

Configuración de Servidores Web Apache Tomcat de forma segura



Sistemas Operacionales 2019 - II.

Ángel Fabian Gómez Estupiñán - 2130535.

Esteban Andrés Niño Méndez – 2142608.

Javier Camilo Rueda Serrano – 2141380.

Juan Felipe Silva Garcés – 2141362.

#LaUISqueQueremos





¿Qué es un Servidor?

Es una aplicación que está en constante ejecución.

Atiende las peticiones de un cliente (en forma de otro programa) y devuelve una respuesta concordante.





¿Qué es una Página Web?



Google Search

I'm Feeling Lucky

Es un documento capaz de contener texto, sonido, vídeo, programas, enlaces e imágenes adaptada para la World Wide Web (WWW) y que puede ser accedida mediante un navegador web.



¿Qué es un Servlet?

Es una clase en el lenguaje de programación Java, utilizada para ampliar las capacidades de un servidor. Estos son utilizados comúnmente para extender las aplicaciones alojadas por servidores web





Servidor HTTP Apache



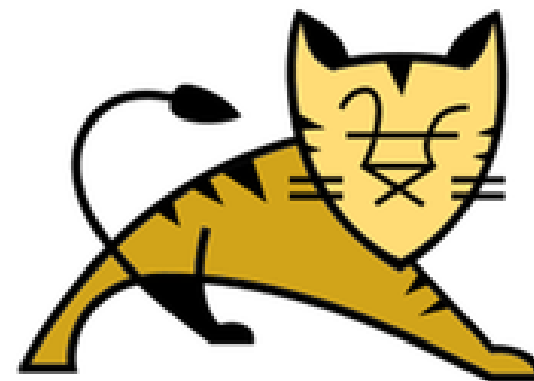
Es un servidor web HTTP de código abierto, para plataformas Unix (BSD, GNU/Linux, etc.), Microsoft Windows, Macintosh y otras.



Apache Tomcat

Funciona como un contenedor de servlets desarrollado bajo el proyecto Jakarta en la Apache Software Foundation.

Implementa las especificaciones de los servlets y de JavaServer Pages (JSP) de Oracle Corporation.



Apache Tomcat





Instalación Servidor Apache

Actualizamos las librerías de el S.O. y luego instalamos los servicios Apache.

```
angel@angel-X456UF ~ $ sudo apt-get update
[sudo] password for angel:
Obj:1 http://archive.canonical.com/ubuntu xenial InRelease
Obj:2 http://archive.ubuntu.com/ubuntu xenial InRelease
Des:3 http://security.ubuntu.com/ubuntu xenial-security InRelease [109 kB]
Ign:4 http://packages.linuxmint.com sylvia InRelease
Des:5 http://archive.ubuntu.com/ubuntu xenial-updates InRelease [109 kB]
Obj:6 http://packages.linuxmint.com sylvia Release
Des:8 http://archive.ubuntu.com/ubuntu xenial-backports InRelease [107 kB]
Descargados 325 kB en 2s (156 kB/s)
Leyendo lista de paquetes... Hecho
angel@angel-X456UF ~ $ sudo apt-get install apache2
```



Esta es la versión de Apache que tenemos instalada.

```
angel@angel-X456UF ~ $ sudo apachectl -v
Server version: Apache/2.4.18 (Ubuntu)
Server built:   2019-10-08T13:31:25
angel@angel-X456UF ~ $
```

Para comprobar que Apache se encuentre correctamente instalado buscamos la dirección IP anexa a nuestro pc y la ingresamos como URL en un navegador web.

```
angel@angel-X456UF ~ $ hostname -i
127.0.1.1
angel@angel-X456UF ~ $
```




Apache2 Ubuntu Default Page: It works! X +

127.0.0.1



Apache2 Ubuntu Default Page

ubuntu

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in `/usr/share/doc/apache2/README.Debian.gz`**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|   |-- ports.conf
|-- mods-enabled
|   |-- *.load
|   |-- *.conf
|-- conf-enabled
|   |-- *.conf
|-- sites-enabled
|   |-- *.conf
```



Configuración Servidor Apache

Habilitaremos los protocolos HTTPS y SSL en nuestro servidor y luego lo reiniciaremos .

