



# **Certificado de Profesionalidad en Seguridad Informática**

**IronHack - SOC**

**Módulo 4**

**Examen Práctico**

**Alumno: Julián Gordon**

# Indice

<b>Enunciado.....</b>	<b>3</b>
<b>Introducción.....</b>	<b>5</b>
<b>Actividad 1 - Registro de dominio en Duckdns.....</b>	<b>6</b>
<b>Actividad 2 - Servidor web en Windows con Internet Information Services (IIS)...</b>	<b>10</b>
<b>Actividad 3 - Configuración del router.....</b>	<b>16</b>
<b>Actividad 4 - Configuración de HTTPS en el servidor web.....</b>	<b>20</b>
<b>Actividad 5 - Importancia de certificados web y beneficios de utilizar HTTPS.....</b>	<b>27</b>
<b>Conclusiones.....</b>	<b>30</b>

# Enunciado

## Actividad 1

(2 punt) Objetivo: Registra un dominio gratuito y comprobar el registro DNS. Tareas:

1. Selecciona un proveedor de registro de dominio gratuito (por ejemplo, duckdns.org).
2. Registra un nuevo dominio y asócialo a la IP pública de la empresa.
3. Comprueba la resolución del dominio en un servidor DNS.
4. Captura pantallas del proceso de registro y comprobación de la resolución DNS.

## Activitat 2

(2 punt) Objetivo: Instala y configura un servidor web en Windows (alternativamente en Linux) utilizando Internet Information Services (IIS). Tareas:

1. Instalar IIS en un servidor Windows.
2. Comprobar el funcionamiento del servidor accediendo desde la red local y desde internet.
3. Documentar los pasos con capturas de pantalla y explicaciones breves.

## Activitat 3

(2 punts) Objetivo: Configura el router para permitir el acceso externo al servidor web. Tareas:

1. Abre los puertos 80 y 443 en el router y redirígelos a la IP del servidor IIS.
2. Prueba el acceso al servidor web desde una red externa.
3. Documenta el proceso con capturas de pantalla.

## Activitat 4

(2 punts) Objetivo: Configurar HTTPS en el servidor web. Tareas:

1. Obtén un certificado SSL utilizando una herramienta como "Certify the Web".
2. Configura IIS para utilizar HTTPS con el certificado SSL.
3. Comprueba que el sitio web es accesible a través de HTTPS y que el certificado es válido.
4. Documenta el proceso con capturas de pantalla.

## Activitat 5

(2 punts) Objetivo: Explica la importancia de certificar el sitio web y los beneficios de utilizar HTTPS. Tareas:

1. Justifica la necesidad de certificar el sitio web, explicando los beneficios que conlleva en cuanto a seguridad para la empresa y los usuarios.
2. Qué riesgos has conseguido mitigar mediante la implementación de HTTPS. ¿Un usuario normal se sentiría seguro? ¿Tú como usuario avanzado te sentirías seguro visitando la web?

## Introducción

Este trabajo tiene como objetivo principal explorar y aplicar conceptos clave en la gestión de dominios, configuración de servidores web y la implementación de seguridad en entornos web mediante la utilización de HTTPS. La importancia de estos elementos radica en su capacidad para asegurar una experiencia de usuario confiable y segura, así como en la protección de datos sensibles que se transmiten a través de Internet.

Las actividades detalladas en este documento abarcan desde el registro de un dominio gratuito utilizando servicios como DuckDNS, hasta la configuración y puesta en marcha de un servidor web con Internet Information Services (IIS) en un entorno Windows. Además, se aborda la configuración del router para permitir el acceso externo al servidor web y la implementación de HTTPS para garantizar la seguridad de las comunicaciones.

El enfoque práctico de estas actividades no solo refuerza el entendimiento teórico de los principios de redes y seguridad web, sino que también proporciona habilidades tangibles para manejar y asegurar infraestructuras web en escenarios reales. La implementación de estas tareas se documenta con capturas de pantalla y explicaciones detalladas, asegurando una comprensión completa del proceso y su relevancia en la protección de datos y la mejora de la experiencia del usuario.

Una curiosidad interesante sobre el uso de HTTPS es que, según un informe de Google, a partir de 2018, más del 70% del tráfico de Chrome en Android y Windows ya se realizaba a través de HTTPS. Esto refleja una tendencia creciente hacia la adopción de conexiones seguras en la web, subrayando la importancia de implementar HTTPS para cumplir con las expectativas de seguridad de los usuarios y de los motores de búsqueda.

## Actividad 1 - Registro de dominio en Duckdns

DuckDNS es un servicio de DNS dinámico gratuito que permite a los usuarios asociar un nombre de dominio fácil de recordar con la dirección IP dinámica de su red doméstica o de pequeños negocios. Esto es particularmente útil para acceder a servicios y dispositivos en tu red local, como cámaras de seguridad, servidores de archivos o sistemas domóticos, sin tener que recordar la dirección IP que cambia con frecuencia.

### Registro y Configuración:

Para la primera actividad, nos vamos a registrar en la página web de Duckdns y crear un nombre de dominio que en nuestro caso será `juliushacker88.duckdns.org`.



### Actualización de la IP:

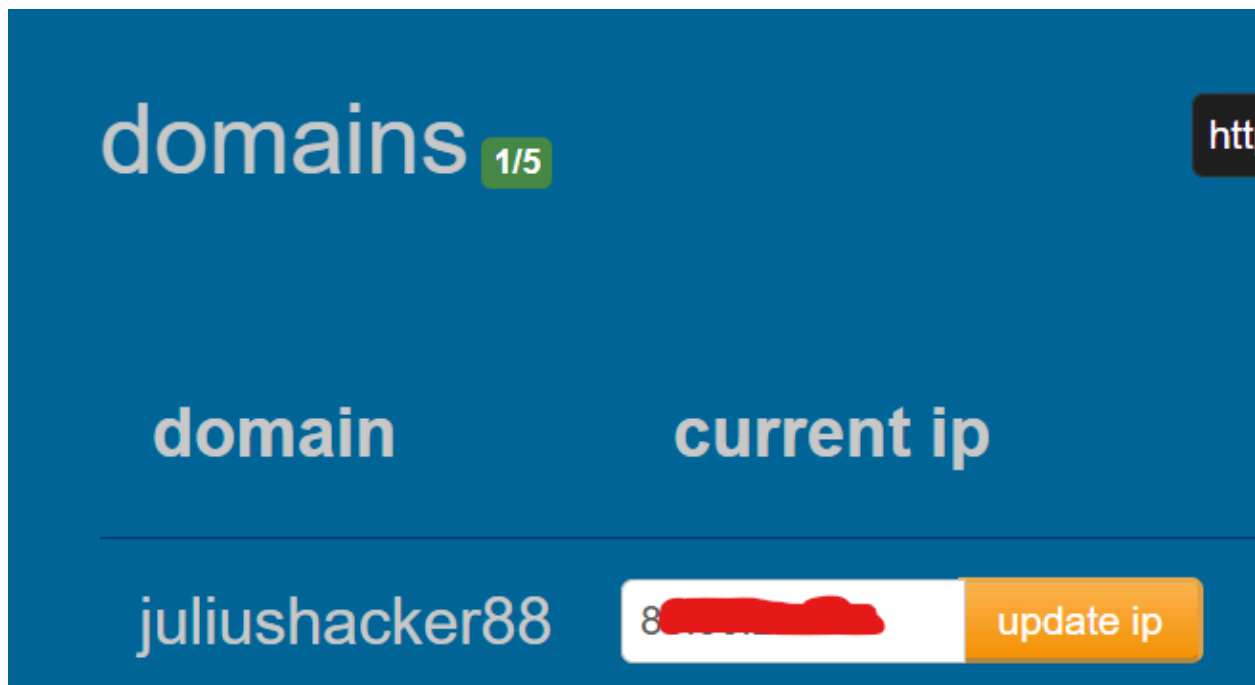
Debemos configurar un cliente de actualización de DuckDNS en nuestro router, servidor, o cualquier dispositivo que esté siempre encendido. Este cliente actualizará regularmente la IP asociada a nuestro subdominio con nuestra IP pública actual.

DuckDNS proporciona scripts y guías para diferentes sistemas operativos y dispositivos para facilitar esta configuración.

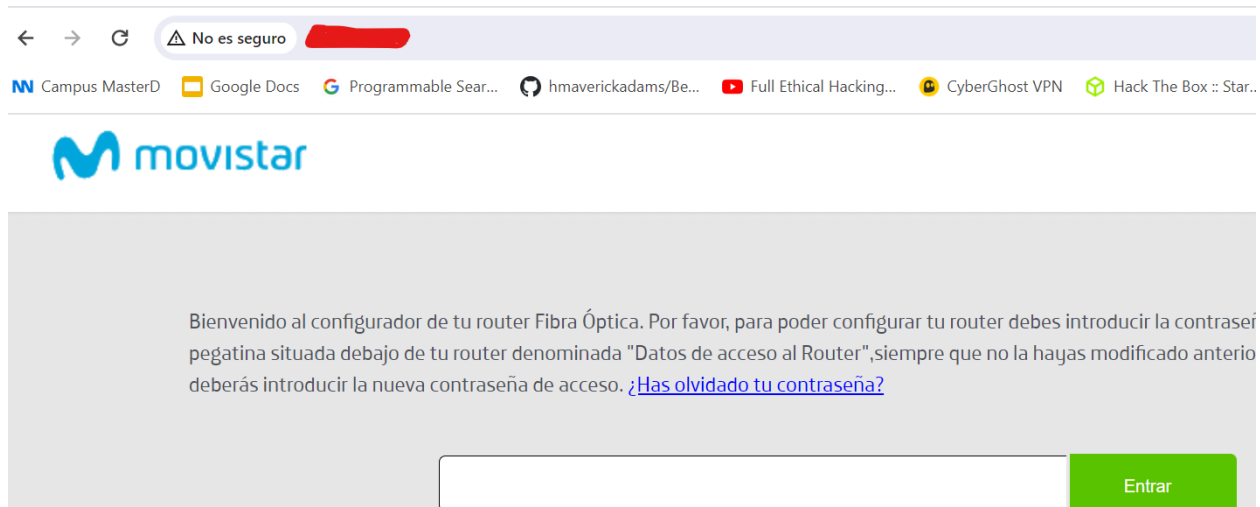
### Beneficios de DuckDNS

- **Gratuito:** No tiene costo y ofrece una forma sencilla de gestionar DNS dinámico.
- **Sencillo de configurar:** Ofrece guías y scripts para varios dispositivos y sistemas operativos.
- **Fiable:** A pesar de ser un servicio gratuito, DuckDNS es conocido por su fiabilidad en mantener los registros de DNS actualizados.

