ANEXO D
CONFIGURACIÓN SERVIDOR WEB IPv6.

D.1 CONFIGURACIÓN DEL SERVIDOR APACHE SEGURO.

El primer paso para la configuración de un servidor Apache seguro es crear un certificado de autenticidad. Dado que no esta dentro del presupuesto del proyecto solicitar a una empresa internacional una firma digital, para validar este certificado, entonces este será autofirmado.

Con permisos de administrador se ejecuta el comando especificado a continuación, para crear una llave privada:

openssl genrsa –des3 –out nombredelallave.key 1024

Entonces se pedirá al usuario una frase secreta como se muestra en la figura D1

```
[root@zeus ~]# openssl req -new -out certificado.crt
Generating a 1024 bit RSA private key
.....................................................++++++
.....................................................++++++
writing new private key to 'privkey.pem'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
```

Figura. D1. Contraseña requerida.

Ahora se debe especificar información adicional que será enviada en el certificado, figura D2.

```
Country Name (2 letter code) [GB]:Colombia
string is too long, it needs to be less than  2 bytes long
Country Name (2 letter code) [GB]:Co
State or Province Name (full name) [Berkshire]:Cauca
Locality Name (eg, city) [Newbury]:Popayan
Organization Name (eg, company) [My Company Ltd]:Universidad del Cauca
Organizational Unit Name (eg, section) []:Facultad de ingenieria Electronica
Common Name (eg, your name or your server's hostname) []:zeus
Email Address []:servicios@ipv6.unicauca.edu.co
```

Figura D2. Información adicional requerida.

Ahora para crear un certificado autofirmado se ejecuta:

Openssl req –new –x509 –days 365 –key nombredelallave.key –out nombredelcertificado.crt

El usuario debe ingresar una frase secreta de igual forma como se ilustra en la figura D1.

En el caso de contar con la posibilidad de obtener una firma digital de una empresa certificadora, se debería enviar un archivo con extensión .csr (Certificate Signing Request), este archivo se obtiene a partir de la ejecución del comando:

Openssl req –new –key nombredelallave.key –out nombredelcertificado.csr

Continuando con la configuración del servidor Web, una vez el anterior proceso se ha completado exitosamente, es necesario configurar los archivos /etc/httpd/conf/httpd.conf y /etc/httpd/conf.d/ssl.conf, de la siguiente manera:

Primero en httpd.conf, en la sección 1 de este archivo (*Global Environment)*, se debe asegurar la presencia de la línea **Include conf.d/*.conf**.

El siguiente paso se registra en la sección 2 (*'Main' server configuration)*, cambiar el nombre del servidor que viene por defecto (localhost), por el adecuado para la red, esto se realiza en la línea **ServerName**, en este caso:

ServerName www.ipv6.unicauca.edu.co:80

Además, en la línea **DocumentRoot**, se debe establecer el directorio sobre el cual las aplicaciones que usaran http estarán ubicadas, en este caso:

DocumentRoot "/var/www/paginaweb/"

Por otro lado en el archivo *ssl.conf* se requiere una configuración especial para proteger las aplicaciones Webmail y Autoconfiguración IPv6 haciendo uso de https, y así garantizar la privacidad de los datos enviados al servidor por parte de los usuarios. Estas dos aplicaciones exigen el uso de Hosts Virtuales, ya que de esta manera se podrán separar los directorios raíz donde estarán alojadas dichas aplicaciones, y así cada una será tratada como un sitio diferente. De esta forma se logra un mayor nivel de organización y flexibilidad en el sistema, dado que los *host* virtuales permiten que apache responda a solicitudes de diferentes dominios.

El primer paso a seguir es aumentar la directiva *NameVirtualHost* al citado archivo de configuración, en este caso:

NameVirtualHost [2001:448:1024:1::10]:443

Luego al final del archivo se pueden agregar los dominios virtuales, los cuales estarán delimitados por las etiquetas:

<VirtualHost Direccion IP: 443>
</VirtualHost>

Dentro de estas etiquetas se encuentra la configuración propia a cada Host virtual. En el caso particular del sistema la siguiente configuración es usada:

<VirtualHost [2001:448:1024:1::10]:443>
DocumentRoot "/var/www/dibblerweb/"
ServerName autoconf.ipv6.unicauca.edu.co:443
ErrorLog logs/ssl_error_log
TransferLog logs/ssl_access_log

SSLCertificateFile /etc/pki/tls/certs/server2.crt
SSLCertificateKeyFile /etc/pki/tls/private/server1.key

```
</VirtualHost>


<VirtualHost [2001:448:1024:1::10]:443>
DocumentRoot "/usr/share/squirrelmail/"
ServerName www.ipv6.unicauca.edu.co/src/:443
ErrorLog logs/ssl_error_log
TransferLog logs/ssl_access_log

SSLCertificateFile /etc/pki/tls/certs/server2.crt
SSLCertificateKeyFile /etc/pki/tls/private/server1.key
</VirtualHost>
```

Nótese que las directivas *SSLCertificateFile* y *SSLCertificateKeyFile* señalan la ruta donde se encuentra el certificado de autenticidad y la llave con la que es autofirmado respectivamente.

