Instalación de Certificados Seguros

Francisco Javier Otero Herrero

Grupo ATU

10-04-2025

Instalación de Certificados Seguros

Francisco Javier Otero Herrero | GRUPO ATU

Instalación de Certificados Seguros

Actividad 4:

1. **Tenemos un servidor recién instalado y queremos instalarle un certificado de seguridad, ¿Qué debemos hacer? Explicar los pasos a seguir para solicitar e instalar un certificado de seguridad.**

Instalar un certificado de seguridad ***SSL/TLS*** en un servidor recién instalado implica varios pasos clave. A continuación, vamos a detallar el proceso completo para configurar un ***certificado SSL/TLS en un servidor:***

a. Verificar los requisitos previos:

- El servidor está configurado correctamente: El servidor web (por ejemplo, Apache, Nginx) debe estar funcionando.
- ***Tienes un dominio registrado:*** Necesitas un nombre de dominio (por ejemplo, www.ejemplo.com) asociado a la dirección IP de tu servidor.
- ***DNS está configurado:*** El dominio debe apuntar al servidor mediante registros DNS.

b. Generar una solicitud de firma de certificado (CSR):

Un CSR (Certificate Signing Request) es un archivo que contiene información sobre tu organización y dominio. Lo necesitas para solicitar un certificado ***SSL/TLS*** a una Autoridad de Certificación ***(CA).*** Pasos para generar un CSR:

- ✓ ***Generar una clave privada:***

```
openssl genpkey -algorithm RSA -out private.key
```

Esto crea un archivo llamado ***private.key,*** que es la clave privada.

- ✓ ***Generar el CSR:***

```
openssl req -new -key private.key -out request.csr
```

Durante este proceso, se nos pedirá información como:

I. ***Nombre común (CN):*** *Tu dominio (por ejemplo, www.ejemplo.com).*
II. ***Organización (O):*** *Nombre de tu empresa o proyecto.*
III. ***Ubicación:*** *Ciudad, estado y país.*

Instalación de Certificados Seguros

- ✓ ***Guarda el CSR (request.csr):***

  Este archivo se enviará a la ***CA*** para solicitar el certificado.

c. *Elegir y comprar un certificado SSL/TLS:*

Existen varias opciones dependiendo de nuestras necesidades:

- ***Certificados gratuitos:*** *Por ejemplo,* ***Let's Encrypt*** *ofrece certificados gratuitos válidos por 90 días.*
- ***Certificados pagados:*** *Emitidos* ***por CAs como DigiCert, Comodo, o GlobalSign,*** *con diferentes niveles de validación* ***(DV, OV, EV).***

d. *Instalar el certificado en el servidor:*

Una vez que tengamos los archivos del certificado (generalmente ***.crt)***, debemos seguir los siguientes pasos:

Para Apache(Linux):

- Coloca los archivos en el directorio adecuado, por ejemplo, en la siguiente ruta: *etc/apache2/ssl/).*
- Edita el archivo de configuración del sitio virtual, por ejemplo, */etc/apache2/sites-available/default-ssl.conf):*

```
<VirtualHost *:443>
     ServerName www.ejemplo.com
     DocumentRoot /var/www/html

     SSLEngine on
     SSLCertificateFile
     /etc/apache2/ssl/certificate.crt
     SSLCertificateKeyFile
     /etc/apache2/ssl/private.key
</VirtualHost>
```

- Habilita el módulo SSL y el sitio seguro.
- Reiniciar Apache.

Instalación de Certificados Seguros

Para Nginx:

- Coloca los archivos en el directorio adecuado (por ejemplo, /etc/nginx/ssl/).
- Edita el archivo de configuración del servidor (por ejemplo, /etc/nginx/sites-available/default):

```
server {
    listen 443 ssl;
    server_name www.ejemplo.com;
    ssl_certificate
/etc/nginx/ssl/certificate.crt;
    ssl_certificate_key
/etc/nginx/ssl/private.key;
    root /var/www/html;
    index index.html;
}
```

- Reinicia Nginx: `sudo systemctl restart nginx`

e. Redirigir el tráfico HTTP a HTTPS

Para garantizar que todo el tráfico use ***HTTPS,*** configura redirecciones desde ***HTTP (puerto 80) a HTTPS (puerto 443):***

Para Apache:

- Edita el archivo de configuración del sitio virtual no seguro:

```
<VirtualHost *:80>
    ServerName www.ejemplo.com
     Redirect permanent /
     https://www.ejemplo.com/
</VirtualHost>
```

Instalación de Certificados Seguros

Para Nginx:

- Edita el archivo de configuración del servidor:

```
server {
    listen 80;
    server_name www.ejemplo.com;
     return 301
     https://$host$request_uri;
}
```

- Reinicia el servidor web después de hacer los cambios.

f. Verificar la configuración

Usa herramientas como ***SSL Labs' SSL Test*** para verificar que tu certificado esté correctamente configurado. Asegúrate de que el candado en la barra de direcciones del navegador aparezca cuando visites tu sitio.

g. Mantener el certificado actualizado

- ✓ Certificados gratuitos (Let's Encrypt): Se pueden configurar renovaciones automáticas.
- ✓ Certificados pagados: Renueva el certificado antes de su fecha de expiración y reinstálalo en el servidor.

Para hacer un pequeño resumen de los pasos que debemos seguir:

I. Generar una clave privada y un CSR.
II. Solicitar el certificado a una CA (gratuita o paga).
III. Instalar el certificado en el servidor.
IV. Configurar redirecciones HTTP a HTTPS.
V. Verificar la configuración y mantener el certificado actualizado.

Este proceso garantiza que el servidor esté protegido con cifrado ***SSL/TLS,*** mejorando la seguridad y la confianza de los posibles usuarios.