DuckDNS facilita la gestión de acceso remoto a redes y dispositivos con IP dinámica, proporcionando un subdominio constante que se actualiza automáticamente con tu IP pública.



Si probamos de acceder a la IP del dominio, podemos verificar que es nuestra IP pública, ya que en la siguiente imagen podemos observar que podríamos acceder a las configuraciones de nuestro router. Tener este acceso al router no es una buena práctica y puede generar vulnerabilidades, deberíamos cambiarlo para que no sea visible.



La siguiente forma de comprobar que el dominio está correctamente registrado, es por línea de comandos hacer un nslookup al dominio generado por Duckdns.

```
C:\Windows\System32>nslookup juliushacker88.duckdns.org
Servidor: 250.red-80-...-...staticip.rima-tde.net
Address: 80.100.100.100

Respuesta no autoritativa:
Nombre: juliushacker88.duckdns.org
Address: 80.100.100.100
```

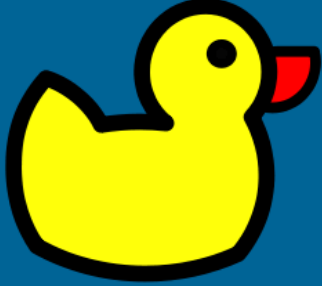
Nos devuelve que no es autoritativa lo que significa que no somos propietarios del host, el servidor DNS es externo.

El siguiente paso a seguir es configurar la actualización automática de nuestra IP. Para ello, en el menú de opciones de la web de DuckDNS, navegamos a "install" y seleccionamos la instalación correspondiente a nuestro sistema operativo. Activamos la opción adecuada y asociamos nuestro nombre de dominio con el token proporcionado. En nuestro caso, al usar Windows 10, seleccionamos "windows-gui" y configuramos el intervalo de tiempo para que la IP se actualice automáticamente según nuestras necesidades.



← → ↻ [www.duckdns.org/install.jsp](http://www.duckdns.org/install.jsp)

Duck DNS spec about why **install** faqs logout logged in with [julius.hacker88@gmail](#)



# Duck DNS

free dynamic DNS hosted on AWS

news: [login with Reddit is no more](#) - legal request  
support us: become a [Patreon](#)

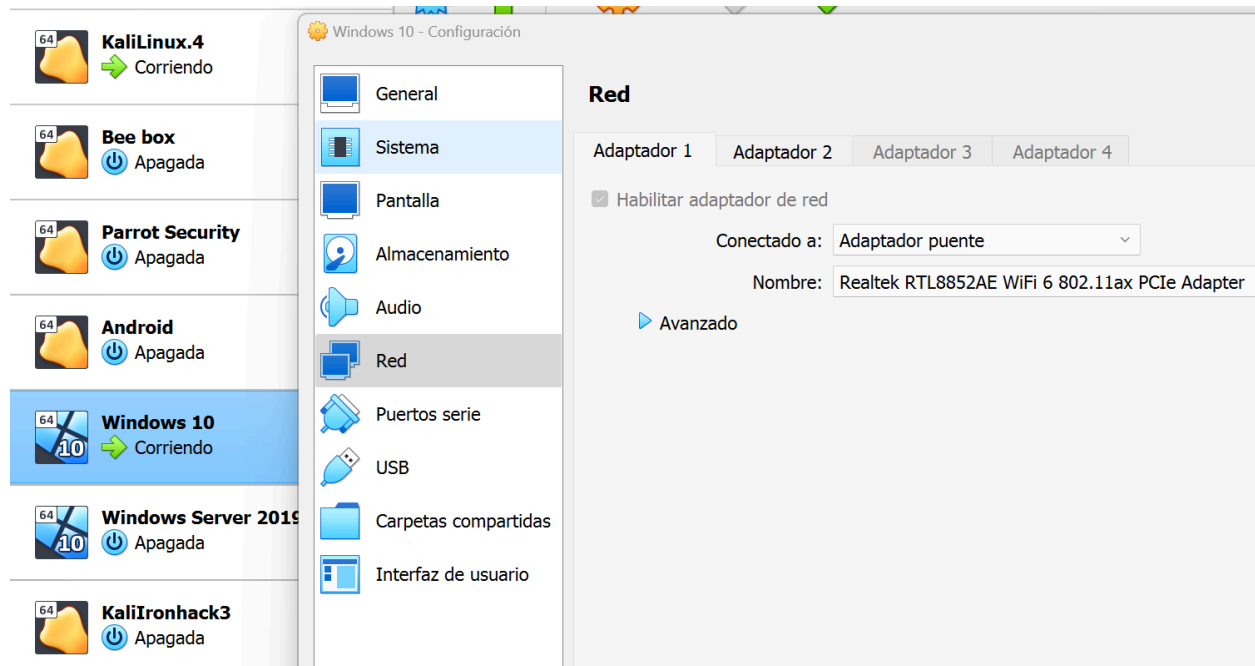
### Operating Systems

linux cron	linux bsd cron	linux netcat cron	linux GUI	DotNet Core Script	mono
<b>windows-gui</b>	windows-script	windows-powershell	windows-c#	osx	
osx-homebrew	osx IP Monitor	osx-ios RealDNS	android	pi	raspbmc
ec2					

### Routers

## Actividad 2 - Servidor web en Windows con Internet Information Services (IIS).

Comenzaremos esta actividad desde nuestra máquina virtual de Windows 10. Pondremos el adaptador de red en modo puente.



Ahora debemos configurar la red de esta máquina virtual para que esté en la misma red que nuestra máquina nativa. Para ello podemos ejecutar el comando ipconfig desde una terminal cmd en nuestra máquina nativa y veremos nuestra IP.

```
Adaptador de LAN inalámbrica Wi-Fi:
```

```
Sufijo DNS específico para la conexión. . . :  
Vínculo: dirección IPv6 local. . . : fe80::7523:9973:3473:ff18%7  
Dirección IPv4. . . . . : 192.168.1.37  
Máscara de subred . . . . . : 255.255.255.0  
Puerta de enlace predeterminada . . . . . : 192.168.1.1
```

