ACTIVIDAD 5 - CERTIFICADO HTTPS

Cristóbal Suárez Abad

SEGURIDAD Y ALTA DISPONIBILIDAD - 2º ASIR

Contenido

Descarga e instalación de “mkcert”.

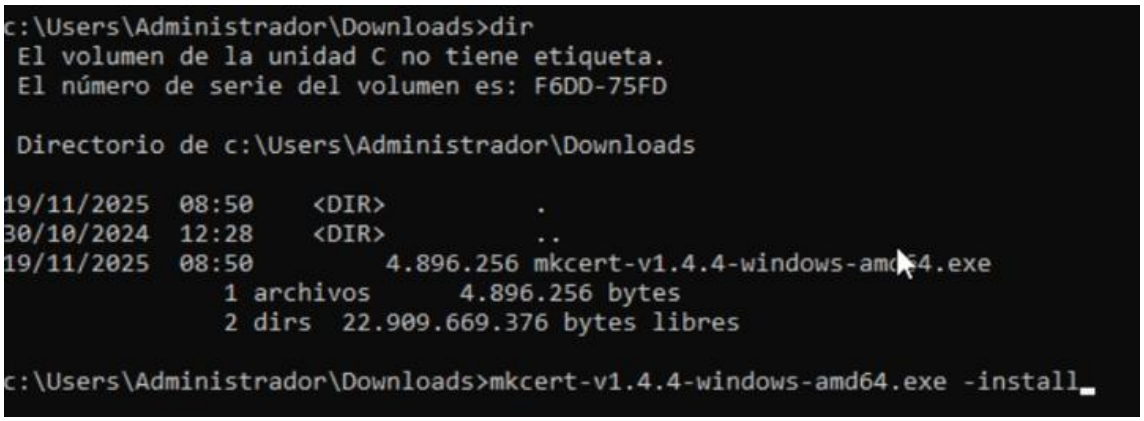
Enlace del proyecto en GitHub:

https://github.com/FiloSottile/mkcert/releases

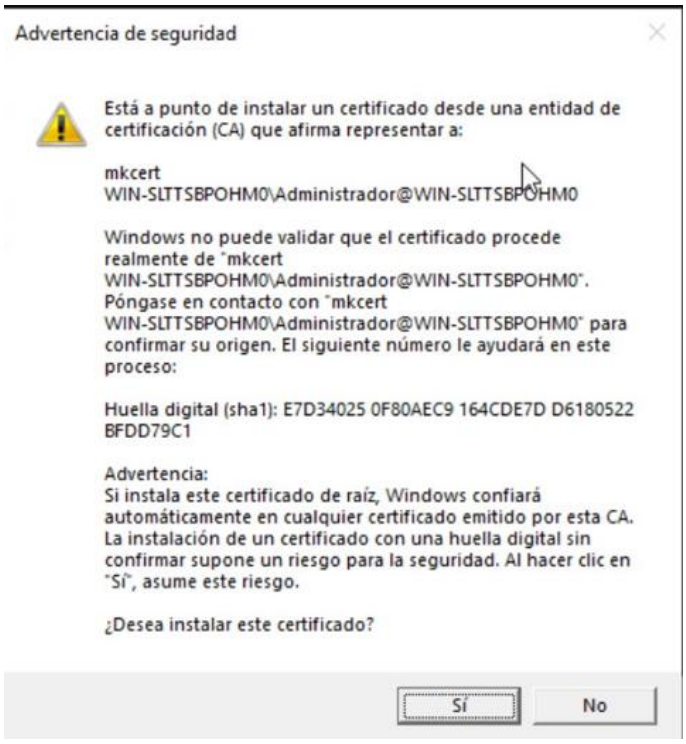
Nos descargamos la versión correspondiente para nuestro sistema operativo. En este caso la de Windows: mkcert-v1.4.4-windows-amd64.exe

Ahora para instalarlo lo haremos desde el CMD. Para ello navegamos hasta el directorio donde hayamos guardado el archivo .exe anterior y ejecutamos:

mkcert -install



Nos saldrá la siguiente ventana y le damos a “si”:

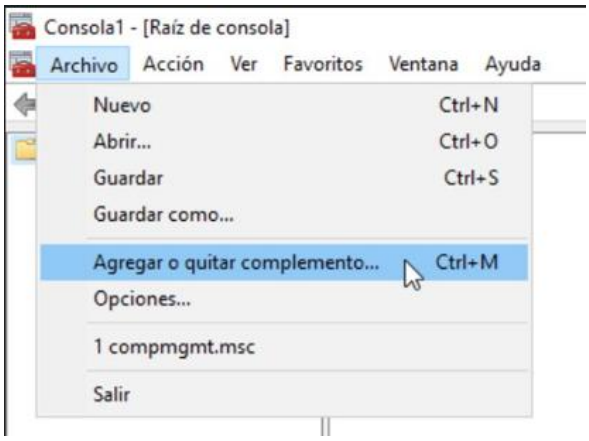


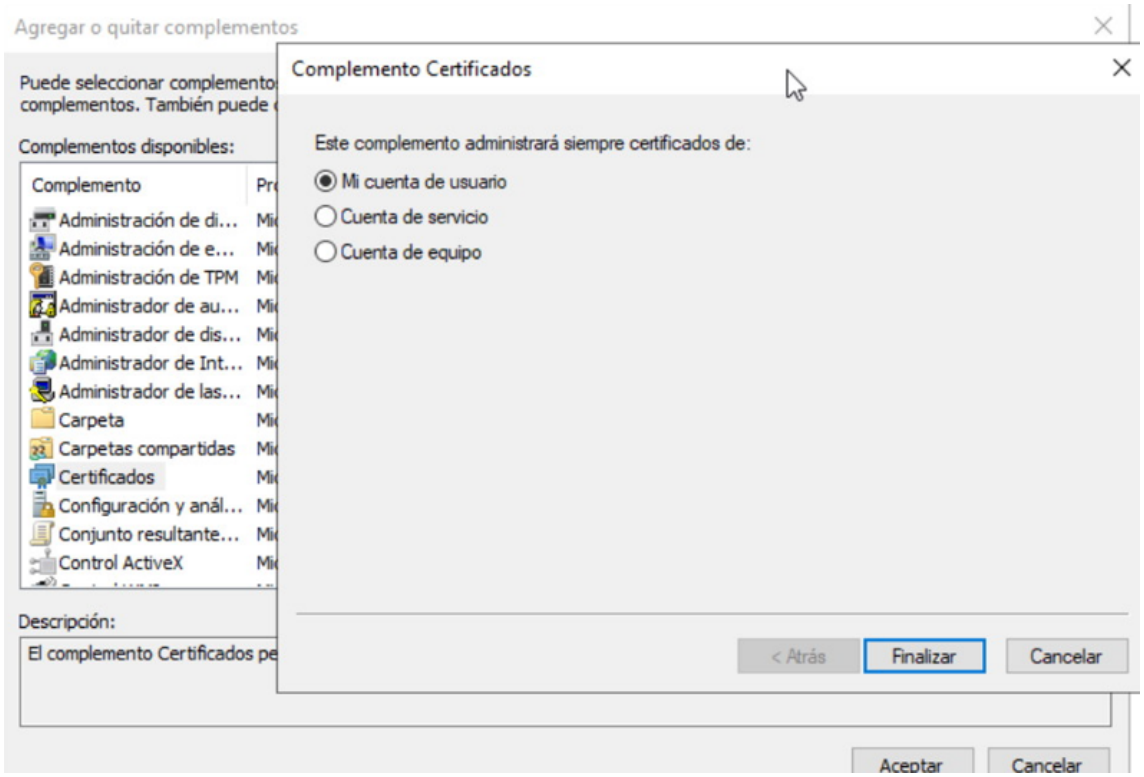
Nos debe salir a continuación esto en el CMD:

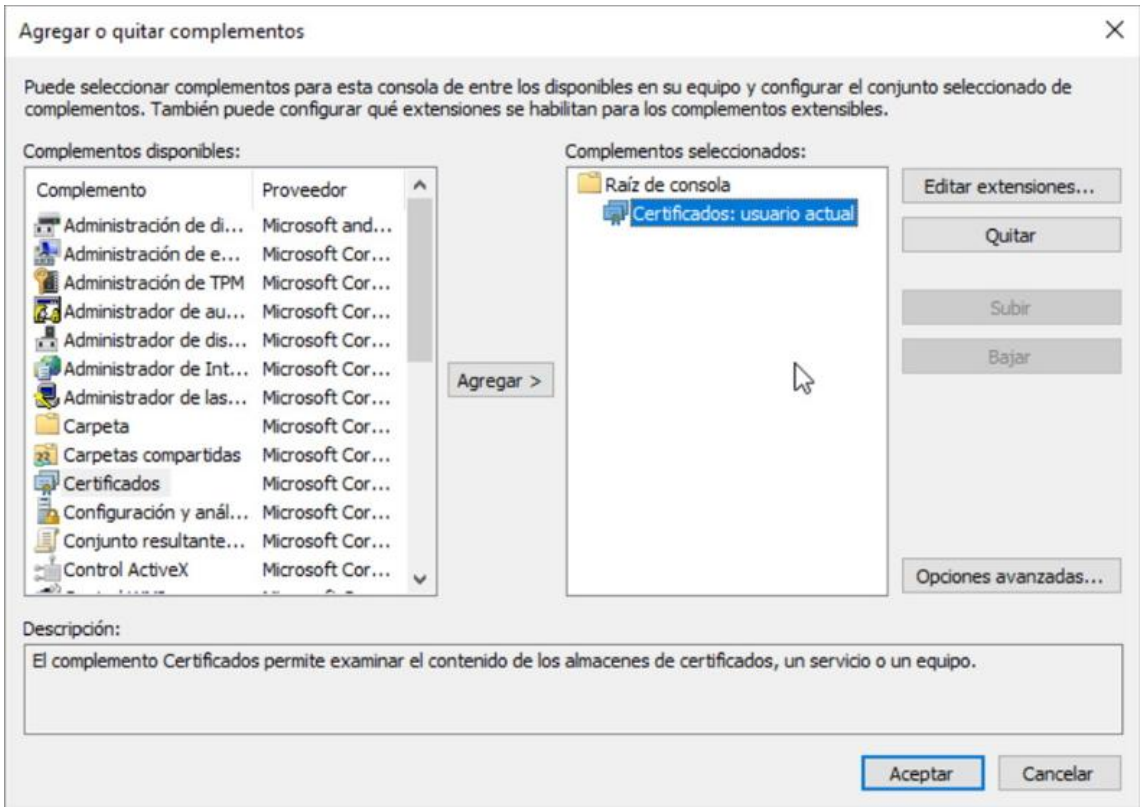
```
c:\Users\Administrador\Downloads>mkcert-v1.4.4-windows-amd64.exe -install
Created a new local CA 🎉
The local CA is now installed in the system trust store! ⚡
```

Ahora vamos a comprobar que el este certificado raíz se ha instalado debidamente.

Para ello ejecutamos "**mmc.exe**" y nos creamos una "consola" o "maletín de herramientas". En él, debemos incluir el complemento de "**Certificados**".