```
angel@angel-X456UF /etc/apache2 $ sudo a2enmod ssl
[sudo] password for angel:
Considering dependency setenvif for ssl:
Module setenvif already enabled
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Enabling module socache_shmcb.
Enabling module ssl.
See /usr/share/doc/apache2/README.Debian.gz on how to configure SSL and create s
elf-signed certificates.
To activate the new configuration, you need to run:
    service apache2 restart
angel@angel-X456UF /etc/apache2 $ service apache2 restart
angel@angel-X456UF /etc/apache2 $
```



Activado el módulo de SSL en nuestro servidor, generaremos un cifrado de tipo RSA para los mensajes que se vayan a transmitir.

```
angel@angel-X456UF /etc/apache2 $ sudo openssl genrsa -des3 -out server.key 2048
[sudo] password for angel:
Generating RSA private key, 2048 bit long modulus
.....+++
....+++
e is 65537 (0x10001)
Enter pass phrase for server.key:
Verifying - Enter pass phrase for server.key:
```

*En nuestro caso usamos como pass phrase para el servidor la palabra “**angel**”, la necesitaremos en nuestros casos posteriores.*





Activamos el certificado CSR (Certificate Signing Request), contiene información incluida en el certificado SSL (nombre, empresa, dirección, etc...)

```
angel@angel-X456UF /etc/apache2 $ sudo openssl req -new -key server.key -out server.csr
Enter pass phrase for server.key:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:CO
State or Province Name (full name) [Some-State]:Santander
Locality Name (eg, city) []:Bucaramanga
Organization Name (eg, company) [Internet Widgits Pty Ltd]:UIS
Organizational Unit Name (eg, section) []:Ingenieria de Sistemas
Common Name (e.g. server FQDN or YOUR name) []:Servidor_angel
Email Address []:ango_1415@hotmail.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:1234
An optional company name []:UIIS
```



Establecemos la duración del certificado SSL, podremos una duración de 365 días.

```
angel@angel-X456UF /etc/apache2 $ sudo openssl x509 -req -days 365 -in server.csr -signkey server.key -out server.crt.  
Signature ok  
subject=/C=CO/ST=Santander/L=Bucaramanga/O=UIS/OU=Ingenieria de Sistemas/CN=Servidor_angel/emailAddress=ango_1415@hotmail.com  
Getting Private key  
Enter pass phrase for server.key:  
angel@angel-X456UF /etc/apache2 $
```

*Haremos un respaldo de los siguientes archivos **server.key** y **server.crt** , corresponden al certificado CSR y la llave del servidor. Copiaremos estos archivos en los directorios “**/etc/ssl/private**” y “**/etc/ssl/certs**” .*

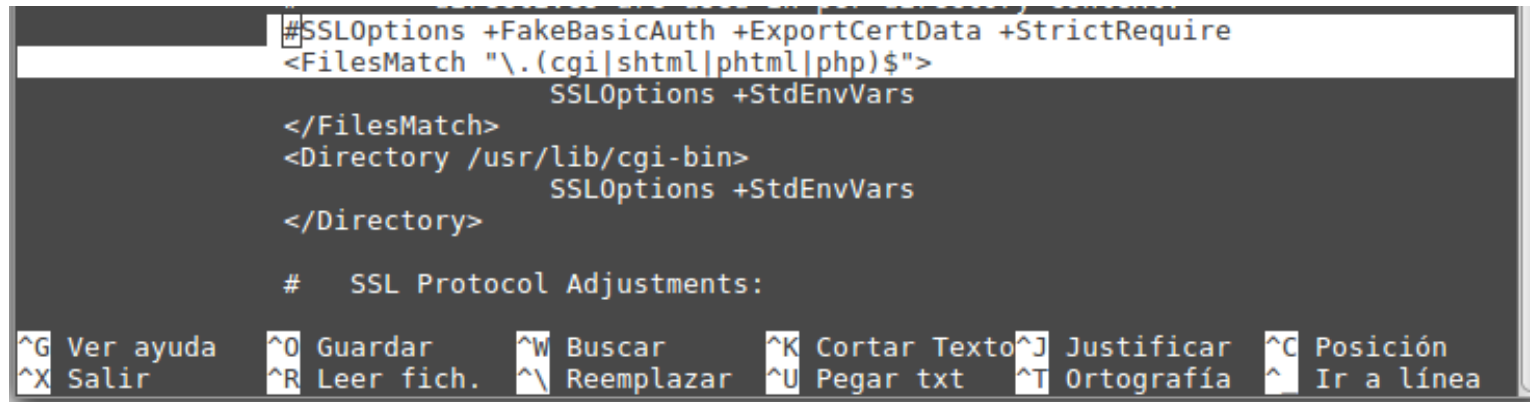
```
angel@angel-X456UF /etc/apache2 $ sudo cp server.key /etc/ssl/private  
angel@angel-X456UF /etc/apache2 $ sudo cp server.crt. /etc/ssl/certs  
angel@angel-X456UF /etc/apache2 $
```



*Editaremos el archivo **default-ssl.conf** que se encuentra en el directorio **sites-available** dentro de **apache2**.*