Hacemos lo mismo en la máquina virtual.

```
C:\Windows\system32>ipconfig

Configuración IP de Windows

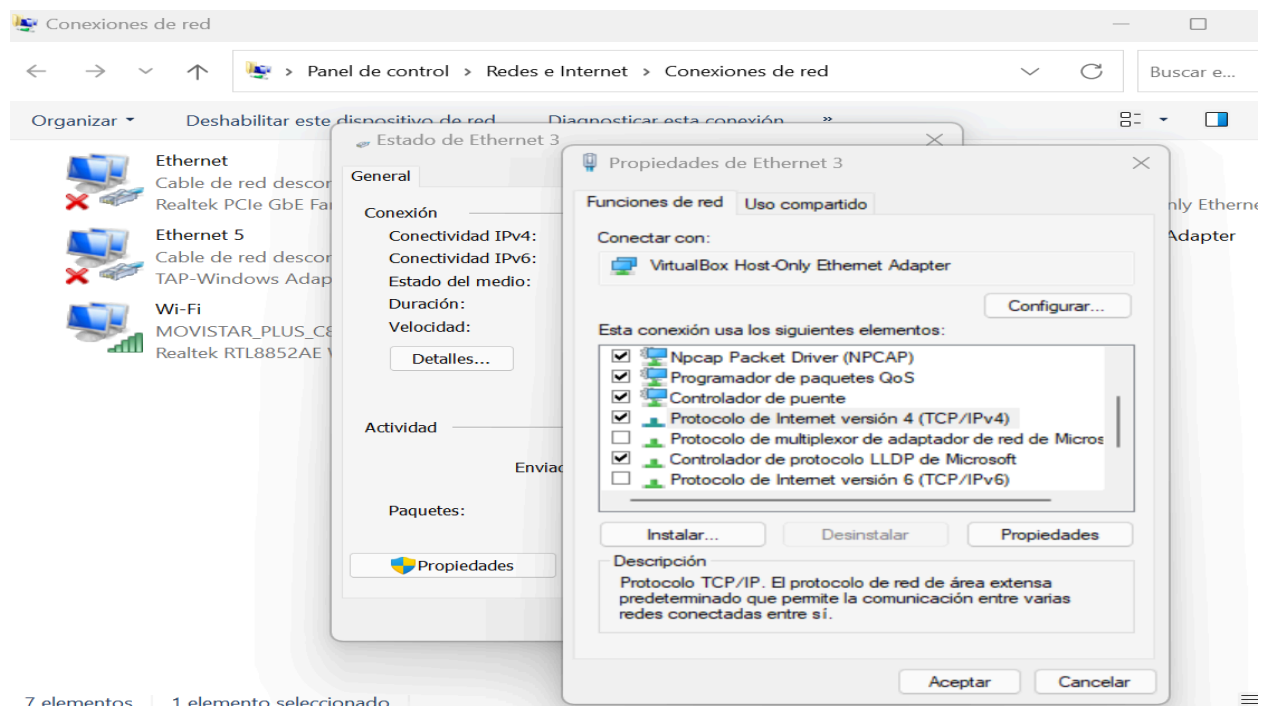
Adaptador de Ethernet LAN:

    Sufijo DNS específico para la conexión. . . :
    Vínculo: dirección IPv6 local. . . : fe80::4707:e92d:9f63:d139%10
    Dirección IPv4. . . . . : 10.0.2.30
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada . . . . . : 10.0.2.1

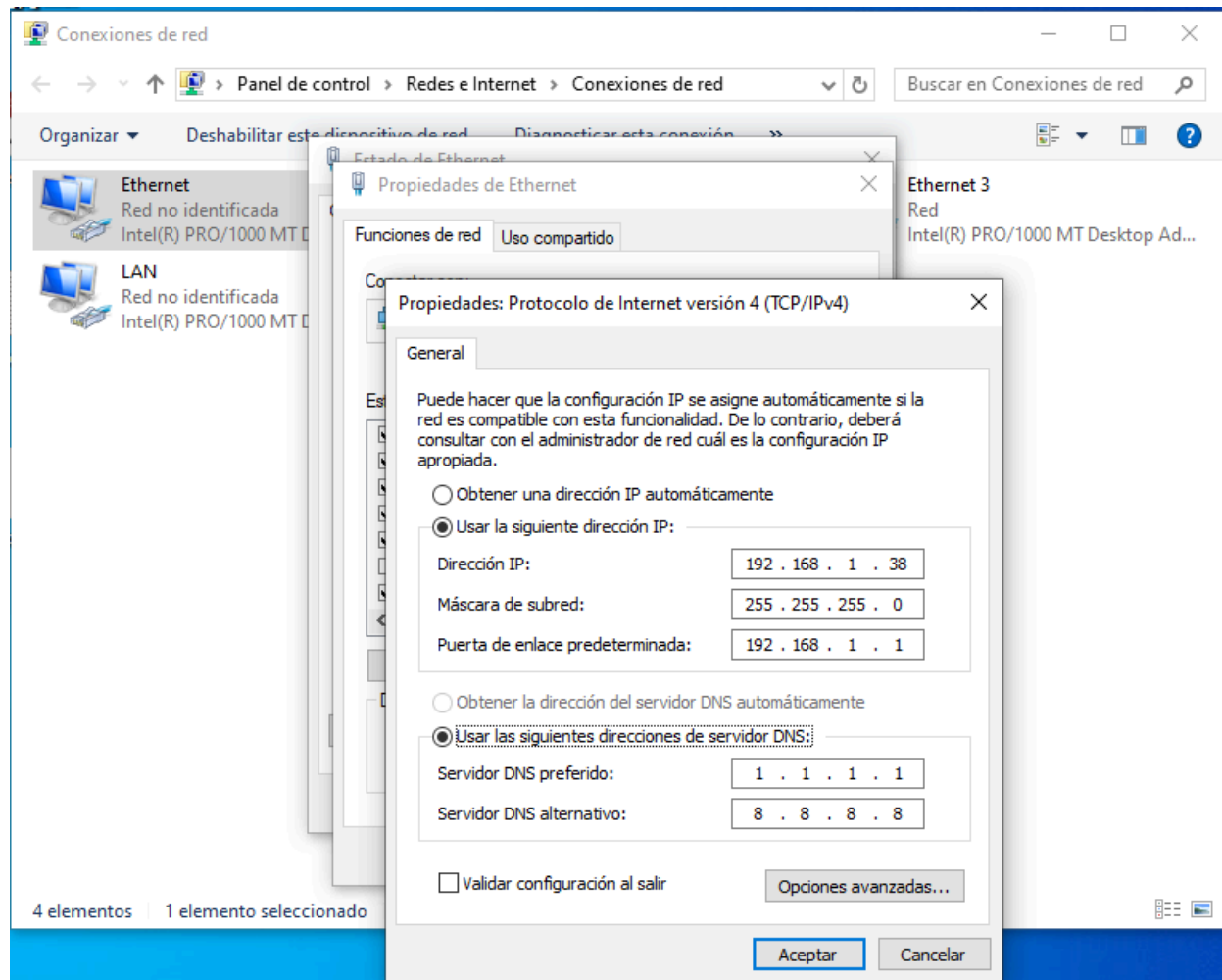
Adaptador de Ethernet Ethernet:

    Sufijo DNS específico para la conexión. . . :
    Vínculo: dirección IPv6 local. . . : fe80::3a03:b87b:e28a:c218%6
    Dirección IPv4. . . . . : 192.168.56.103
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada . . . . . : 192.168.10.100
```

Ahora modificaremos la IP para que estén en la misma red, para ello abrimos ncpa.cpl y vamos a propiedades de ethernet 3 y luego protocolo TCP/IPV4



Configuramos de esta manera.



## Instalación de IIS

Windows IIS (Internet Information Services) es un servidor web y una plataforma de servicios de aplicaciones creada por Microsoft. Está disponible en las versiones de servidor de Windows (como Windows Server) y en algunas versiones de Windows para escritorio (como Windows 10 y Windows 11 Pro). IIS permite a los administradores publicar información en la intranet, internet o en aplicaciones de web.

IIS funciona como un servidor web que recibe solicitudes HTTP y HTTPS de los usuarios y responde con páginas web, archivos o datos de aplicaciones web. Un cliente (navegador web) envía una solicitud HTTP o HTTPS al servidor IIS. Esta solicitud podría ser para una página web, un archivo, o una acción específica en una aplicación web. IIS recibe la solicitud y la pasa a uno de sus componentes para procesarla.

Dependiendo del tipo de solicitud, puede pasarla a:

**Módulos de IIS:** Estos son componentes que manejan aspectos específicos de la solicitud, como autenticación, caché, compresión, etc.

**ASP.NET:** Si la solicitud es para una aplicación ASP.NET, IIS la pasa al motor ASP.NET para su procesamiento.

**PHP/CGI:** Para aplicaciones PHP, IIS puede usar módulos CGI o FastCGI para manejar la solicitud.

**1. Respuesta al Cliente:**

- Después de procesar la solicitud, IIS genera una respuesta (como una página HTML o un archivo) y la envía de vuelta al cliente.

**2. Log y Monitoreo:**

- IIS también registra las solicitudes y respuestas en archivos de log, que se pueden usar para monitorear y analizar el tráfico del sitio web y el rendimiento del servidor.

## **Características Principales de IIS**

**1. Compatibilidad con Múltiples Protocolos:**

- Soporta HTTP, HTTPS, FTP, FTPS, SMTP y más.

**2. Módulos Extensibles:**

- Permite la instalación de módulos adicionales para extender las funcionalidades, como autenticación, autorización, caché, etc.

**3. Soporte para Aplicaciones Web:**

- Compatible con ASP.NET, PHP, Node.js y otros lenguajes y marcos de aplicaciones web.

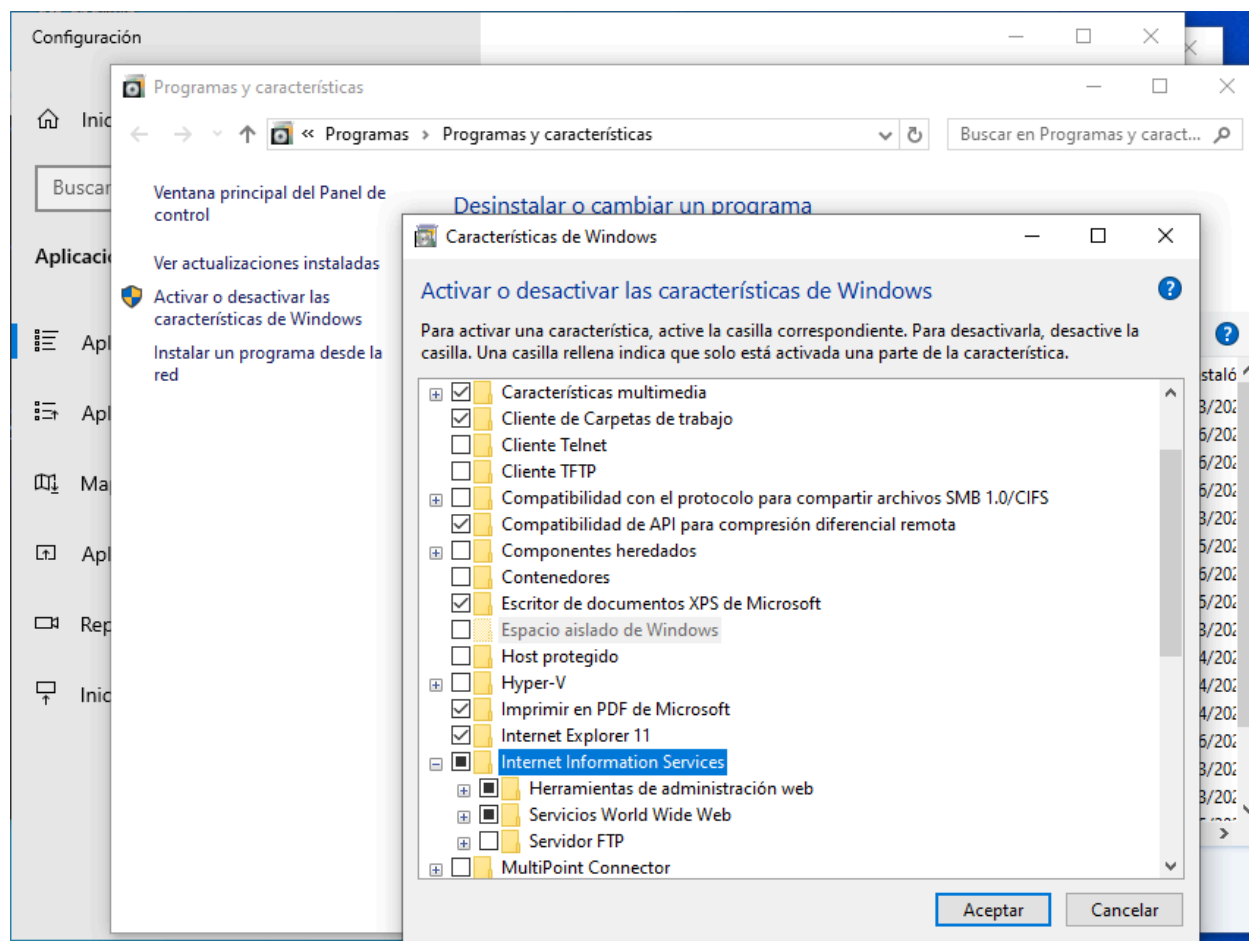
**4. Seguridad:**

- Proporciona características de seguridad como autenticación, autorización, filtrado de solicitudes, y soporte para SSL/TLS.

