

**Práctica 3 – Autenticación y confidencialidad.**

**El principal objetivo de esta práctica es que el alumno sea capaz establecer mecanismos para asegurar las comunicaciones entre el cliente y el servidor, obtener e instalar certificados digitales y configurar los mecanismos de autenticación ofrecidos por Apache.**

1. Por defecto, Apache incorpora un certificado de autorización propio. Comprueba, que si escribimos <https://localhost> funciona correctamente y podemos mantener una conexión segura. ¿Qué aviso nos da el navegador? ¿Por qué motivo nos da este mensaje? ¿Cuál es la principal diferencia entre este certificado y el certificado que aparece, por ejemplo de <https://www.bankia.es>?
2. Virtualhost seguro. Configura uno de los virtualhost creados en la práctica 1 de manera que este virtualhost utilice una conexión segura por defecto mediante SSL. Para ello:
   1. Obtén un **certificado auto firmado** para tu dominio (mediante OpenSSL y ayuda de los contenidos de la web)
   2. Configura tu virtualhost haciendo uso de los certificados generados anteriormente:

<VirtualHost rafagion.com:443>

DocumentRoot "C:\xampp\htdocs\rafagion"

ServerName rafagion.com

SSLEngine On

SSLCertificateFile "C:/xampp/apache/conf/ssl.crt/rafagion.crt"

SSLCertificateKeyFile "C:/xampp/apache/conf/ssl.key/rafagion.key"

<Directory "C:\xampp\htdocs\rafagion">

Order deny,allow

Allow from all

</Directory>

</VirtualHost>

Verifica que en http.conf está habilitado: LoadModule ssl\_module modules/mod\_ssl.so

Si es así, comprueba que en tu virtualhost ya puedes navegar de manera segura.

1. Vamos a comprobar el acceso a nuestro virtualhost web utilizando la **autenticación básica** ofrecida por el protocolo HTTP. Para ello, realizaremos los siguientes pasos:
   1. Crea un fichero con dos usuarios y dos passwords.
   2. **Sin utilizar .htaccess,** configura el directorio de tu virtualhost y comprueba el acceso a diferentes carpetas de tu servidor.

<https://httpd.apache.org/docs/trunk/es/mod/mod_auth_basic.html>