```
angel@angel-X456UF /etc/apache2 $ cd sites-available
angel@angel-X456UF /etc/apache2/sites-available $ sudo nano default-ssl.conf
```

*Ahora buscaremos la línea de texto que contenga la palabra “**SSLOPTIONS**” y eliminaremos el “**#**” al principio de la línea.*



```
#SSLOptions +FakeBasicAuth +ExportCertData +StrictRequire
<FilesMatch "\.(cgi|shtml|phtml|php)$">
    SSLOptions +StdEnvVars
</FilesMatch>
<Directory /usr/lib/cgi-bin>
    SSLOptions +StdEnvVars
</Directory>

#  SSL Protocol Adjustments:
```

^G Ver ayuda ^O Guardar ^W Buscar ^K Cortar Texto ^J Justificar ^C Posición
^X Salir ^R Leer fich. ^\ Reemplazar ^U Pegar txt ^T Ortografía ^_ Ir a línea



Universidad
Industrial de
Santander

Activamos las configuraciones por default para SSL.

```
angel@angel-X456UF ~ $ sudo a2ensite default-ssl
Site default-ssl already enabled
angel@angel-X456UF ~ $ sudo a2ensite default-ssl.conf
Site default-ssl already enabled
angel@angel-X456UF ~ $
```

Recargamos nuevamente el servidor Apache.

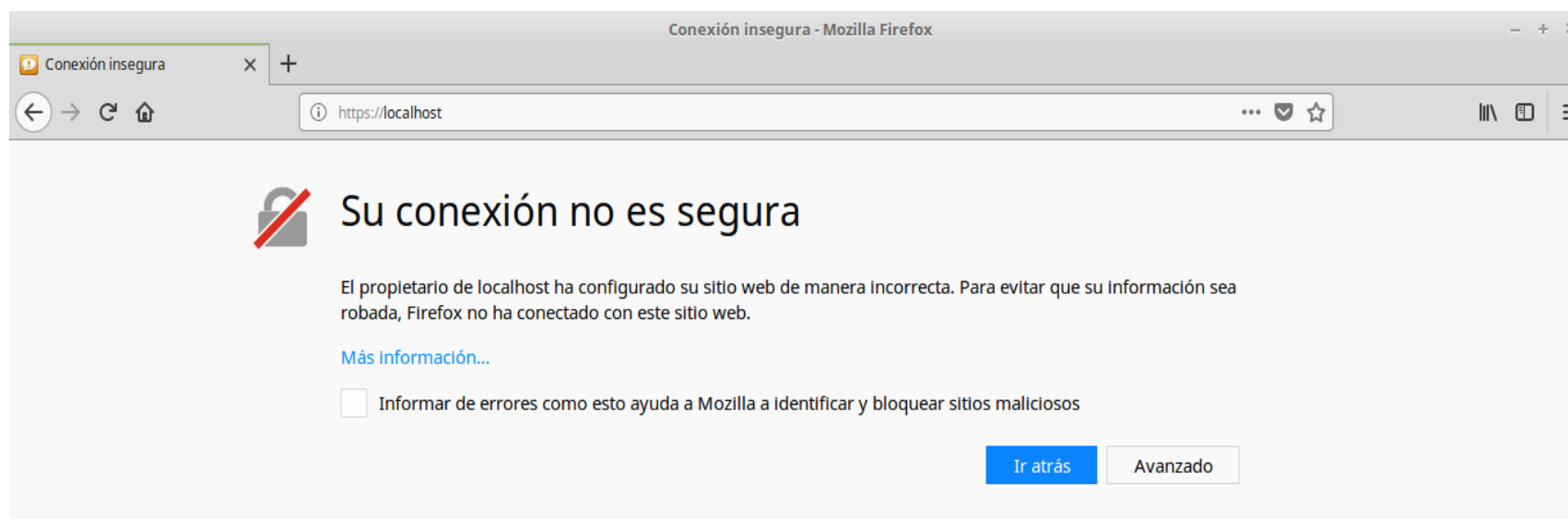
```
angel@angel-X456UF ~ $ sudo service apache2 reload
angel@angel-X456UF ~ $
```

Somos **el mejor** escenario
de creación e innovación.

www.uis.edu.co



Probamos la conexión actual de nuestro localhost, para ver si ya tenemos acceso al mismo





Instalación Tomcat

Java comenzaremos con la instalación del JDK (Java Development Kit).

