Crea un sitio Web seguro usando tu propio certificado digital (Windows y Linux).

Windows

Abrimos la ventana del Administrador de IIS, desde Herramientas administrativas.

Documentos		
	🕌 Terminal Services 🔹 🕨	
Equipo	📆 Administración de almacenamiento y recursos com	
	Administración de equipos	
Red	🎕 Administrador de Internet Information Services (IIS)	Į.
	🚠 Administrador del servidor	Ì.
Panel de control	🚡 Asistente para configuración de seguridad	
	🙀 Certification Authority	
Herramientas administrativas 🕨	🕗 Configuración del sistema	
Avuda v soporte técnico	🍓 Copias de seguridad de Windows	
,,	🚡 Directiva de seguridad local	
Ejecutar	Explorador de almacenamiento	
	🗁 Firewall de Windows con seguridad avanzada	
	Herramienta de diagnóstico de memoria	

Entramos en Certificados de servidor.

📲 Administrador de Internet Inform	nation Services (IIS)		
🚱 💿 🥞 🖣 WIN-ENHZGVSSN65 🕨 🔯 🔯			
Archivo Ver Ayuda			
Conexiones	Pégina principal de	Acciones	
🔍 - 🔚 🖄 😥		Abrir característica	
Página de inicio		Administrar servidor	
	Agrupar por: Area 🔹 📷 🔹	💝 Reiniciar	
		Detener	
	Configuración Delegación de características	Ver grupos de aplicaciones Ver sitios	
	115	Ayuda Ayuda en pantalla	
	🖗 🔊 🔏 🗕		
	Almacenamiento Asignaciones de Autenticación en caché de r controlador		
	Certificados de servidor		

En el menú de la derecha, hacemos clic en Crear certificado autofirmado...

Administrador de Internet Inform	ation Services (IIS)		X
G S № WIN-ENHZGVSSN6	5 🕨		🗾 🖸 🐼 🕼 I 🕐 🔹
Archivo Ver Ayuda			
Conexiones &	Certificados de	servidor	Acciones Importar
Página de inicio WIN-ENHZGVSSN65 (WIN-ENHZ Grupos de aplicaciones D- Sitios	Utilice esta característica para solic puede usar el servidor web con sit Nombre A	citar y administrar certificados que ios web configurados para SSL. Emitido para WIN-FNHZGVSSN65-CA	Crear una solicitud de certificado Completar solicitud de certificado Crear certificado de dominio
			Crear certificado autofirmado Crear certificado autofirmado Image: Crear certificado aut

Le especificamos un nombre al certificado.

Crear certificado autofirmado	
Especificar nombre descriptivo	
Especifique un nombre de archivo para la solicitud de certificado. Esta información se pue una entidad de certificación para que la firme:	:de enviar a
Especifique un nombre descriptivo para el certificado:	
CertificadoWindows	

Si hacemos *clic derecho > Ver* sobre el certificado creado, podemos ver sus características.

Conexiones	Cartifica das da consider	Acciones
🔍 - 🕞 🖄 😽		Importar
Página de inicio WIN-ENHZGVSSN65 (WIN-ENHZ Grupos de aplicaciones	Utilice esta característica para solicitar y administrar certificados que puede usar el servidor web con sitios web configurados para SSL.	Crear una solicitud de certificado Completar solicitud de
	Nombre 🔺 Emitido para	certificado
_	WIN-ENHZGVSSN65-CA	Crear certificado de dominio
	CertificadoWindows Importar Importar Crear una solicitud de certificado Completar solicitud de certificado Completar solicitud de certificado Crear certificado de dominio Crear certificado autofirmado Ver Exportar Quitar Quitar Quida Ayuda en pantalla	Crear certificado autofirmado Ver Exportar X Quitar X Ayuda Ayuda en pantalla



Vamos a Default Web Site, y entramos en Enlaces... en el menú de la derecha.



En la nueva ventana que se abre, pinchamos en el botón Agregar...

Tipo	Nombre de host	Puerto	Dirección IP	Info	Agregar
nttp		80	*		h
					Modificar
					Quitar
(►	Examinar

Seleccionamos el tipo HTTPS y elegimos nuestro certificado. Aceptamos y ya tenemos nuestro certificado instalado en Windows.

r 1	Modificar enlace de sitio	E
Enlac Ti ht	Tipo: Dirección IP: Puerto: https Todas las no asignadas 443 Nombre de host:	
•	Certificado SSL:	
	Aceptar Cancelar	

Vamos a un cliente para entrar a nuestro servidor y comprobamos que el certificado funciona correctamente.





<u>Linux</u>

El primer paso es crear nuestra clave privada. Abrimos el terminal, y escribimos el comando openssl genrsa > clave.key. Esto generará una clave privada y la guardará en un fichero llamado clave.key

La clave pública se encuentra incluida dentro de la clave privada, y para extraerla usaremos el comando **openssl rsa –in clave.key –pubout –out publica.key**. Estará en un fichero llamado publica.key

servidorubuntu@ubuntu:~\$ openss1 rsa -in clave.key -pubout -out publica.key writing RSA key Usando ambas claves, crearemos nuestro certificado digital en un archivo llamado servidor.pem usando el comando **openssi req –new –key clave.key –x509 –days 365 –out servidor.pem**.

servidorubuntu@ubuntu:~\$ openssl req -new -key clave.key -x509 -days 365 -out se rvidor.pem 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]: State or Province Name (full name) [Some-State]: Locality Name (eg, city) []: Organization Name (eg, company) [Internet Widgits Pty Ltd]: Organizational Unit Name (eg, section) []: Common Name (e.g. server FQDN or YOUR name) []: Email Address []:

Para instalar el certificado en nuestro servidor Apache, llevamos la clave privada clave.key al directorio /etc/ssl/private y el certificado servidor.pem al directorio /etc/ssl/certs

servidorubuntuQubuntu:~\$ sudo cp clave.key /etc/ssl/private/clave.key servidorubuntuQubuntu:~\$ sudo cp servidor.pem /etc/ssl/certs/servidor.pem

Modificamos el fichero /etc/apache2/sites-available/default-ssl para incluir las rutas de la clave privada y el certificado, tal como se indica en la captura.

GNU nano 2.2.6 Archivo: /etc/apache2/sites-available/default-ssl Modificado
SSL Engine Switch:
Enable/Disable SSL for this virtual host.
SSLEngine on
A self-signed (snakeoil) certificate can be created by installing
the ssl-cert package. See
/usr/share/doc/apache2.2-common/README.Debian.gz for more info.
If both key and certificate are stored in the same file, only the
SSLCertificateFile directive is needed.
SSLCertificateFile /etc/ssl/certs/servidor.pem
SSLCertificateKeyFile /etc/ssl/private/clave.key

Escribimos el comando sudo a2enmod ssl y después reiniciamos el servicio apache2.



Después, el comando sudo a2ensite default-ssl y sudo service apache2 reload.



Usamos un cliente para comprobar que el certificado funciona correctamente.



It works!

This is the default web page for this server.

The web server software is running but no content has been added, yet.