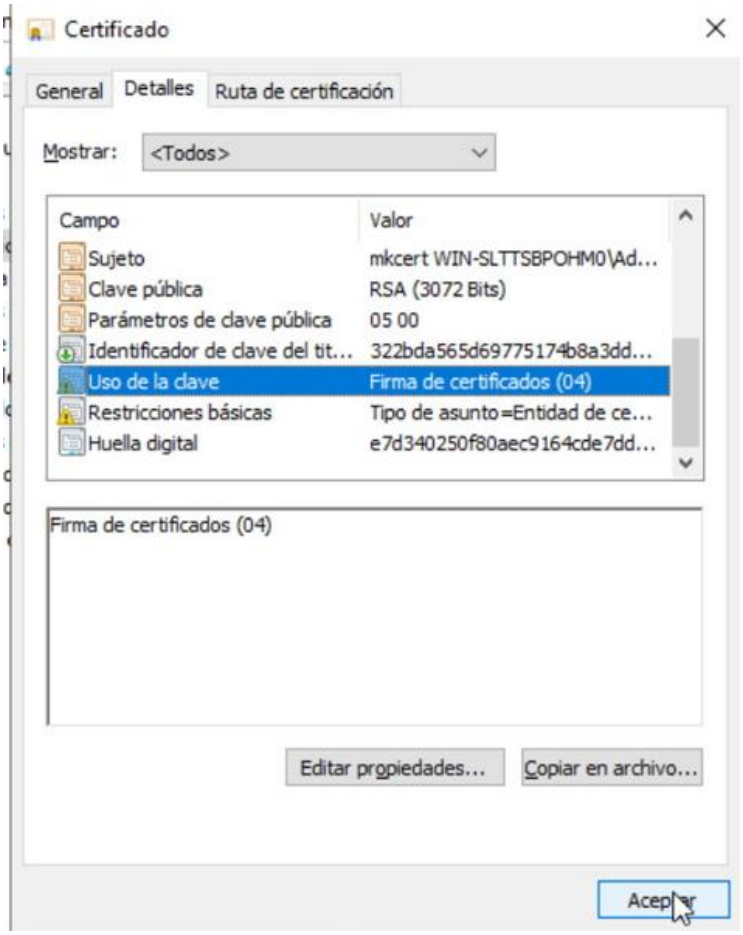






Lo abrimos y buscamos el certificado:

Si hacemos doble clic sobre ella, veremos cual es su función:



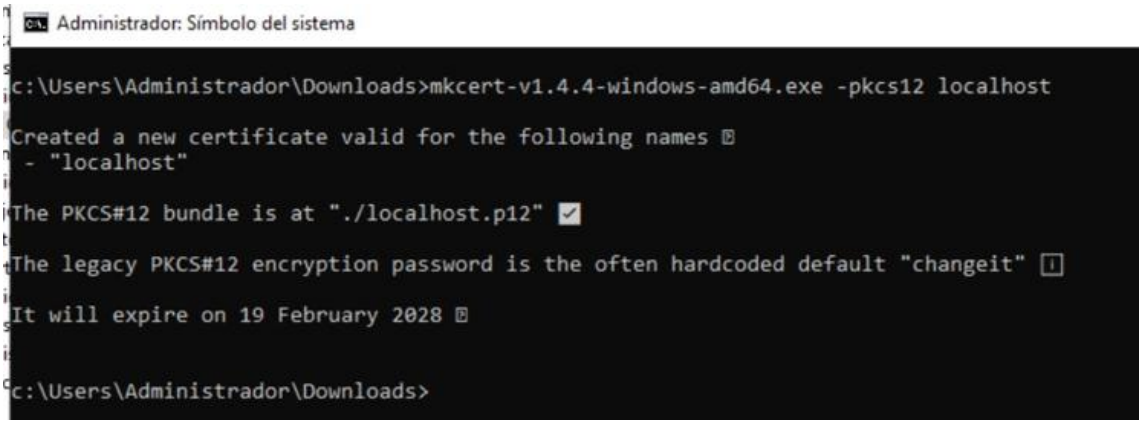
Generando certificados con mkcert.

"Hacerlo es muy sencillo: basta con ejecutar mkcert seguido del nombre o nombres de dominio para los que queremos generar certificados. Por ejemplo, para un certificado válido para localhost:"

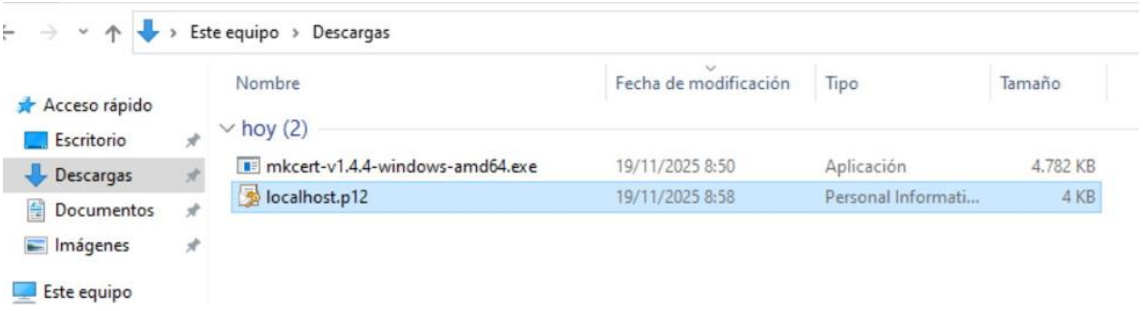
mkcert localhost

Este comando generará un certificado digital y un archivo de clave privada en formato PEM (se usará para Linux y MacOS). Para Windows es necesario usar el formato "PKCS 12", por lo tanto, usaremos la opción "-pkcs12".