Por último es imperativo que algunos archivos usados en la aplicación Interfaz de autoconfiguración, se oculten por razones de seguridad, para ello se utilizan las directivas <Directory Directory-path > y </Directory> las cuales permitan englobar un grupo de instrucciones que se aplicarán solamente al directorio especificado y a sus subdirectorios. *Directory-path* puede ser tanto la ruta completa a un directorio, como una cadena de caracteres comodín que use las reglas de equivalencia de los *shells* de Unix.

En el caso del archivo de configuración *ssl.conf*, esta es la configuración presentada:

```
 <Directory "/var/www/dibblerweb/lib">
    Order deny,allow
    Deny from all
</Directory>

<Directory "/var/www/dibblerweb/config">
    Order deny,allow
    Deny from all
</Directory>
```

De esta manera se deniega el acceso a los clientes que deseen ingresar a estos directorios.

Es de resaltar que para que todo el sistema funcione correctamente es fundamental una correcta configuración del Sistema de Nombres de Dominio, para más información al respecto consúltese el ANEXO A

D.2 INSTALACIÓN Y CONFIGURACIÓN DE MAMBO

D.2.1 Instalación MAMBO.

El primer paso es descargar este software, dada su popularidad este paso no supone ningún problema, ya que puede ser obtenido desde una infinidad de sitios Web y FTP en toda la red, el sitio oficial de descarga es http://mamboxchange.com Una vez descargado

debe descomprimirse y ubicarse en el directorio raíz de Apache, generalmente */var/www/* o en el directorio que se elija para su instalación.

En este punto debemos preparar el sistema para la posterior instalación, para ello se requiere crear una base de datos en Mysql, los pasos a seguir para lograrlo son los siguientes:

Primero se debe establecer una contraseña para el administrador de Mysql, si no se ha creado previamente, ejecutando el comando:

```
$ mysql -u root
set password for root@localhost = password('hack_me');
flush privileges;
quit;
```

Luego se debe crear una base de datos, mediante:
```
# mysqladmin create nombre_database -p
```

Ahora se asigna un usuario del sistema como administrador de esta base de datos. Ingresamos el comando
```
#myql -p
```

y luego

```
GRANT ALL ON nombre_database.* TO nombre_admin@localhost IDENTIFIED BY 'Password_admin';
FLUSH PRIVILEGES;
```

Ahora bien se debe crear un archivo dentro del directorio de instalación de mambo llamado *configuration.php* con permisos de escritura. Además es necesario tomar precauciones que todos los directorios que posee Mambo tienen permisos de escritura también.

Una vez terminado este proceso, empezamos la instalación en si de Mambo. Accedemos al sitio donde fue depositado todo el código PHP de este software desde un cliente Web, en este caso www.ipv6.unicauca.edu.co, y este iniciará la instalación automáticamente:

En un principio Mambo mostrará la disponibilidad de los componentes necesarios (php, mysql) figura D3, además de la configuración de php.ini, figura D4, así como también advertirá si todos los directorios necesarios tienen permisos de escritura, figura D5.

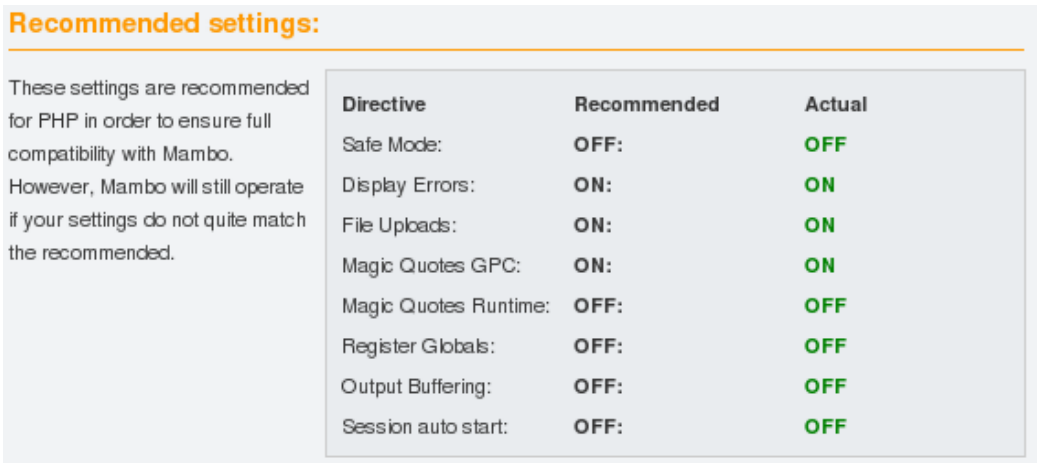
Pre-installation check for:

Mambo 4.6.0 Stable [Graff] 18-Sept-2006 03:00 GMT

If any of these items are highlighted in red then please take actions to correct them. Failure to do so could lead to your Mambo installation not functioning correctly.

PHP version >= 4.3.0	**Yes**
- zlib compression support	**Available**
- XML support	**Available**
- MySQL support	**Available**
configuration.php	**Writeable**
Session save path	**/var/lib/php/session, Writeable**

Figura D3. Soporte a Mambo.



Recommended settings:

These settings are recommended for PHP in order to ensure full compatibility with Mambo. However, Mambo will still operate if your settings do not quite match the recommended.