```
angel@angel-X456UF /etc/apache2 $ sudo apt-get install default-jdk
[sudo] password for angel:
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
  ca-certificates-java default-jdk-headless default-jre default-jre-headless
  openjdk-8-jdk openjdk-8-jdk-headless openjdk-8-jre openjdk-8-jre-headless
```

creación de un usuario y grupo adicional en el directorio “/opt/tomcat” para su correcto funcionamiento.

```
angel@angel-X456UF /etc/apache2 $ sudo useradd -m -U -d /opt/tomcat -s /bin/false tomcat
angel@angel-X456UF /etc/apache2 $
```



Instalamos unzip y wget, herramientas para descargar e instalar Tomcat.

```
angel@angel-X456UF /etc/apache2 $ sudo apt install unzip wget
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
```

*Descargamos **apache-tomcat-9.0.31.zip** en la carpeta **/temp**.*

<https://downloads.apache.org/tomcat/tomcat-9/v9.0.31/bin/apache-tomcat-9.0.31.zip>

```
angel@angel-X456UF /tmp $ wget https://downloads.apache.org/tomcat/tomcat-9/v9.0.31/bin/apache-tomcat-9.0.31.zip
```

*Descomprimimos **apache-tomcat-9.0.31.zip** en la carpeta **/temp**.*

```
angel@angel-X456UF /tmp $ unzip apache-tomcat-9.0.31.zip
```



*Movemos el directorio **apache-tomcat-9.0.31** a **/opt/tomcat***

```
angel@angel-X456UF ~ $ sudo mv apache-tomcat-9.0.31 /opt/tomcat/
```

*Iremos al directorio **/etc/systemd/system** y con el editor **nano** creamos el archivo **tomcat.service**.*

```
angel@angel-X456UF /etc/systemd/system $ sudo nano tomcat.service
```



Dentro del archivo creado colocamos los siguientes valores de configuración para Tomcat.

[Unit]

Description=Tomcat 9 servlet container

After=network.target

[Service]

Type=forking

User=tomcat

Group=tomcat



Universidad
Industrial de
Santander

Somos **el mejor** escenario
de creación e innovación.

www.uis.edu.co





Environment="JAVA_HOME=/usr/lib/jvm/default-java"

Environment="JAVA_OPTS=-Djava.security.egd=file:///dev/urandom"

Environment="CATALINA_BASE=/opt/tomcat/apache-tomcat-9-0-31"

Environment="CATALINA_HOME=/opt/tomcat/apache-tomcat-9-0-31"

Environment="CATALINA_PID=/opt/tomcat/latest/temp/tomcat.pid"

Environment="CATALINA_OPTS=-Xms512M -Xmx1024M -server -XX:+UseParallelGC"

ExecStart=/opt/tomcat/apache-tomcat-9-0-31/bin/startup.sh

ExecStop=/opt/tomcat/apache-tomcat-9-0-31/bin/shutdown.sh

[Install]

WantedBy=multi-user.target



Universidad
Industrial de
Santander



Somos **el mejor** escenario
de creación e innovación.

www.uis.edu.co



Comprobamos el estado del servicio, si está activo o no

