se refiere a todos los hosts en todas las subredes de la red especificada. En principio, los "router" pueden propagar broadcasts por todas las subredes, aunque no están obligados a hacerlo.

En la práctica, no lo hacen; hay pocas circunstancias en las que un broadcast sea deseable, y puede causar problemas, particularmente si un host se ha configurado incorrectamente sin su máscara de subred. Considerar el derroche de recursos que se produciría si el host 9.180.214.114 en la red local clase A con subredes no fuera consciente de la existencia de esas subredes y usara 9.255.255.255 como dirección de broadcast "local" en vez de 9.180.214.255 y todos los "router" aceptaran la solicitud de enviar mensajes a todos los clientes.

Si los "router" respetan todos los mensajes de broadcast dirigidos a subredes, utilizan un algoritmo llamado Retransmisión Inversa (***"Reverse Path Forwarding")*** para evitar que los mensajes de broadcast se multipliquen descontroladamente.

ANALISIS Y DISEÑO ORIENTADO A OBJETOS

Actualmente, el enfoque orientado a objetos forma parte de la tendencia principal para el desarrollo de software, porque ha demostrado ser válido en la construcción de sistemas en

toda clase de dominios de problemas, abarcando todo el abanico de tamaños y complejidades.
Los métodos orientados a objetos para el análisis de requerimientos de software permiten al analista obtener el modelo de un problema representando clases, objetos, atributos y operaciones como componentes principales de modelización.

Los objetos modelan casi cualquier aspecto identificable del ámbito del problema: entidades externas, cosas, sucesos, papeles, unidades organizativas, lugares y estructuras. Como punto importante, los objetos encapsulan datos y procesos. Las operaciones de procesamiento son parte del objeto y son iniciadas pasando un mensaje al objeto. Una definición de una clase forma la base para la reusabilidad en los niveles de análisis, diseño e implementación.

Las actividades de diseño orientado a objetos están agrupadas en los cuatro componentes principales del sistema final: el componente de problema, el componente de interfaz humana, el componente de manejo de datos y el componente de manejo de tareas.

Toda la documentación del análisis debe llevar directamente hacia la etapa del diseño. En este punto se necesitan pocas herramientas nuevas. El diseño orientado a objetos crea un modelo de mundo real que puede ser realizado en software. Los objetos proporcionan un mecanismo para representar el ámbito de información, mientras que las operaciones describen el procedimiento asociado con el ámbito de información. Los mensajes proporcionan el medio por el que se invocan las operaciones.

El ADOO ha evolucionado como resultado de una nueva clase de lenguaje de programación orientado a programación orientada a objetos. La metodología ADOO consiste en tres pasos que requieren que el diseñador establezca el problema, defina una estrategia informal de resolución y formalice la estrategia, identificando objetos y operaciones, especificando interfaces y procedimientos. El papel del DOO es tomar las clases básicas definidas en el AOO y refinarlos con detalles adicionales de diseño.

La utilización de metodologías orientadas a objetos crea varios interrogantes como: ¿Cuál es la estructura de una buena arquitectura orientada a objetos?, o ¿Qué artefactos debería crear el proyecto?

Visualizar, especificar, construir y documentar sistemas orientados a objetos es el propósito del Lenguaje unificado de Modelado (Unified Modeling Language) UML.

LENGUAJE UNIFICADO DE MODELADO UML

El lenguaje Unificado de Modelado (UML) es un lenguaje para especificar, visualizar, construir y documentar los artefactos de los sistemas de software. Así como para el modelado del negocio y otros sistemas no software.

UML se ha convertido en la notación visual estándar de facto para el modelado orientado a objetos. Comenzó como una iniciativa de Grady Booch y Jim Rumbaugh en 1994 para combinar las notaciones visuales de sus dos populares métodos como los métodos de Booch y OMT (Object Modeling Technique). Más tarde se les unió Ivar Jacobson, el creador del método Objetory, y el grupo empezó a ser conocido como los ***tres amigos.*** Muchos otros contribuyeron a UML, quizás más notablemente Cris Kobryn, que lidera el proceso de refinamiento que todavía continua.

UML fue adoptado en 1997 como estándar por el OMG (Object Management Group, organización que promueve estándares para la industria), y continua siendo refinado en nuevas versiones.

Los objetivos primarios que se persiguen al diseñar UML son:

- Modelar sistemas, desde el concepto hasta los artefactos ejecutables, utilizando técnicas orientadas a objetos.
- Ser independiente de cualquier lenguaje de programación y de cualquier proceso de desarrollo.
- Fomentar el crecimiento de las herramientas OO (Orientadas a Objetos).
- Crear un lenguaje de modelado utilizable tanto por las personas como por las máquinas.