Directive	Recommended	Actual
Safe Mode:	**OFF:**	**OFF**
Display Errors:	**ON:**	**ON**
File Uploads:	**ON:**	**ON**
Magic Quotes GPC:	**ON:**	**ON**
Magic Quotes Runtime:	**OFF:**	**OFF**
Register Globals:	**OFF:**	**OFF**
Output Buffering:	**OFF:**	**OFF**
Session auto start:	**OFF:**	**OFF**

Figura D4. php.ini

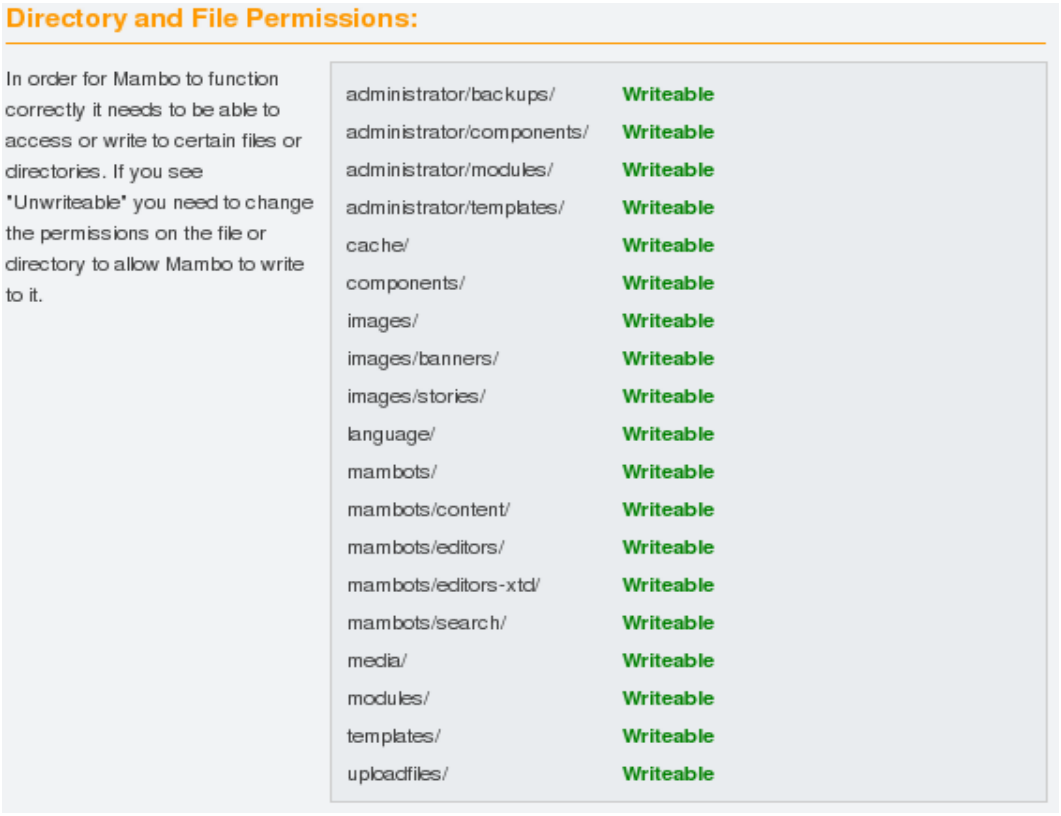


Figura D5. Permisos actuales en los directorios de Mambo

Luego se muestra la licencia del producto. En este punto se debe marcar la casilla yo entiendo que este software es realizado bajo licencia GNU/GPL.

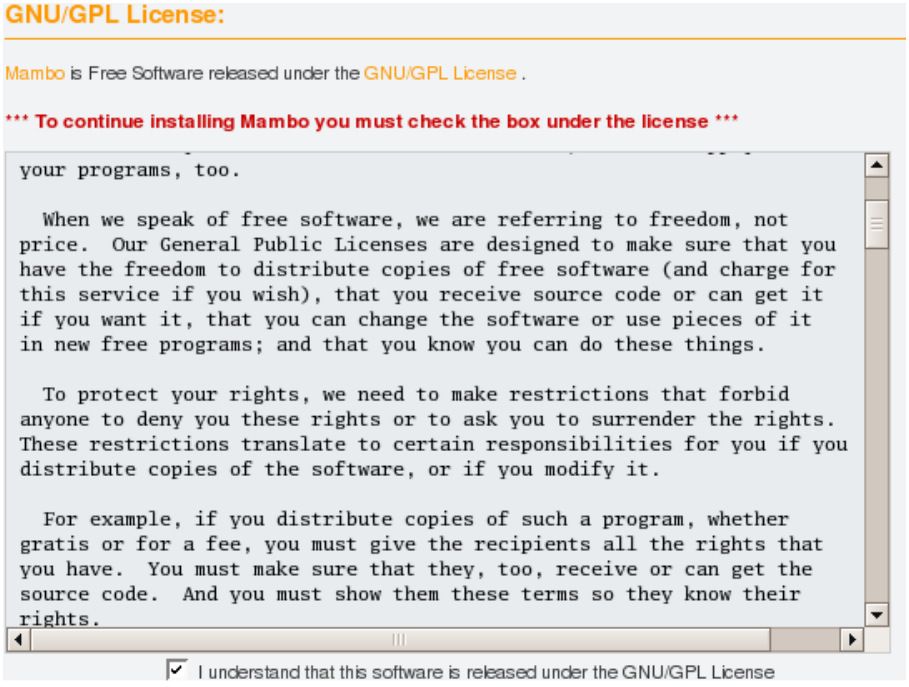


Figura D6. Licencia del producto.