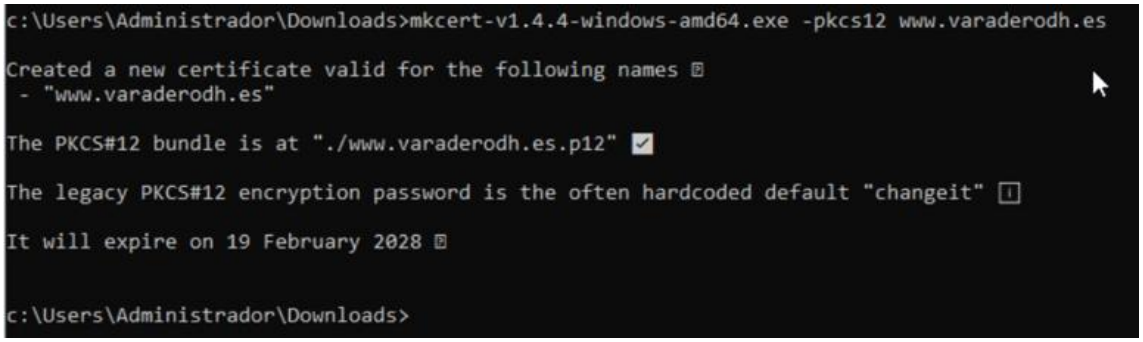
Ejemplo: **mkcert -pkcs12 localhost**

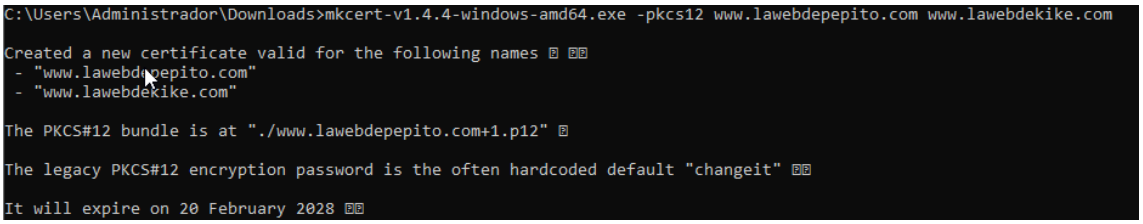


Vemos el archivo generado:



Podemos crear para otros dominios e incluso para varios a la vez.