```
angel@angel-X456UF /etc/systemd/system $ sudo systemctl daemon-reload
angel@angel-X456UF /etc/systemd/system $ sudo systemctl start tomcat
angel@angel-X456UF /etc/systemd/system $ sudo systemctl status tomcat.service
● tomcat.service - Tomcat 9 servlet container
   Loaded: loaded (/etc/systemd/system/tomcat.service; disabled; vendor preset
   Active: active (running) since jue 2020-03-12 21:39:58 COT; 11min ago
   Main PID: 4327 (java)
   CGroup: /system.slice/tomcat.service
           └─4327 /usr/lib/jvm/default-java/bin/java -Djava.util.logging.confi

mar 12 21:39:58 angel-X456UF systemd[1]: Starting Tomcat 9 servlet container..
mar 12 21:39:58 angel-X456UF systemd[1]: Started Tomcat 9 servlet container.
mar 12 21:51:50 angel-X456UF systemd[1]: Started Tomcat 9 servlet container.
lines 1-10/10 (END)
```



Universidad
Industrial de
Santander

Activamos el firewall de seguridad para el puerto 8080.

```
angel@angel-X456UF /etc/systemd/system $ sudo ufw allow 8080/tcp
Reglas actualizadas
Reglas actualizadas (v6)
```

*Configuramos una interfaz para el administrador web editando el archivo
tomcat-users.xml*

```
angel@angel-X456UF ~ $ sudo nano /opt/tomcat/apache-tomcat-9.0.31/conf/tomcat-users.xml
angel@angel-X456UF ~ $
```

Somos **el mejor** escenario
de creación e innovación.

www.uis.edu.co





Al final del archivo agregamos nombres de rol y usuario.

```
examples web application, do not forget to remove the <!-- ..> that surrounds
them. You will also need to set the passwords to something appropriate.
-->
<!--
<role rolename="tomcat"/>
<role rolename="role1"/>
<user username="tomcat" password="<must-be-changed>" roles="tomcat"/>
<user username="both" password="<must-be-changed>" roles="tomcat,role1"/>
<user username="role1" password="<must-be-changed>" roles="role1"/>
-->
<role rolename="admin-gui"/>
<role rolename="manager-gui"/>
<user username="admin" password="admin123" roles="admin-gui, manager-gui"/>
</tomcat-users>
```

^G Ver ayuda ^O Guardar ^W Buscar ^K Cortar Tex ^J Justificar ^C Posición
^X Salir ^R Leer fich. ^\ Reemplazar ^U Pegar txt ^T Ortografía ^_ Ir a línea



Probamos el puerto localhost:8080.



Universidad
Industrial de
Santander


Apache Tomcat/9.0.31 - Mozilla Firefox

Apache Tomcat/9.0.31 localhost:8080 90%

Home Documentation Configuration Examples Wiki Mailing Lists Find Help

Apache Tomcat/9.0.31

If you're seeing this, you've successfully installed Tomcat. Congratulations!



Recommended Reading:

- [Security Considerations How-To](#)
- [Manager Application How-To](#)
- [Clustering/Session Replication How-To](#)

[Server Status](#)
[Manager App](#)
[Host Manager](#)

Developer Quick Start

- [Tomcat Setup](#)
- [First Web Application](#)
- [Realms & AAA](#)
- [JDBC DataSources](#)
- [Examples](#)
- [Servlet Specifications](#)
- [Tomcat Versions](#)

Managing Tomcat

For security, access to the [manager webapp](#) is restricted. Users are defined in:

```
$CATALINA_HOME/conf/tomcat-users.xml
```

In Tomcat 9.0 access to the manager application is split between different users.
[Read more...](#)

[Release Notes](#)
[Changelog](#)
[Migration Guide](#)
[Security Notices](#)

Documentation

[Tomcat 9.0 Documentation](#)
[Tomcat 9.0 Configuration](#)
[Tomcat Wiki](#)

Find additional important configuration information in:

```
$CATALINA_HOME/RUNNING.txt
```

Developers may be interested in:

- [Tomcat 9.0 Bug Database](#)
- [Tomcat 9.0 JavaDocs](#)
- [Tomcat 9.0 Git Repository at GitHub](#)

Getting Help

[FAQ and Mailing Lists](#)

The following mailing lists are available:

- [tomcat-announce](#)
Important announcements, releases, security vulnerability notifications. (Low volume).
- [tomcat-users](#)
User support and discussion
- [taglibs-user](#)
User support and discussion for [Apache Taglibs](#)
- [tomcat-dev](#)
Development mailing list, including commit messages

Somos **el mejor** escenario
de creación e innovación.

www.uis.edu.co




Configuración de un directorio web

Crearemos un directorio para nuestro primer sitio web “operativos.com”.