Ahora se debe llenar el formulario correspondiente a la ubicación, *login* y *password* de la *database*, estos datos deben estar en coincidencia con lo configurado anteriormente en el momento de la construcción de la base de datos, observar figura D7.

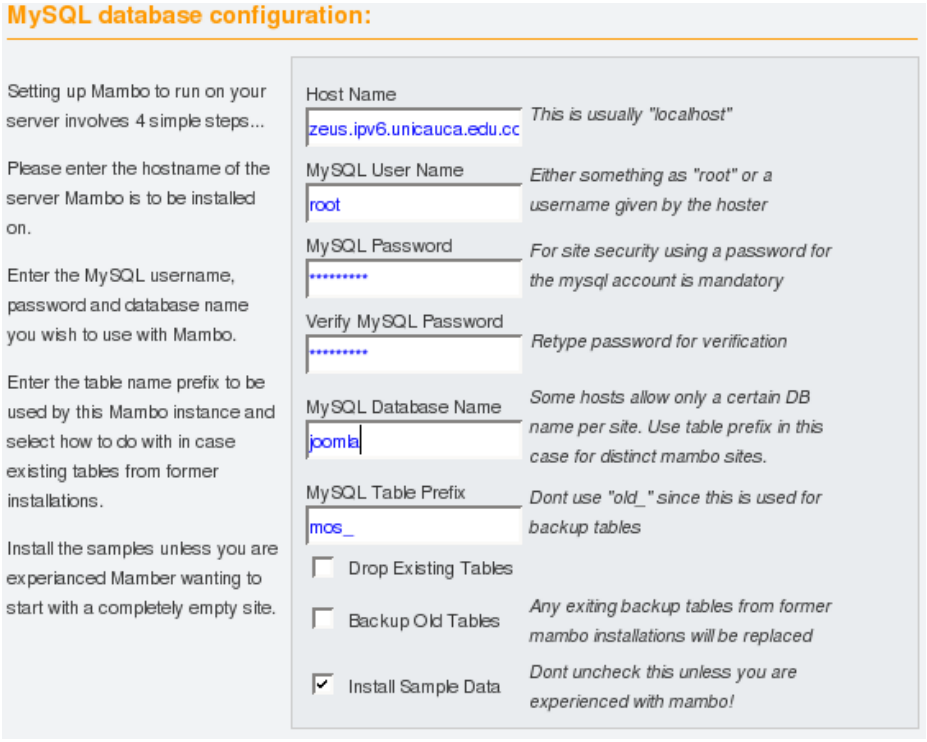


Figura D7. Configuración Base de Datos.

Ahora se introduce un nombre para el sitio, figura D8

Figura D8 Introducir un nombre.

Por último se debe confirmar el *path* del directorio raíz y el nombre para la página.