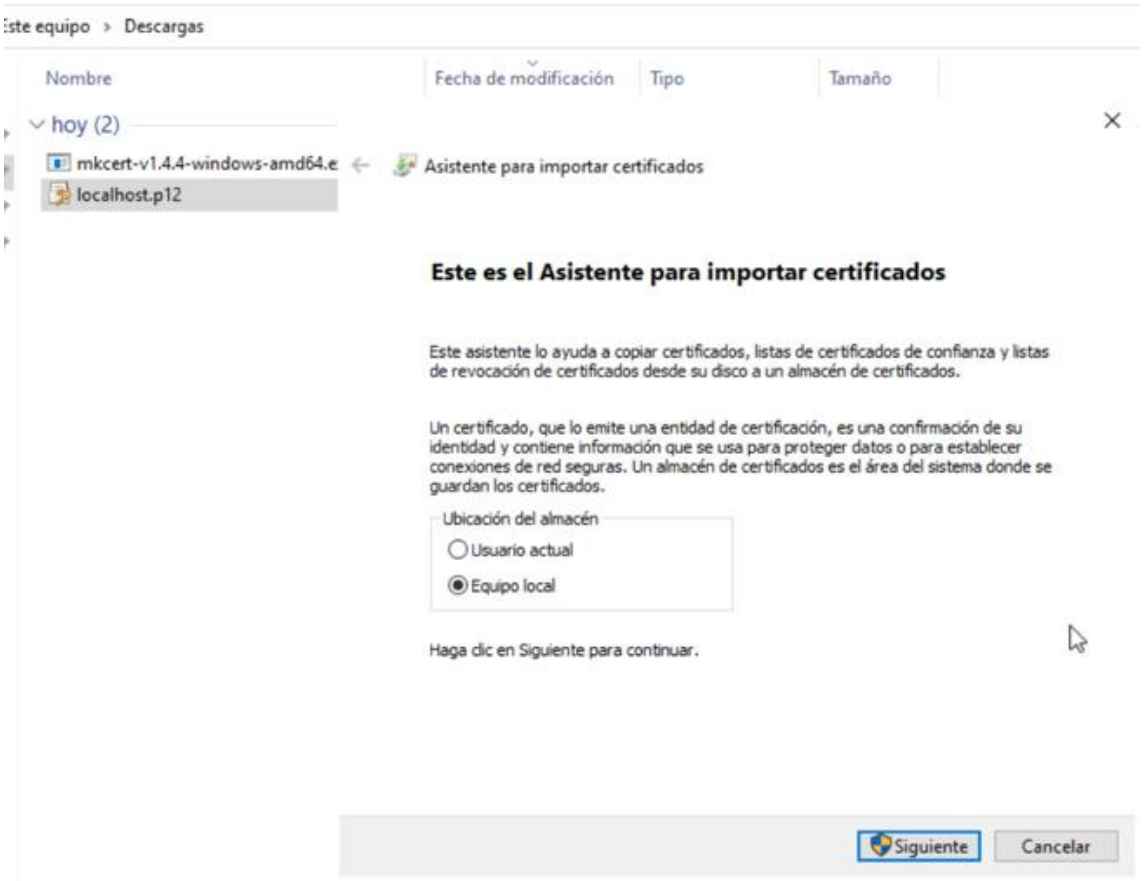


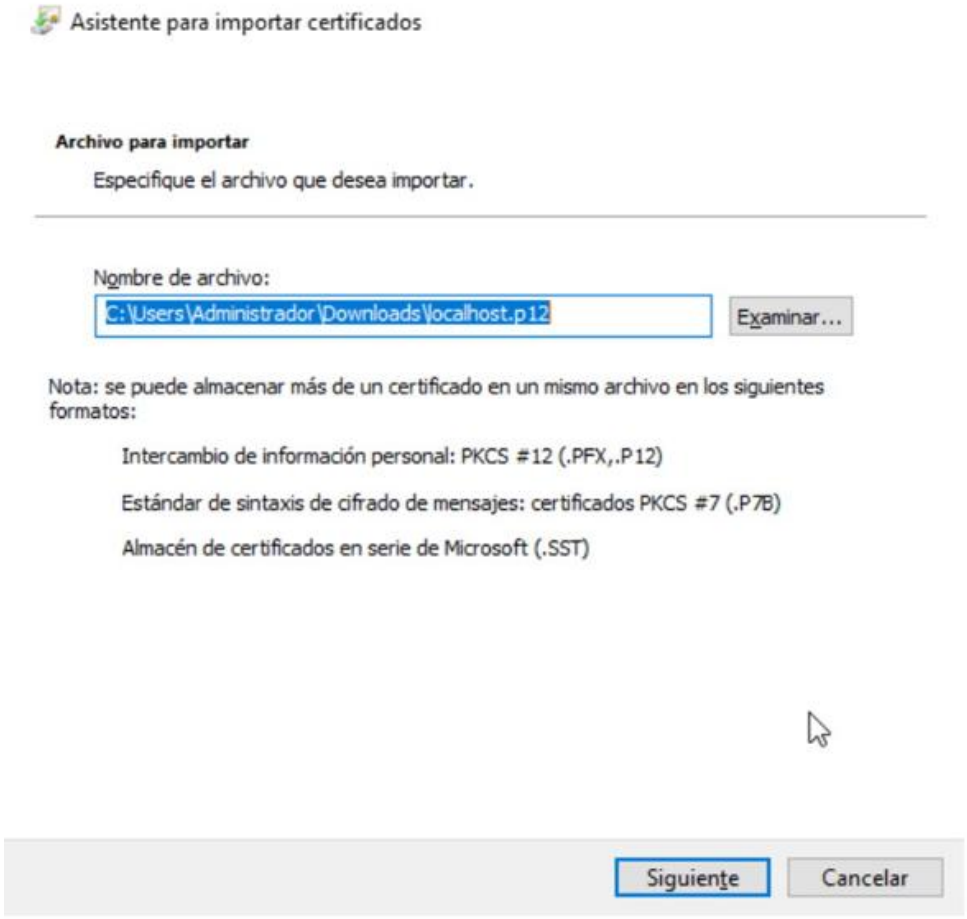


Ahora solo nos queda incorporarlo a la lista de los certificados de la máquina y asignarlos a un sitio web. En este caso vamos a hacerlo en Windows Server.