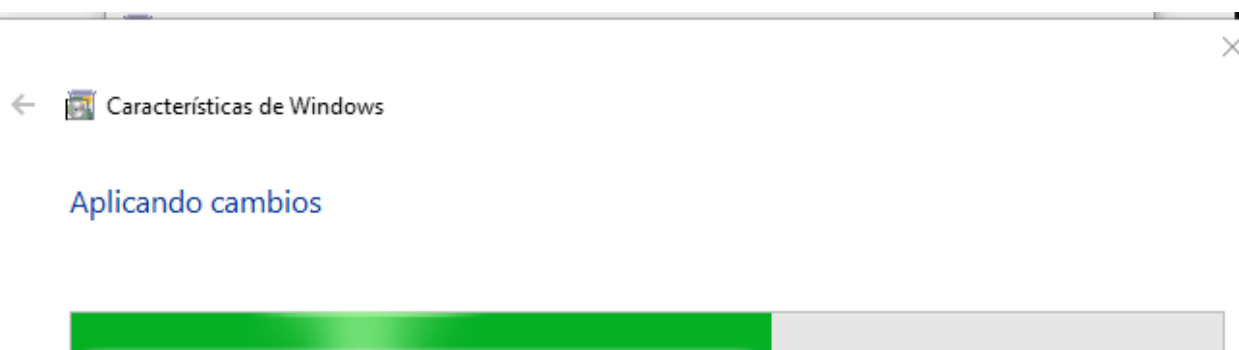
**5. Escalabilidad y Rendimiento:**

- Optimizado para manejar múltiples sitios web y aplicaciones en el mismo servidor, y puede escalar para soportar grandes volúmenes de tráfico.

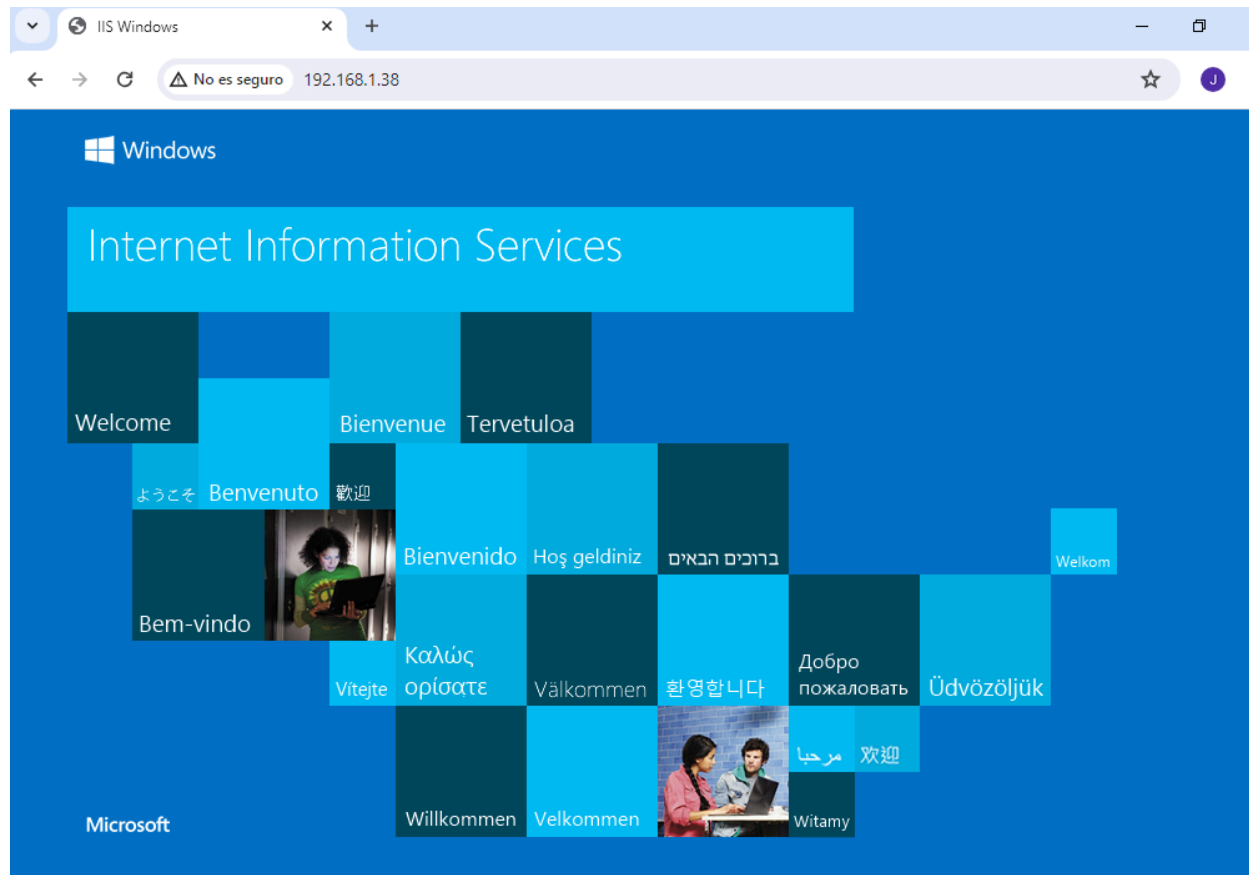
Para instalar este programa vamos a agregar o quitar programas > configuracion > programas y características > características de windows y tildamos Internet Information Services.



Se aplicarán los cambios.

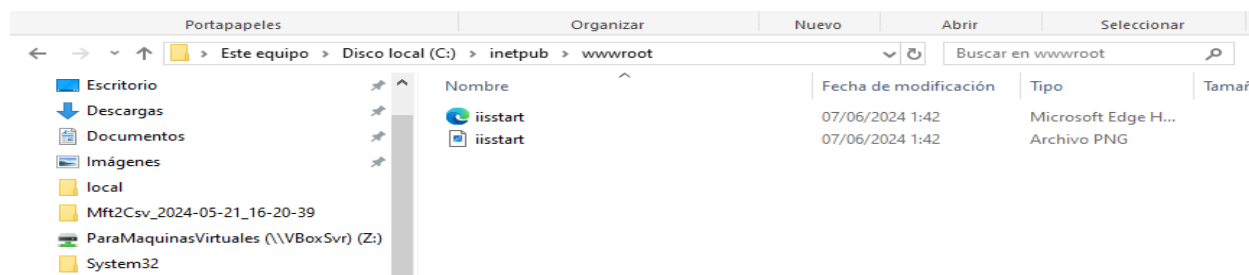


Comprobamos que funciona, abriendo un navegador y accediendo a nuestra IP.



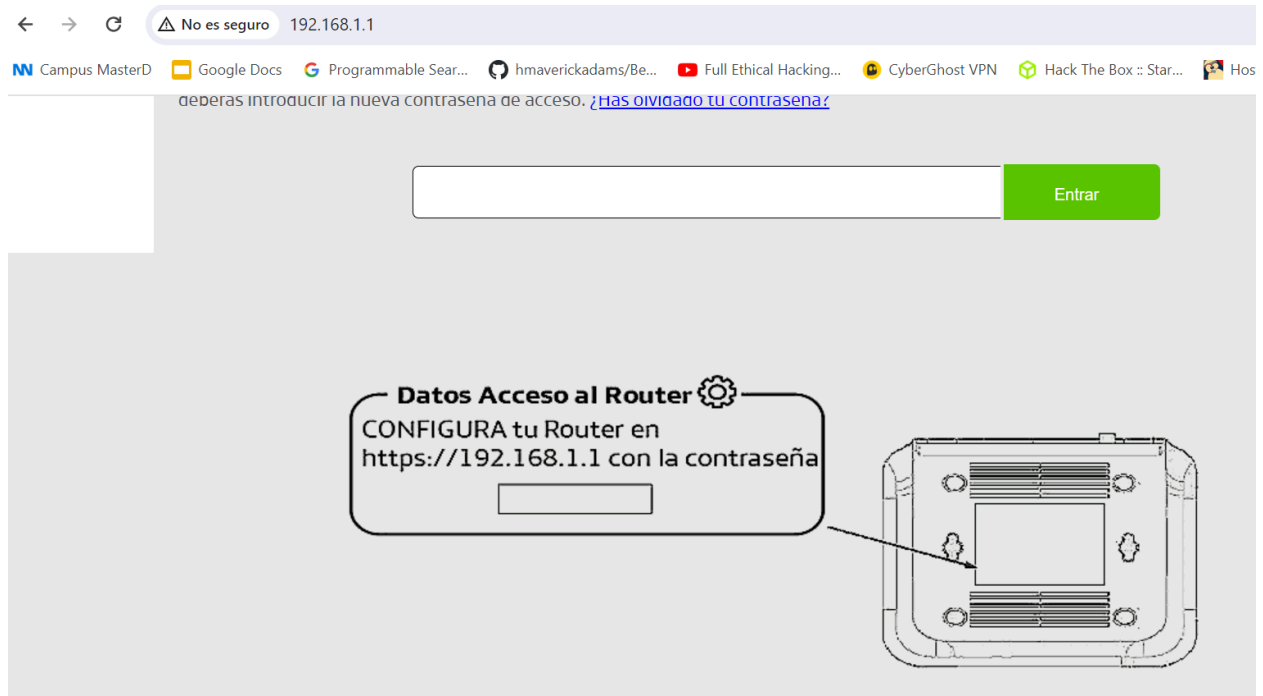
Se nos abrirá esta página web, esto quiere decir que está funcionando correctamente.