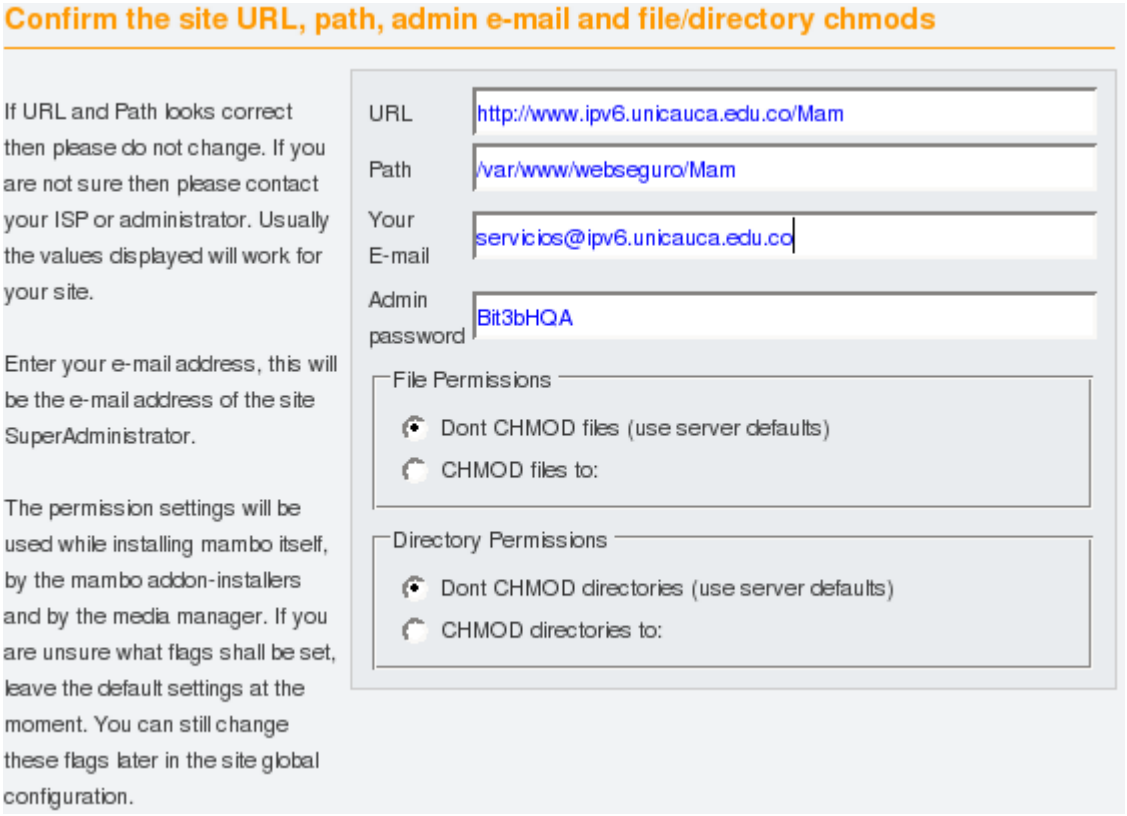


Figura D9. Confirmación de la instalación.

Antes de arrancar el servicio se debe borrar la carpeta *INSTALL* ubicada dentro del directorio de instalación, en esta imagen (figura D10) se entrega el login y password por defecto para hacer uso de la interfaz de administrador.

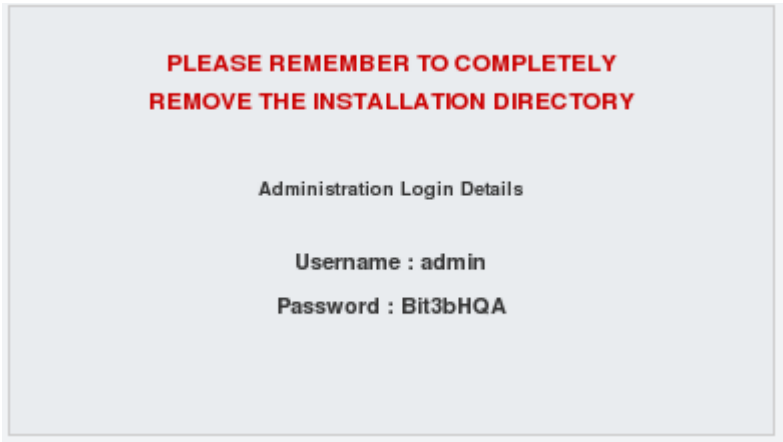


Figura D10. Pantalla final proceso de instalación.

D.2.2 MANUAL DE USUARIO ADMINISTRADOR MAMBO.

Para ingresar en la interfaz del administrador se debe hacer *click* sobre el enlace ubicado en el menú izquierdo de la página www.ipv6.unicauca.edu.co.

De esta manera se logra ingresar en el panel principal de la aplicación, figura D11:

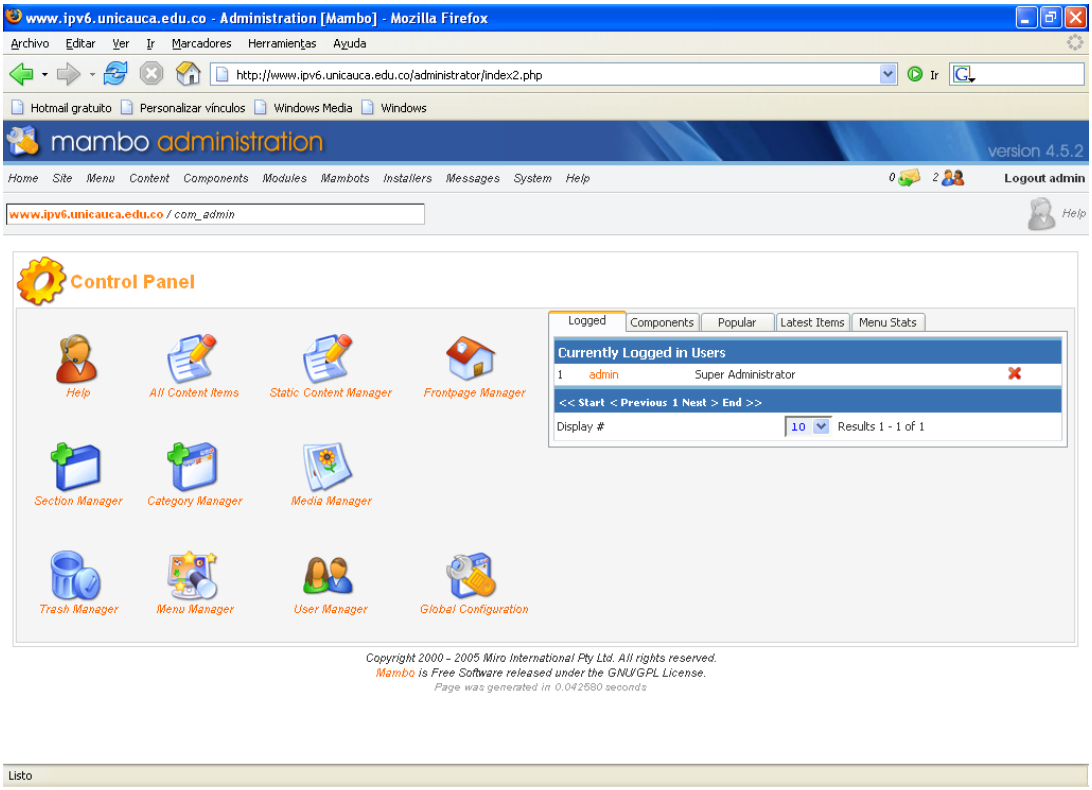


Figura D11. Panel principal de control.