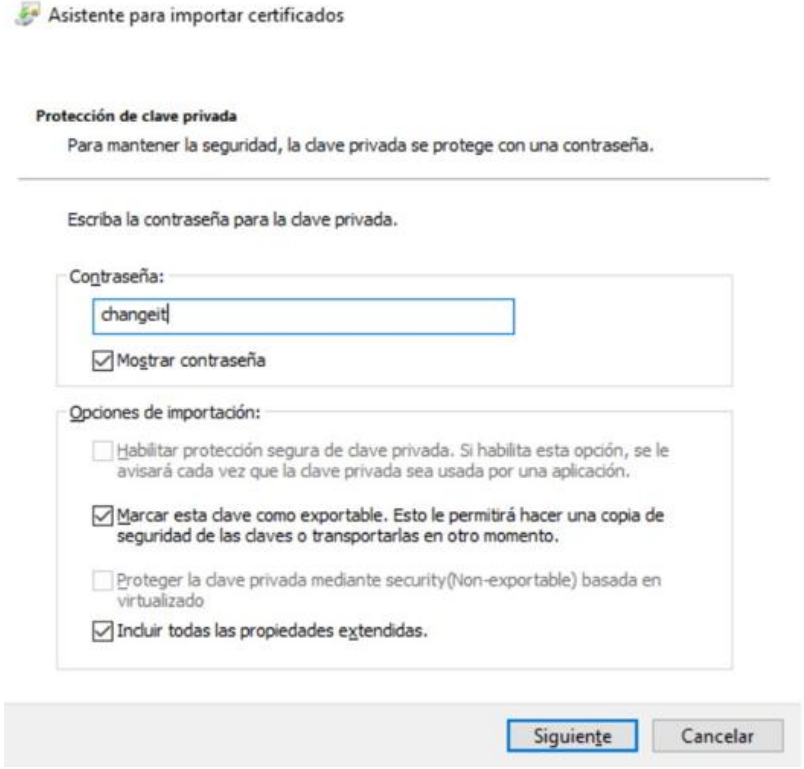
Instalar el certificado en el sistema

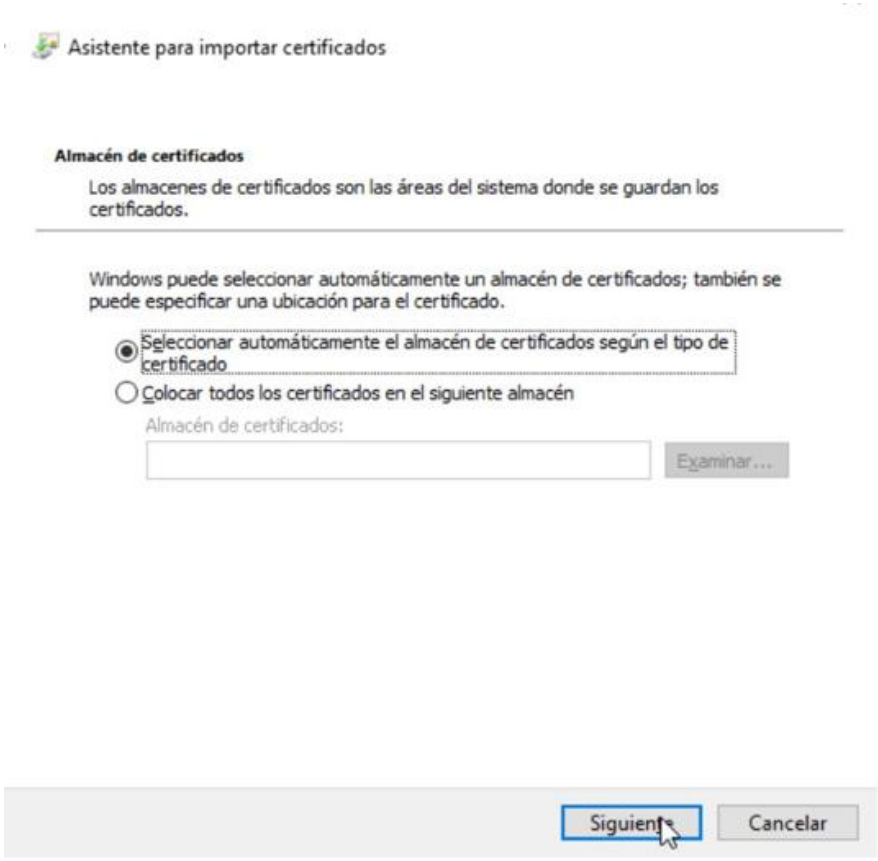
Para ello solo debemos hacer doble clic en el archivo que hemos generado anteriormente. Entonces nos aparecerá la ventana del asistente. Para la ubicación del almacén, le daremos a “Equipo Local”.

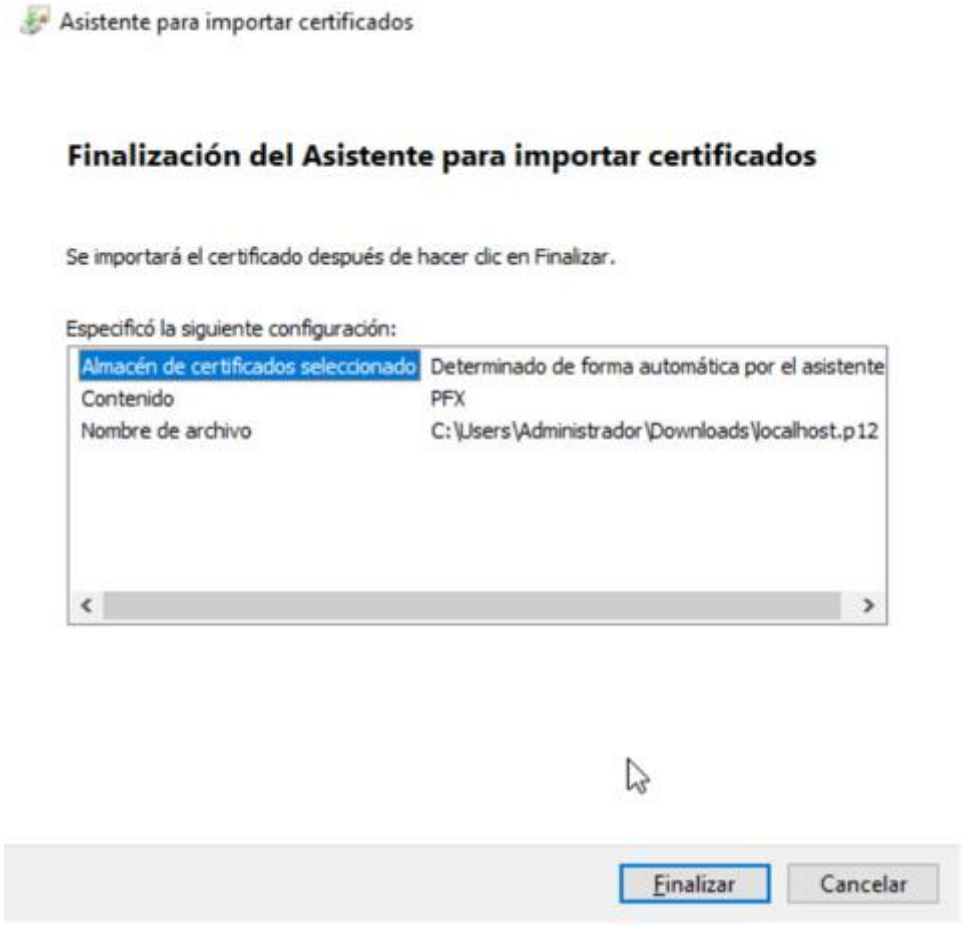




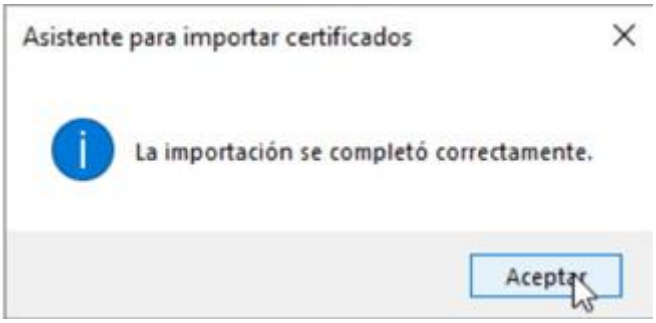
La contraseña es la que nos aparecía cuando generábamos el archivo.