Al acceder desde la red local, notaremos que se ha creado automáticamente una carpeta llamada inetpub en la raíz de la unidad C. Para verificar que todo funciona correctamente, podemos ir a la subcarpeta wwwroot dentro de inetpub. Allí encontraremos dos archivos iisstart. Uno de ellos es un enlace que, al abrirlo, nos lleva a la página web como documento. Este es el lugar donde debemos subir los archivos de nuestra página web, ya que aquí es donde se aloja. Una vez completado este proceso, podemos confirmar que el servicio de página web está activado y funcionando perfectamente.



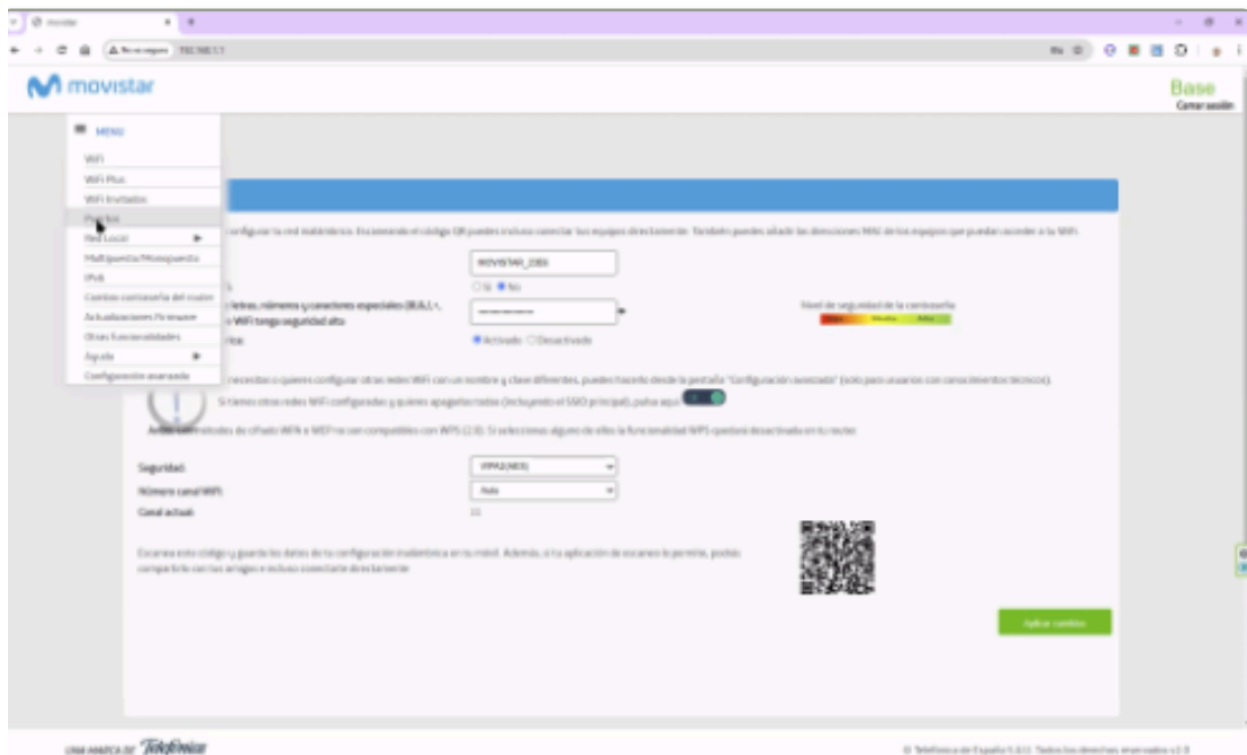
## Actividad 3 - Configuración del router

La siguiente actividad será configurar el router para permitir el acceso externo al servidor web. Para ello debemos abrir los puertos 80 y 443 en el router y redirigirlos a la IP del servidor IIS. Para acceder a nuestro router debemos entrar en nuestro navegador y acceder a la dirección 192.168.1.1.

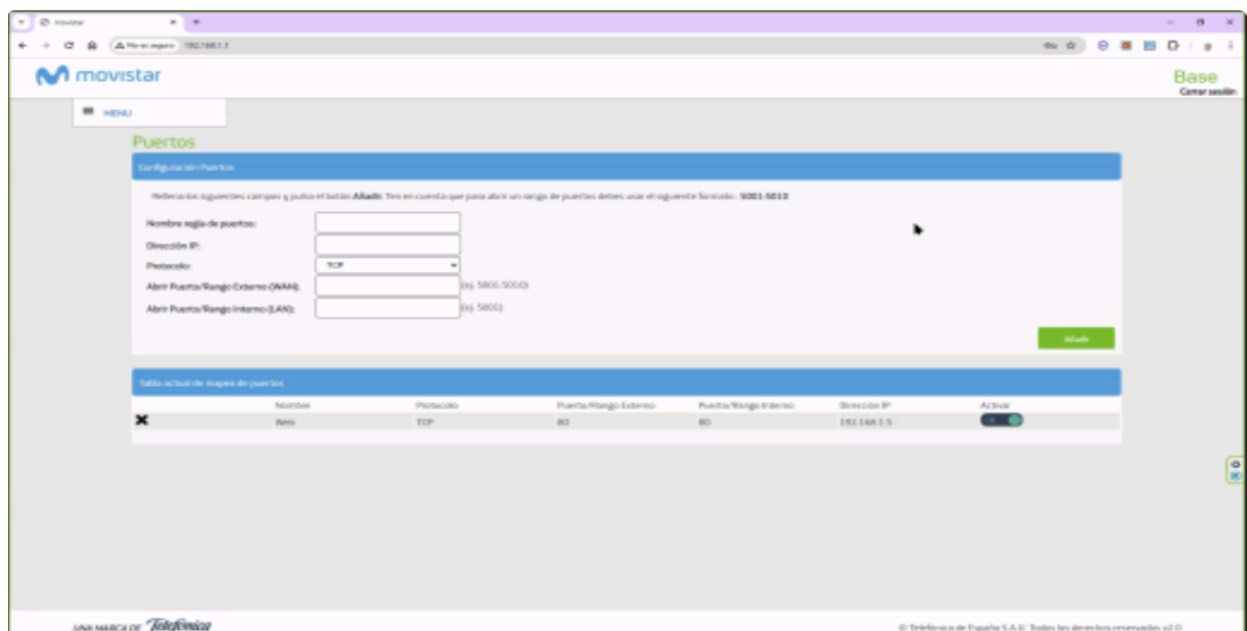




Luego vamos a la opción puertos dentro del menú desplegable.

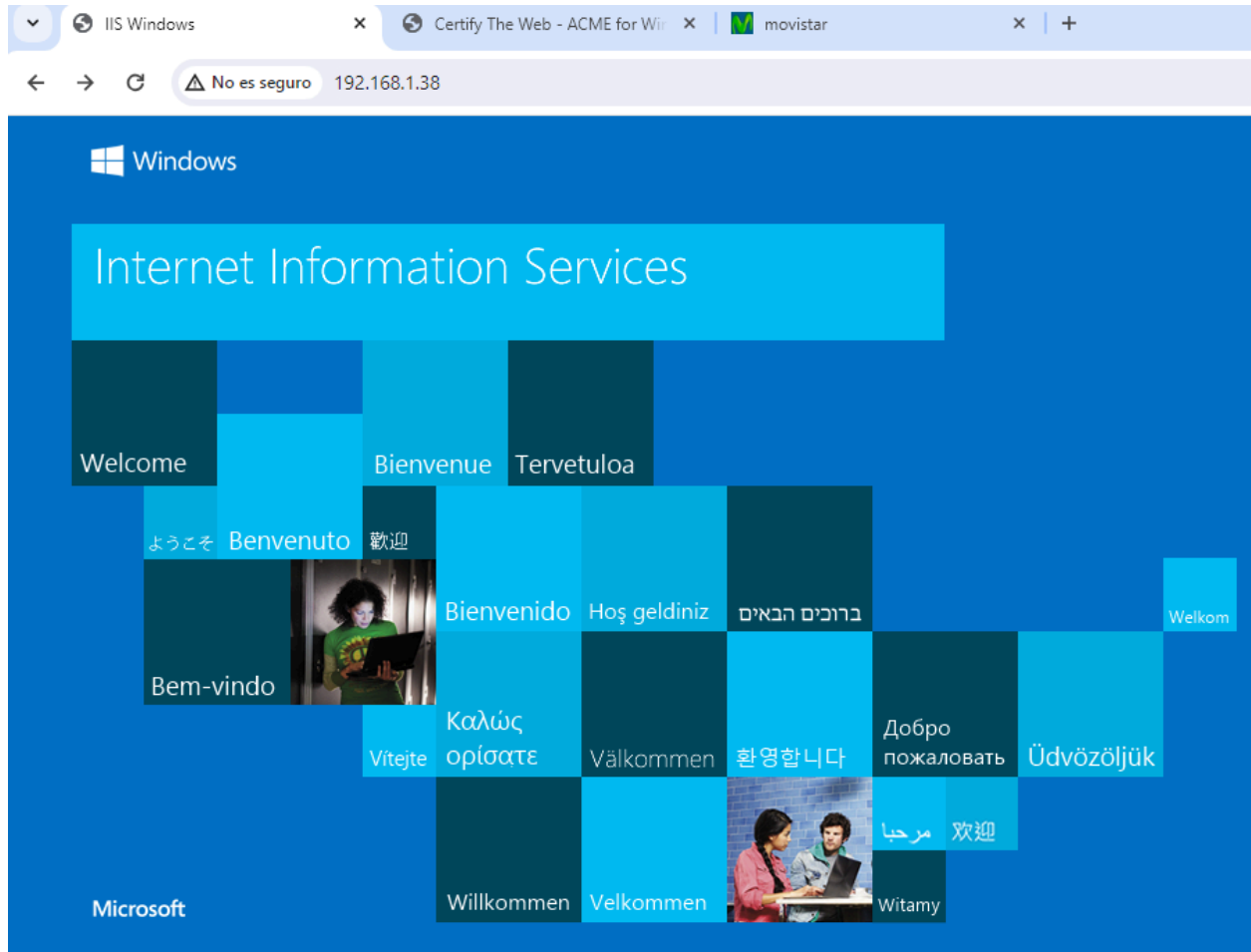


Vamos a crear 2 reglas, para puerto 80 y puerto 443. Ambas reglas con protocolo TCP y dirección IP 192.168.1.38. Después, configuramos cada una de ellas con su respectivo Puerto/Rango Externo e Interno, utilizando los puertos específicos 80 y 443.