D.2.2.1 Instalación de Interfaces.

Primero se debe ingresar al menú de instalaciones haciendo *click* sobre la pestaña instalar *Templates*, como se observa en la figura D12.

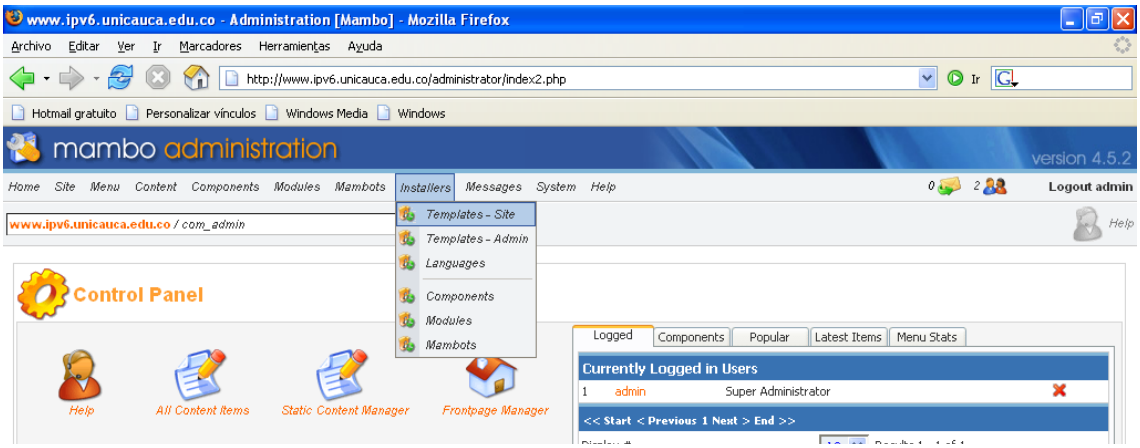


Figura D12. Instalación interfaces parte 1.

Luego desde la interfaz mostrada en la figura D13. Se deben montar los archivos e instalarlos; los *templates* o interfaces para el portal deben estar compresos en formato ZIP.

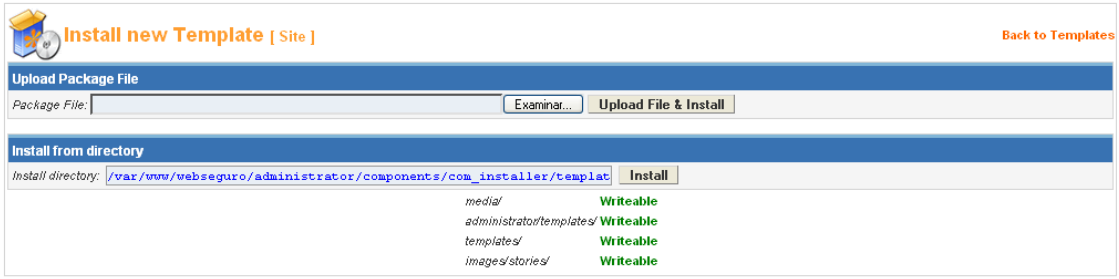


Figura D13. Instalación interfaces parte 2.

Luego de realizar la instalación, la siguiente etapa es seleccionar la nueva interfaz en el administrador de *Templates*, el cual esta ubicado en el submenú: Site>Template Manager>Site templates. Figura D14.

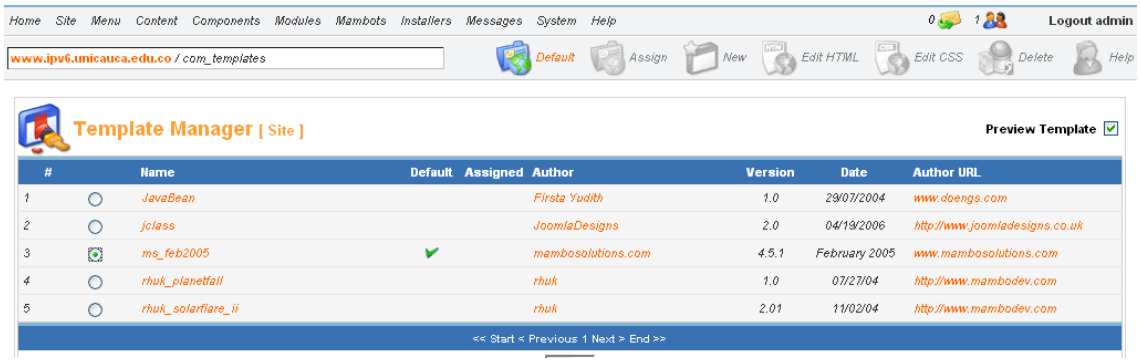


Figura D14. Instalación interfaces parte 3.

D.2.2.2 Administración de contenidos.

Para insertar, borrar o editar un contenido publicado en el portal primero se debe acceder a la interfaz especializada haciendo doble *click* sobre la sección en la cual se desea

trabajar, por ejemplo en la figura D15, se observa como se ingresa a trabajar sobre la sección noticias.