Asistente para importar certificados
Almacén de certificados
Los almacenes de certificados son las áreas del sistema donde se guardan los certificados.
Windows puede seleccionar automáticamente un almacén de certificados; también se puede especificar una ubicación para el certificado.
Seleccionar automáticamente el almacén de certificados según el tipo de certificado
Colocar todos los certificados en el siguiente almacén
Almacén de certificados:
Examinar...
Siguiente
Cancelar

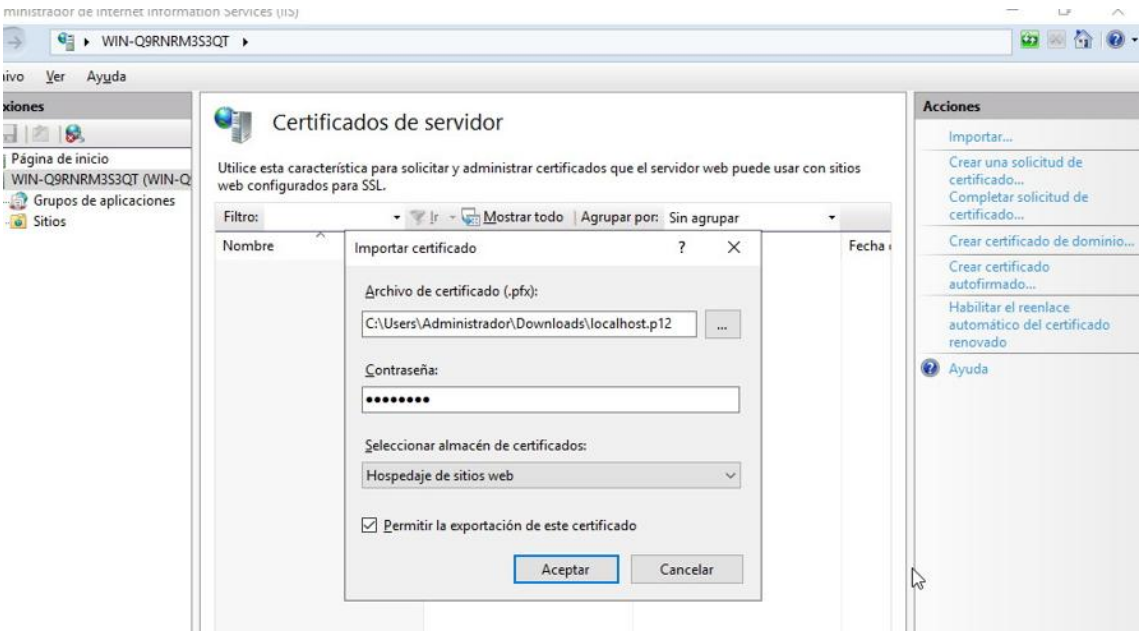

Asistente para importar certificados
Finalización del Asistente para importar certificados
Se importará el certificado después de hacer clic en Finalizar.
Especificó la siguiente configuración:
Almacén de certificados seleccionado
Determinado de forma automática por el asistente
Contenido
PFX
Nombre de archivo
C:\Users\Administrador\Downloads\localhost.p12
Finalizar
Cancelar

Finalizado.