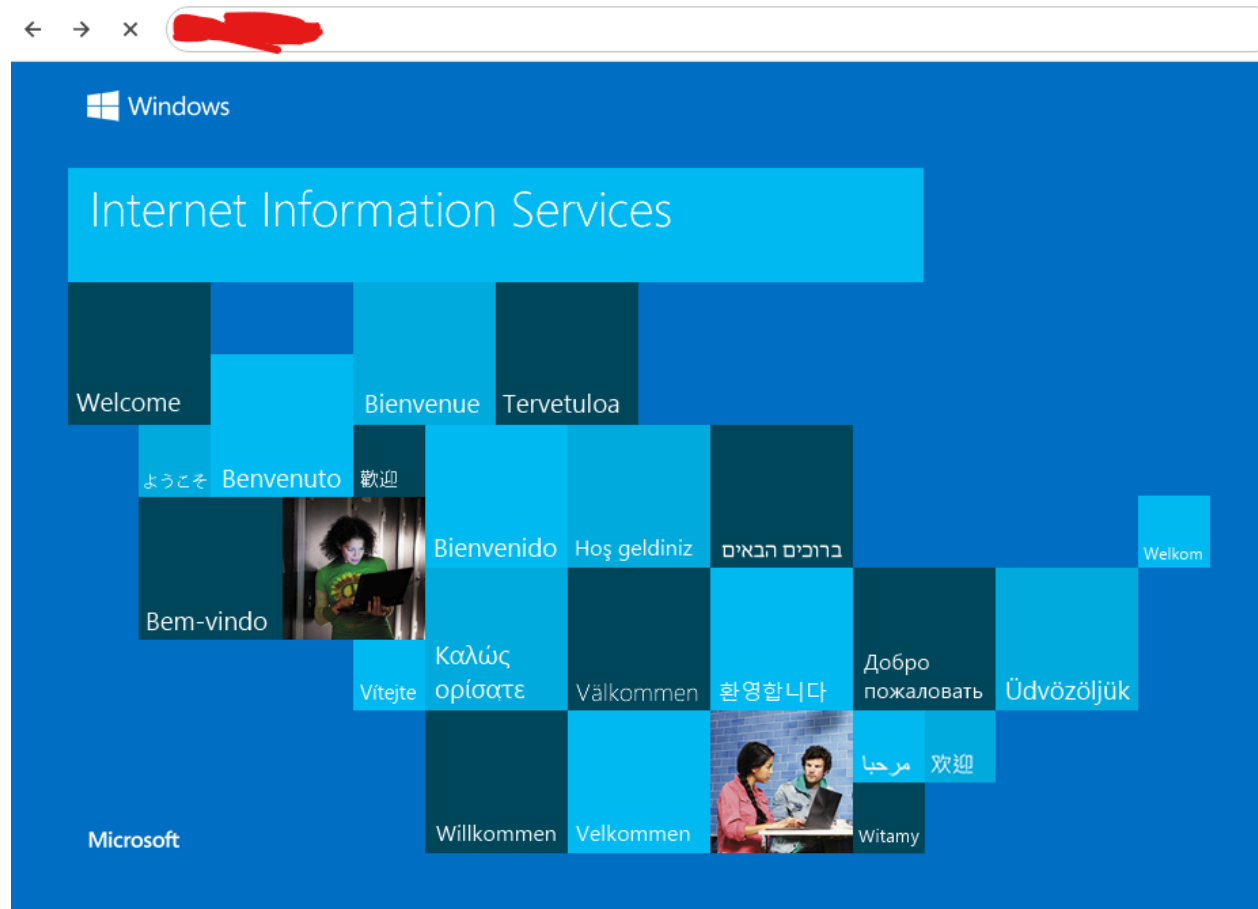


Ahora si queremos entrar a nuestro sitio web creado accediendo tanto por la ip local como por la ip pública, nos llevará correctamente a nuestro sitio.

IP Local:



IP pública:



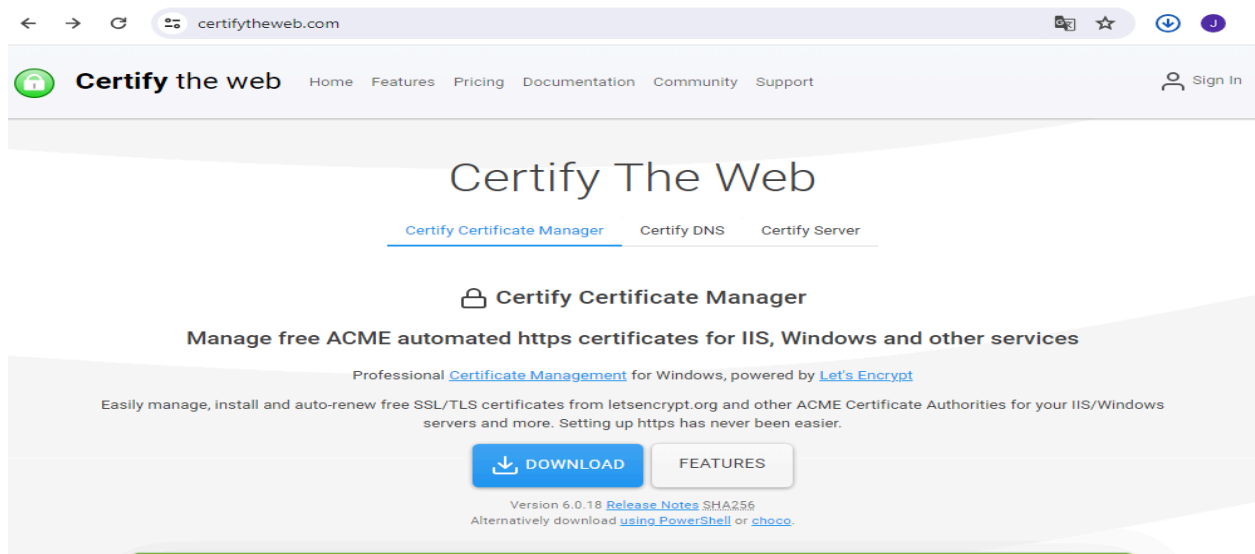
## Actividad 4 - Configuración de HTTPS en el servidor web

HTTPS (HyperText Transfer Protocol Secure) es una versión segura de HTTP, el protocolo utilizado para la comunicación entre navegadores web y servidores. HTTPS utiliza cifrado TLS (Transport Layer Security) para proteger los datos transmitidos, asegurando la confidencialidad e integridad de la información.

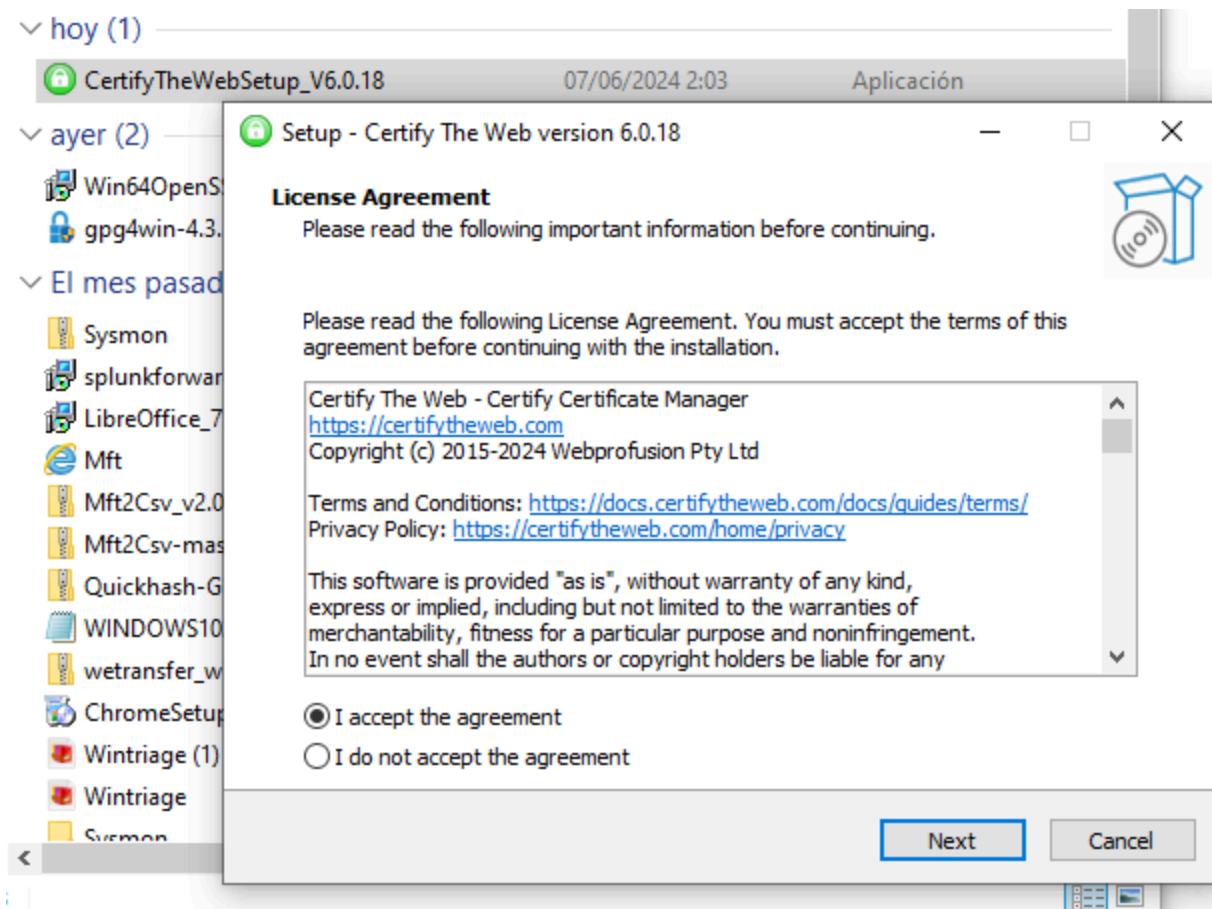
Esto le dará a nuestro servidor web muchas ventajas como:

1. **Seguridad:** HTTPS cifra los datos transmitidos, protegiendo información sensible (como contraseñas y datos personales) de ser interceptada por atacantes.
2. **Confianza:** Los usuarios confían más en sitios web que utilizan HTTPS, lo que puede aumentar la credibilidad y la confianza en tu sitio.
3. **SEO:** Los motores de búsqueda, como Google, favorecen los sitios web con HTTPS, mejorando potencialmente el posicionamiento en los resultados de búsqueda.
4. **Integridad de los datos:** HTTPS asegura que los datos no sean modificados durante la transmisión, garantizando que la información que llega al usuario es la misma que se envió.