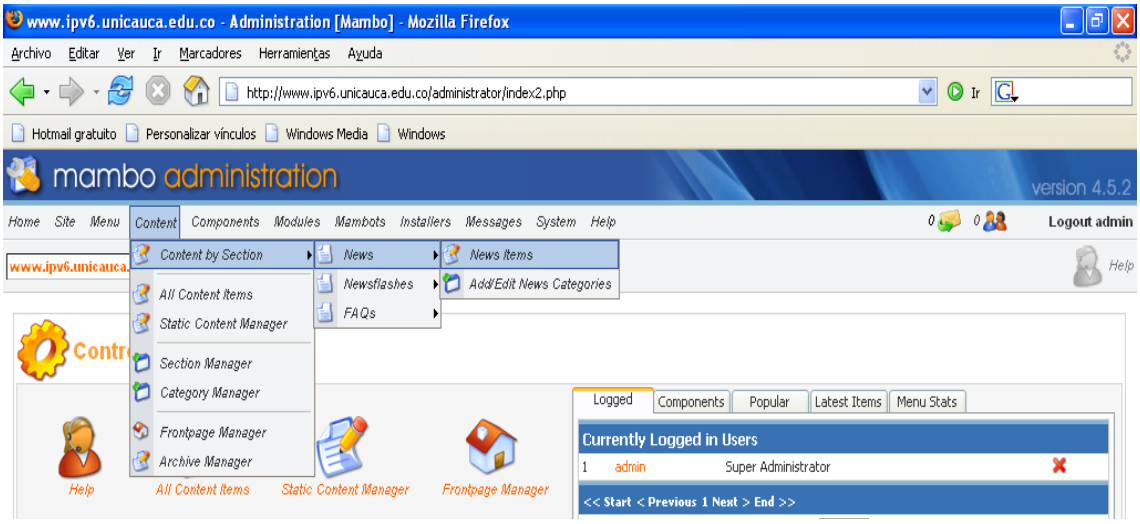


Figura D15. Ingreso a la sección news.

Dependiendo de lo que se desea, se debe hacer uso de los iconos de la interfaz mostrados en la figura D16.

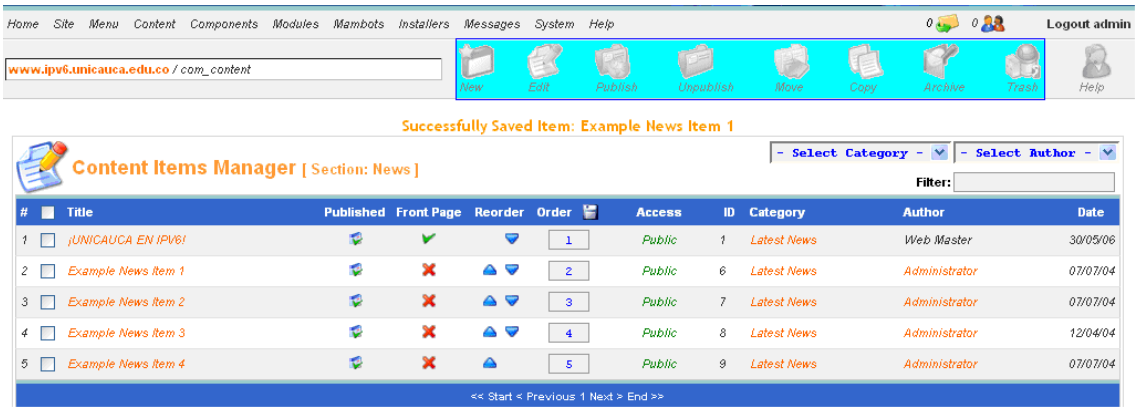


Figura D16. Iconos usados en la edición de contenidos.

Si se desea borrar una noticia basta con señalarla y luego pulsar el icono Trash.

Para publicar una nueva noticia se hace *click* sobre el icono *New*, entonces aparecerá una interfaz con todas la herramientas necesarias para la realización del contenido.

De la misma manera si se desea editar un contenido en particular primero se lo debe señalar, y luego hacer click sobre el icono Edit.

D.3 PRUEBAS REALIZADAS.

Las pruebas de accesibilidad realizadas fueron:

1. Prueba de acceso interno IPv6.

2. Prueba de acceso externo IPv4.
3. Prueba de acceso externo IPv6.

Prueba 1. Desde un host de la red interna dotado con una dirección IPv6, se intenta acceder al portal www.ipv6.unicauca.edu.co, el cliente accederá con el protocolo IPv6, aunque cuente con las dos pilas, por que el primer intento se realizará siempre con la respuesta de un registro AAAA. Figura D17:

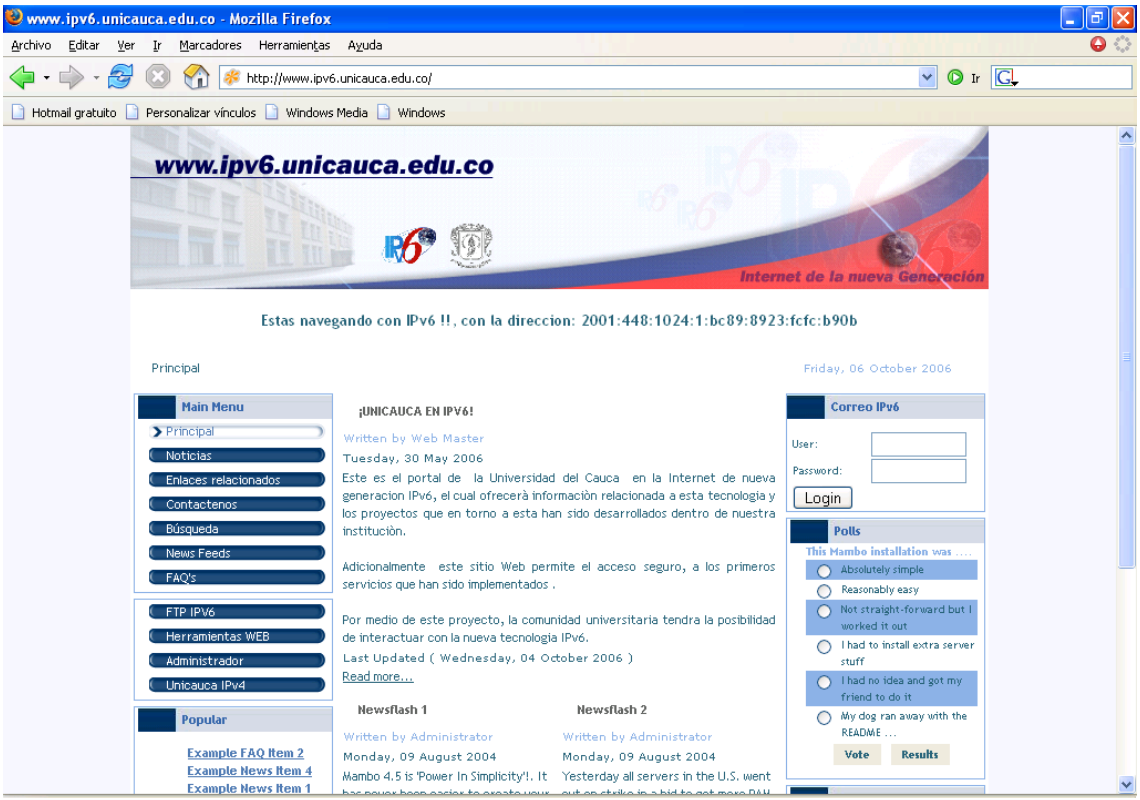


Figura D17. Navegación Interna IPv6.

Prueba 2. Un host en la Internet intentará acceder al portal www.ipv6.unicauca.edu.co, el cliente solo tiene la pila IPv4, por tanto el *script* encargado de obtener la dirección IP lo identificará de este modo, figura D18.

Figura D18. Navegación externa IPv4.

Prueba 3. En la figura D19, se aprecia un nodo con soporte IPv6 que ingresa al portal www.ipv6.unicauca.edu.co.

Figura D19. Navegación externa IPv6.

Desde un sitio IPv6 en México se realizaron pruebas de conectividad con el Servidor DNS zeus.ipv6.unicauca.edu.co, los resultados se ilustran en la figura D20.

```
C:\RD@R!O>tracert6 www.ipv6.unicauca.edu.co

Traza a la dirección www.ipv6.unicauca.edu.co [2001:448:1024:1::10]
desde 2002:c877:3073::c877:3073 sobre un máximo de 30 saltos:

  1    116 ms  109 ms  125 ms  2002:c058:6301::c058:6301
  2    124 ms  109 ms  109 ms  iad0-b1-ge0.hotnic.net [2001:4810:0:100::2]
  3    109 ms  125 ms  125 ms  equi6ix-ash.ipv6.us.occaid.net [2001:504:0:2:
0:3:71:1]
  4    140 ms  140 ms  140 ms  2.ge-0-0.cr1.ord1.us.occaid.net [2001:4830:ff
:f151::1]
  5    156 ms  156 ms  156 ms  57.fe0-0.cr1.mci1.us.occaid.net [2001:4830:ff
:1753::1]
  6    187 ms  187 ms  187 ms  6.fe-0-0.cr1.sfo2.us.occaid.net [2001:4830:ff
:1750::2]
  7    218 ms  218 ms  218 ms  2001:448::2d0:58ff:fef3:6d41
  8    406 ms  406 ms  375 ms  2001:448:1024:1::10

Traza completa.

C:\RD@R!O>ping6 www.ipv6.unicauca.edu.co

Haciendo ping www.ipv6.unicauca.edu.co [2001:448:1024:1::10]
de 2002:c877:3073::c877:3073 con 32 bytes de datos:

Respuesta desde 2001:448:1024:1::10: bytes=32 tiempo=373ms
Respuesta desde 2001:448:1024:1::10: bytes=32 tiempo=375ms
Respuesta desde 2001:448:1024:1::10: bytes=32 tiempo=390ms
Respuesta desde 2001:448:1024:1::10: bytes=32 tiempo=437ms

Estadísticas de ping para 2001:448:1024:1::10:
   Paquetes: enviados = 4, recibidos = 4, perdidos = 0 (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
   Mínimo = 373ms, Máximo = 437ms, Media = 393ms
```

Figura D20. Trazado de ruta y Ping6 desde una red externa IPv6.