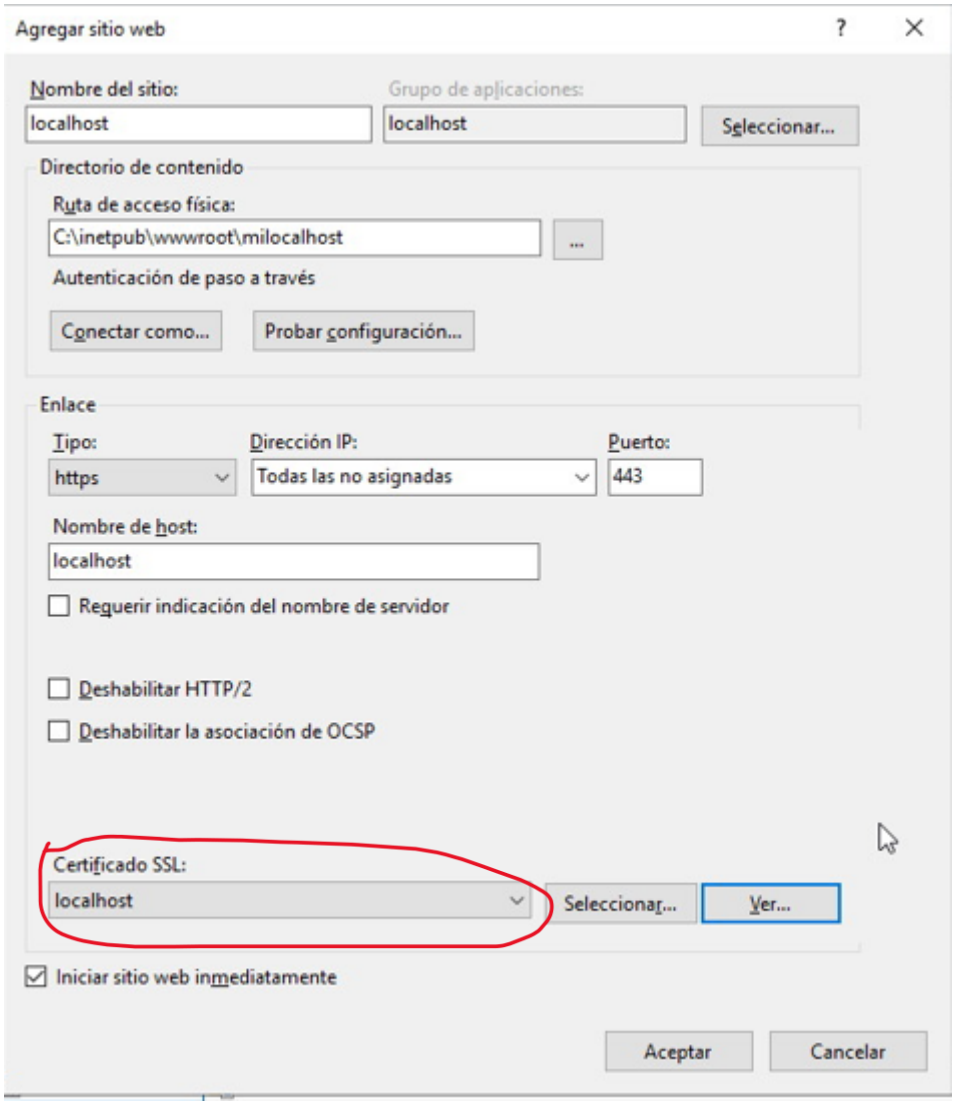

Asistente para importar certificados
La importación se completó correctamente.
Aceptar

Crea servicio https con el certificado creado y pruébalo desde propio Windows Server.

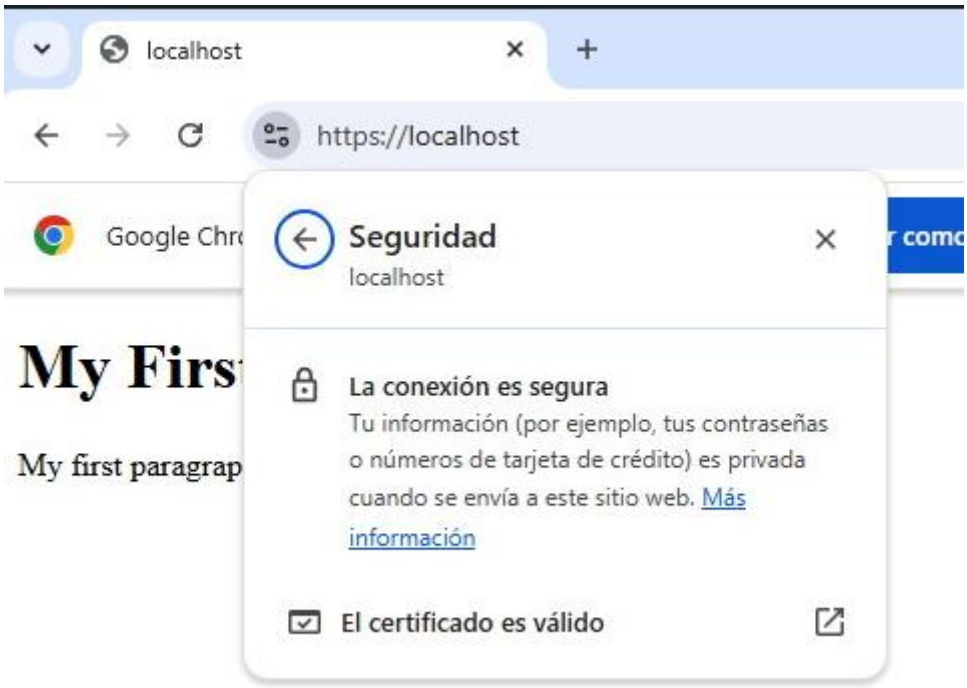
En el servicio IIS de Windows nos vamos a la sección "**Certificados del Servidor**". Si por cualquier motivo no nos aparece el certificado anterior, debemos incorporarlo nosotros mismos. Le damos a "**Importar**". Elegimos el archivo, ponemos su contraseña ("changeit") y seleccionamos que será para "**Hospedaje de sitios web**".



Luego cuando vayamos a crear un nuevo sitio web, debemos indicar que su Certificado SSL es el que hayamos importado.



Ahora cuando vayamos a la página, usando "**localhost**", desde el propio servidor web. Podremos acceder directamente, sin la típica señal de advertencia del navegador diciendo que no reconoce el certificado.



Visor de certificados: localhost

General | Detalles

Enviado a

Nombre común (CN)	localhost
Organización (O)	mkcert development certificate
Unidad organizativa (OU)	WIN-Q9RNRM3S3QT\Administrador@WIN-Q9RNRM3S3QT

Emitido por

Nombre común (CN)	mkcert WIN-Q9RNRM3S3QT\Administrador@WIN-Q9RNRM3S3QT
Organización (O)	mkcert development CA
Unidad organizativa (OU)	WIN-Q9RNRM3S3QT\Administrador@WIN-Q9RNRM3S3QT

Período de validez

Emitido el	jueves, 20 de noviembre de 2025, 16:55:51
Vencimiento el	domingo, 20 de febrero de 2028, 16:55:51

Huellas digitales SHA-256

Certificado	461e4ea1834ea20010327018f06bc134c3a21a959bc34d202324fb23204b0a72
Clave pública	4226f0fc225ed779e60a437a6910583c216e72fac150fae210d605f4da1f242f

Si lo intentamos poniendo su IP, incluso desde el servidor web, nos saldrá la ventana de advertencia mencionada previamente.