# DAW Práctica 2.5: Certificados Nginx en host virtual.

Creamos el directorio ssl en /etc/nginx y generamos la clave privada y el certificado con los comandos:

sudo openssl genpkey -algorithm RSA -out /etc/nginx/ssl/server.key -pkeyopt rsa\_keygen\_bits:2048

Texto

Descripción generada automáticamente

* **genpkey**: Especifica que estamos generando una clave privada.
* -**algorithm RSA**: Indica que queremos usar el algoritmo RSA para generar la clave.
* **-out /etc/nginx/ssl/server.key**: Define el archivo donde se guardará la clave privada.
* **-pkeyopt rsa\_keygen\_bits:2048**: Configura la longitud de la clave, en este caso, 2048 bits.

Después creamos el certificado con el comando:  
sudo openssl req -x509 -nodes -days 365 -key /etc/nginx/ssl/server.key -out /etc/nginx/ssl/server.crt

Texto

Descripción generada automáticamente

Esta configuración no cuenta con passphrase ya que el parámetro -nodes desactiva la solicitud de passphrase. Sí en la pagina anterior estaba implementada. La diferencia es que con passphrase la clave privada esta protegida con una contraseña y que sin passphrase no se requiere utilizar contraseña.

* **req**: Genera una solicitud de certificado o un certificado autofirmado.
* **-x509**: Crea un certificado X.509, que es el estándar para certificados digitales.
* **-nodes**: No cifra la clave privada (sin passphrase).
* **-days 365**: Establece la validez del certificado en 365 días.
* **-key**: Especifica la clave privada a utilizar.
* **-out**: Define el archivo donde se guardará el certificado autofirmado.

Editamos el archivo de configuración de nuestro host virtual. Por ejemplo, si el archivo es /etc/nginx/sites-available/default.

Una vez hecho confirmamos la correcta sintaxis con sudo nginx -t y reiniciamos el servidor.

Captura de pantalla de computadora

Descripción generada automáticamente



Cuando intentamos acceder al sitio, el navegador mostrará un mensaje de advertencia porque el certificado es autofirmado. Esto ocurre porque los navegadores no confían en certificados que no estén emitidos por una autoridad certificadora (CA) reconocida.

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Interfaz de usuario gráfica, Texto

Descripción generada automáticamente

Después modificaremos el archivo de configuración de nuevo para que nos redirija al https si intentamos acceder a http. Una vez hecho reiniciamos el servicio.

Texto

Descripción generada automáticamente

De esta manera si intentamos acceder al sitio web mediante http se nos redirigirá automáticamente al sitio web con https