```
angel@angel-X456UF ~ $ sudo mkdir -p /var/www/operativos.com/html  
[sudo] password for angel:  
angel@angel-X456UF ~ $
```

Asignamos un usuario propietario con la siguiente línea de código.

```
angel@angel-X456UF ~ $ sudo chown -R $USER:$USER /var/www/operativos.com/html  
angel@angel-X456UF ~ $
```



El usuario tendrá permisos de escritura, los pertenecientes al mismo grupo del usuario y otros podrán únicamente leer y ejecutar lo que se encuentre en nuestro directorio

```
angel@angel-X456UF ~ $ sudo chmod -R 755 /var/www/operativos.com/html
angel@angel-X456UF ~ $
```

*Creamos nuestro archivo “**index.html**” .*

```
angel@angel-X456UF ~ $ sudo nano /var/www/operativos.com/html/index.html
```



Index.html :

```
<html>
  <head>
    <title> Directorio Operativos </title>
  </head>
  <body>
    <h1> !!Hola!! Saludos desde /var/www/operativos.com
    <br>
    <h2> Has logrado acceder a nuestro directorio, todo funciona de maravilla
  </body>
</html>
```





Universidad
Industrial de
Santander

Creamos un archivo que contenga las directivas para la ejecución del directorio operativos.com en Apache.

```
angel@angel-X456UF ~ $ sudo nano /etc/apache2/sites-available/operativos.com.conf
```



Somos **el mejor** escenario
de creación e innovación.

www.uis.edu.co



operativos.com.conf :

```
<VirtualHost *:8085>  
    ServerAdmin admin@operativos.com  
    ServerName operativos.com  
    ServerAlias www.operativos.com  
    DocumentRoot /var/www/operativos.com/html  
    ErrorLog ${APACHE_LOG_DIR}/error.log  
    CustomLog ${APACHE_LOG_DIR}/access.log combined  
</VirtualHost>
```



Universidad
Industrial de
Santander

Somos **el mejor** escenario
de creación e innovación.

www.uis.edu.co



Activamos el puerto 8085 en Apache

```
angel@angel-X456UF ~ $ sudo nano /etc/apache2/ports.conf
```

```
GNU nano 2.5.3      Archivo: /etc/apache2/ports.conf

# If you just change the port or add more ports here, you will likely also
# have to change the VirtualHost statement in
# /etc/apache2/sites-enabled/000-default.conf

Listen 80
Listen 8085

<IfModule ssl_module>
    Listen 443

[ 16 líneas leídas ]

^G Ver ayuda    ^O Guardar      ^W Buscar       ^K Cortar Texto  ^J Justificar
^X Salir        ^R Leer fich.   ^\ Reemplazar    ^U Pegar txt     ^T Ortografía
```



Universidad
Industrial de
Santander

Activamos y validamos las directivas creadas anteriormente.

```
angel@angel-X456UF ~ $ sudo a2ensite operativos.com.conf
Enabling site operativos.com.
To activate the new configuration, you need to run:
    service apache2 reload
angel@angel-X456UF ~ $
```

Test útil para encontrar errores de configuración del servidor

```
angel@angel-X456UF ~ $ sudo apache2ctl configtest
AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1. Set the 'ServerName' directive globally to suppress this message
Syntax OK
```

Somos **el mejor** escenario
de creación e innovación.

www.uis.edu.co





Recargamos el servidor Apache.

```
angel@angel-X456UF ~ $ sudo service apache2 reload
angel@angel-X456UF ~ $
```

Probamos que obtengamos respuesta del puerto 8085.





Universidad
Industrial de
Santander

#LaUISqueQueremos

iGracias!