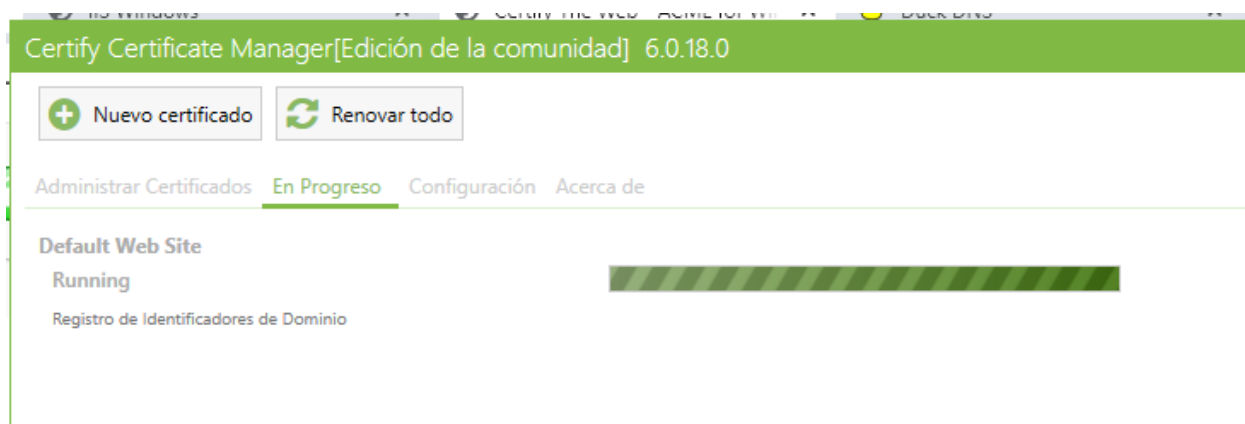
Para esta actividad vamos a utilizar la página web <https://certifytheweb.com/> y le damos a Download.



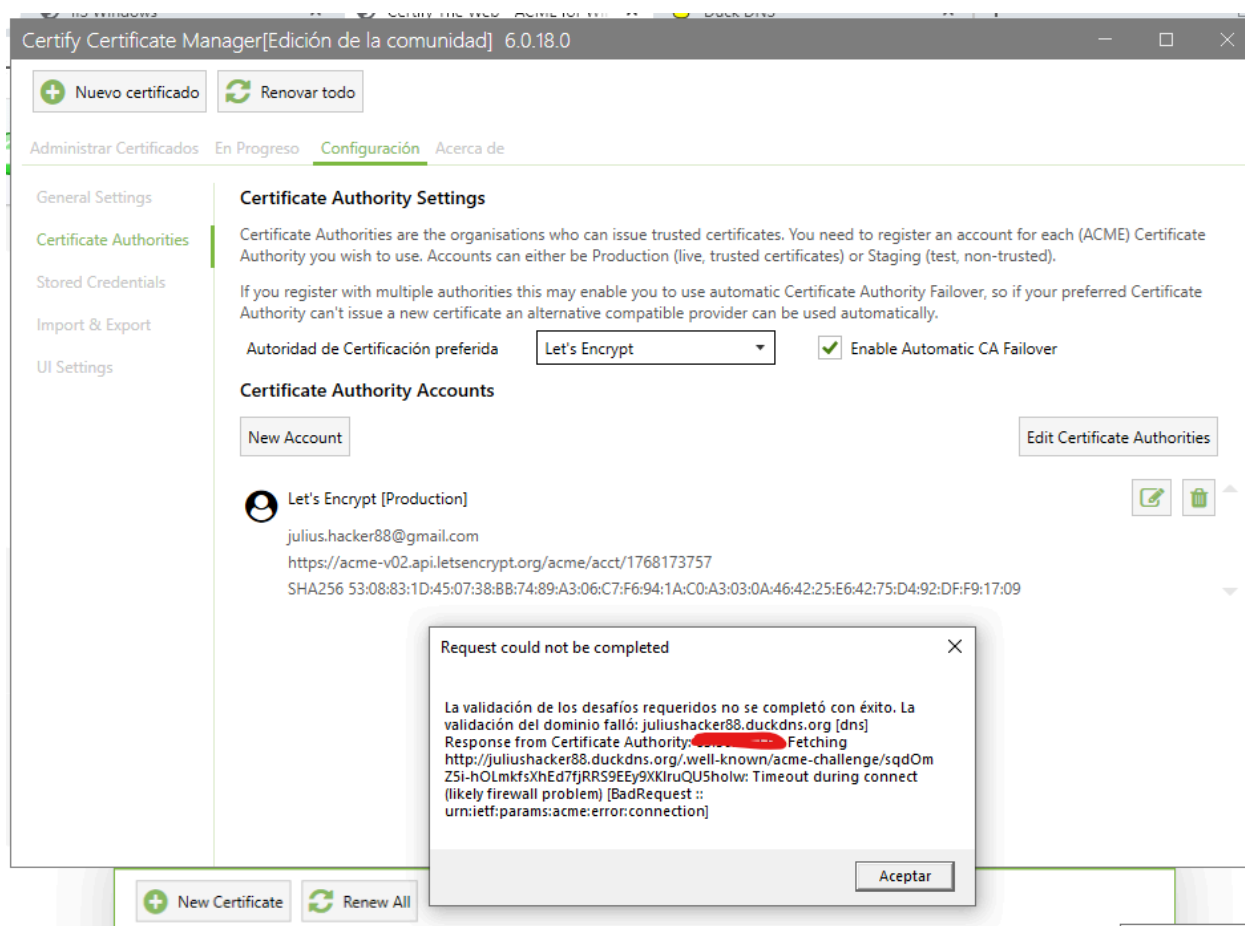
Ejecutamos el fichero descargado.



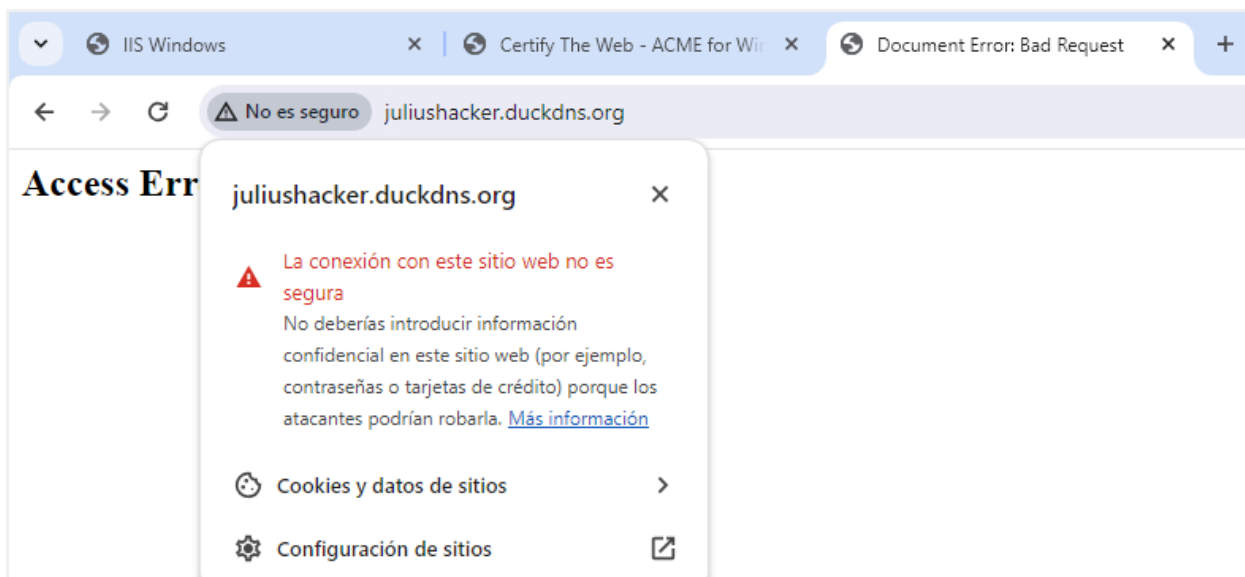
La instalación la dejamos la que viene por default. Y vamos a nuevo certificado



Ahora debemos configurar IIS para utilizar HTTPS con el certificado SSL. Para ello vamos a configuración > Certificados authorities > y podemos ver las características.