Artefactos de Uml Los artefactos que se utilizan para el desarrollo de anubis- suite de aplicaciones destinadas a la administración de servicios de redes de área local tipo IP bajo plataforma GNU/Linux son:

- **Funciones del Sistema.** Identifican lo que el sistema habrá de hacer. Deben agruparse en grupos lógicos. Los atributos del sistema son cualidades no funcionales, entre ellas la facilidad de uso. Las funciones se clasifican en categorías para establecer prioridades entre ellas; las categorías son:

a. Evidente: debe realizarse, y el usuario debería saber que se ha realizado.

b. Oculta: debe realizarse, aunque no es visible para los usuarios.

c. Superflua: opcionales, su inclusión no repercute significativamente en el costo ni en otras funciones.

- **Casos de Uso.** El caso de uso es un documento narrativo que describe la secuencia de eventos de un actor (agente externo) que utiliza un sistema para completar un proceso.

- **Diagramas de Casos de Uso.** Muestran las distintas operaciones que se esperan de una aplicación o sistema y como se relacionan con su entorno. Los elementos de los diagramas, son:

  - Casos de Uso: Se representa en el diagrama por una elipse, denota un requerimiento solucionado por el sistema. Cada caso de uso es una operación completa desarrollada por los actores y por el sistema en un diálogo. El conjunto de casos de uso representa la totalidad de operaciones desarrolladas por el sistema. Va acompañado de un nombre significativo, cabe destacar que aunque en UML los casos de uso se representan por diagramas, el UP o proceso unificado exige una clara descripción y documentación en texto antes de entrar al dibujo.

- Actor: Es cualquier cosa con comportamiento, incluyendo el propio sistema que se está estudiando (SuD System Under Discusión) cuando solicita los recursos de otros sistemas. Los actores principales y de apoyo aparecerán en los pasos de acción del texto del caso de uso. Los actores no son solamente roles que juegan personas, sino también organizaciones, software y máquinas. Hay tres tipos de actores externos con relación al SuD:

- Actor Principal: Tiene objetivos de usuario que se satisfacen mediante el uso de los servicios del SuD. Por ejemplo un cajero. ¿Por qué se identificá? Para encontrar los objetivos de usuario, los cuales dirigen los casos de uso.

- Actor de apoyo: proporciona un servicio (por ejemplo, información) al SuD. El servicio de autenticación y autorización de usuarios. Normalmente, se trata de un sistema informático, pero podría ser una organización o una persona. ¿Por qué se identifica? Para clarificar las interfaces externas y los protocolos.

- Actor pasivo: está interesado en el comportamiento del caso de uso, pero no es principal ni de apoyo; por ejemplo la administración de la empresa o institución que se beneficia directa o indirectamente del sistema informático. ¿Por qué se identifica? Para asegurar que todos los intereses necesarios se han identificado y satisfecho. Los intereses de los actores pasivos algunas veces son sutiles o es fácil no tenerlos en cuenta, a menos que estos actores sean identificados explícitamente.

- Relaciones. Entre los elementos de un diagrama de casos de uso se pueden presentar tres tipos de relaciones, representadas por líneas dirigidas entre ellos. Estas relaciones son:

- Comunica (communicates). Relación entre un actor y un caso de uso, denota la participación del actor en el caso de uso determinado.

- Usa (uses o include). Relación entre dos casos de uso, denota la inclusión del comportamiento de un escenario en otro.

- Extiende (extends). Relación entre dos casos de uso, denota cuando un caso de uso es una especialización de otro.

- **Diagrama Conceptual.** Explica los conceptos significativos en un dominio del problema; es el artefacto más importante a crear durante el análisis orientado a objetos. Un modelo conceptual es una representación de conceptos en un dominio del problema. Consta de conceptos, asociaciones entre conceptos y atributos de conceptos.

- **Diagrama Secuencial.** Es una representación que muestra, en determinado escenario de un caso de uso, los eventos generados por actores externos, su orden y los eventos internos del sistema. A todos los sistemas se les trata como una caja negra; los diagramas se centran en los eventos que trasciende las fronteras del sistema y que fluyen de los actores a los sistemas. Un evento de un sistema es un hecho externo de entrada que un actor produce en un sistema. El evento da origen a una operación de respuesta por parte del sistema.

- **Caso de Uso Reales.** Un caso real de uso describe el diseño concreto del caso de uso a partir de una tecnología particular de entrada y salida, así como de su implementación global.

- **Diagramas de Interacción**. Explican gráficamente cómo los objetos interactúan a través de mensajes para realizar las tareas. El UML define dos tipos de estos diagramas; ambos sirven para expresar interacciones semejantes de mensaje, estos son: ***diagramas de colaboración*** y ***diagramas de secuencia***.

- **Diagrama de Clases.** Describe gráficamente las especificaciones de las clases de software y de las interfaces en una aplicación. Contiene clases, asociaciones y atributos; interfaces, con sus operaciones y constantes; métodos; información sobre los tipos de los atributos; navegabilidad y dependencias. A diferencia del modelo conceptual, este diagrama contiene las definiciones de las entidades del software en vez de conceptos del mundo real.