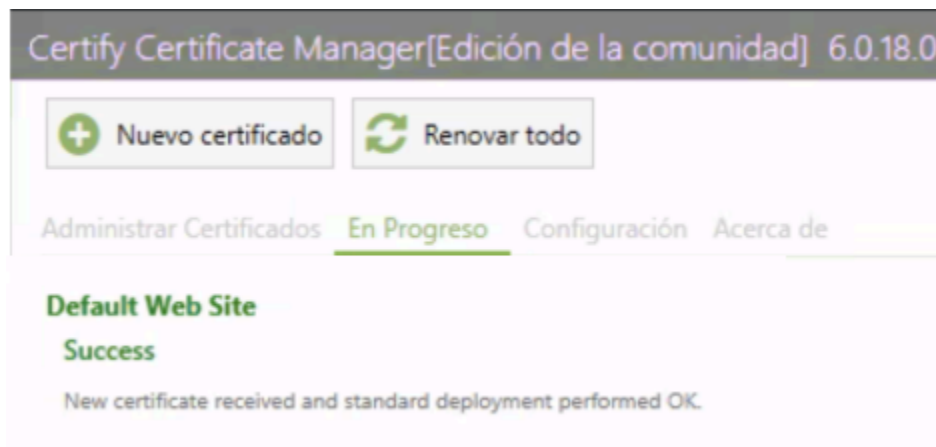
Mientras esperábamos el proceso para generar nuestro certificado nos apareció este error. Intentamos acceder nuevamente a nuestro dominio y tenemos un nuevo error.



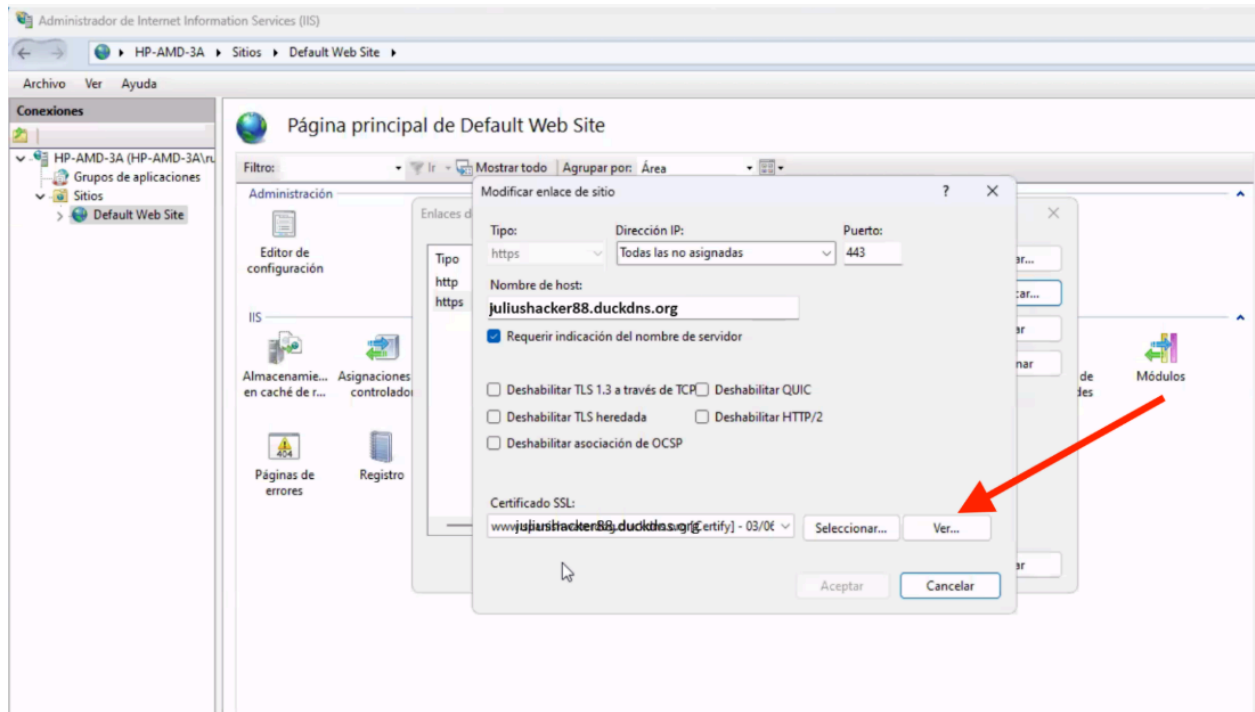
Volvemos a realizar el proceso reseteando el ordenador y el servidor web.



Podemos ver que esta vez funcionó correctamente.

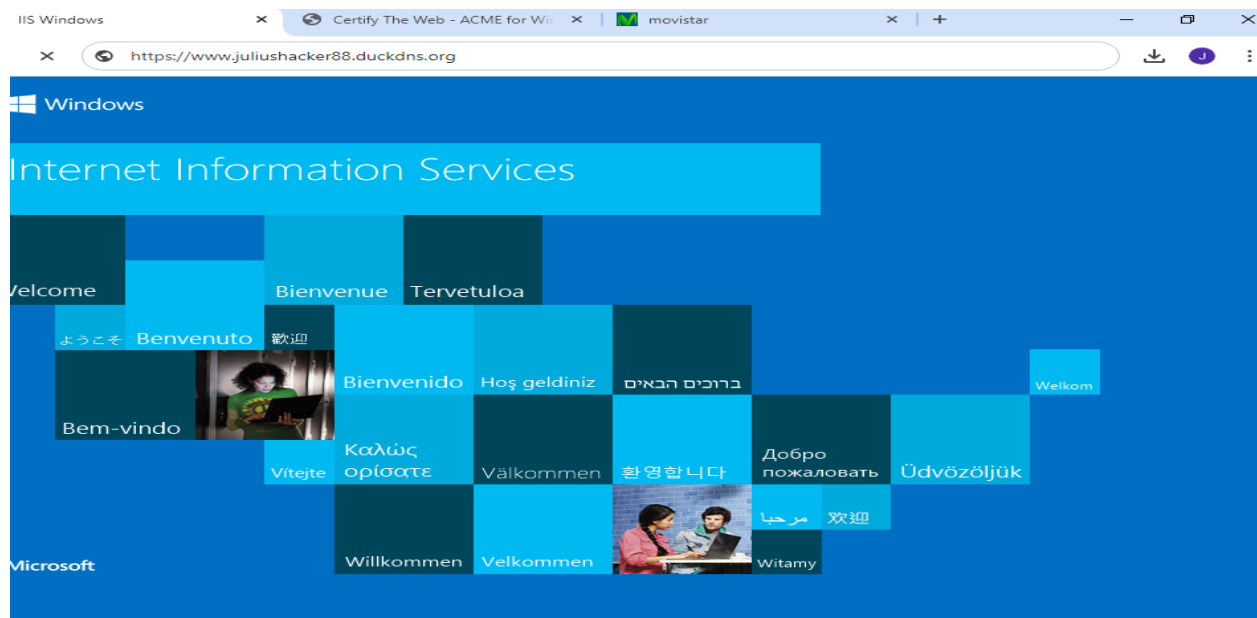


Una vez creado correctamente el certificado, podemos verificar en internet services IIS que está incorporado para nuestro sitio web.





Con el certificado generado, podemos acceder nuevamente a nuestro servidor y veremos que la web es ahora segura, pudiendo verificar el certificado que lo confirma.



## Visor de certificados:

General

Detalles

### Emitido para

Nombre común	www.ironpug.duckdns.org
Organización (O)	<No forma parte del certificado>
Unidad organizativa (UO)	<No forma parte del certificado>

### Emitido por

Nombre común	R3
Organización (O)	Let's Encrypt
Unidad organizativa (UO)	<No forma parte del certificado>

### Período de validez

Emitido el	lunes, 3 de junio de 2024, 12:18:51
Fecha de expiración	domingo, 1 de septiembre de 2024, 12:18:50

### Huellas digitales de SHA-256

Certificado	67afb2df0b2b52f8bd8f77a6ca116d86cbe21c616319192b016e a70b721e971d
Clave pública	5e9583f974660b3db497c64413b023d6bd098899b0655825fb 5871b41f34f927

## Actividad 5 - Importancia de certificados web y beneficios de utilizar HTTPS

1. Justifica la necesidad de certificar el sitio web, explicando los beneficios que conlleva en cuanto a seguridad para la empresa y los usuarios.

Importancia de Certificar el Sitio Web:

### Seguridad de la Información:

- **Confidencialidad:** La certificación SSL/TLS cifra los datos transmitidos entre el servidor y el cliente, lo que impide que terceros intercepten o accedan a información sensible, como contraseñas, datos personales y números de tarjetas de crédito.
- **Integridad:** Asegura que los datos no sean alterados durante la transmisión. Cualquier intento de modificar los datos sería detectado.
- **Autenticidad:** Un certificado SSL/TLS valida la identidad del sitio web, asegurando a los usuarios que están comunicándose con el sitio legítimo y no con un impostor.

### Confianza del Usuario:

- **Indicadores de Seguridad:** Los navegadores muestran un candado verde y usan "https://" en la URL para indicar que la conexión es segura. Esto proporciona una señal visual clara a los usuarios de que el sitio es confiable.
- **Aumento de la Credibilidad:** Un sitio web con un certificado SSL/TLS es visto como más profesional y confiable, lo que puede aumentar la confianza de los clientes y visitantes.

### Mejora del SEO:

- **Posicionamiento en Búscadores:** Google y otros motores de búsqueda dan preferencia a los sitios web seguros (HTTPS) en sus resultados de búsqueda, lo que puede mejorar significativamente el tráfico orgánico y la visibilidad del sitio.

### Cumplimiento Normativo:

- **Regulaciones de Protección de Datos:** Muchas normativas y leyes de protección de datos (como GDPR en Europa) requieren que las empresas protejan la información personal de los usuarios. El uso de HTTPS es un paso crucial para cumplir con estas regulaciones.

## Reducción del Riesgo de Ataques:

- **Prevención de Ataques de Phishing:** Un certificado SSL/TLS ayuda a prevenir ataques de phishing al confirmar la autenticidad del sitio web, dificultando que los atacantes se hagan pasar por el sitio legítimo.
- **Protección contra Ataques de Hombre en el Medio (MitM):** El cifrado TLS protege contra ataques en los que un tercero intercepta y potencialmente altera la comunicación entre el servidor y el cliente.

2. Qué riesgos has conseguido mitigar mediante la implementación de HTTPS. ¿Un usuario normal se sentiría seguro? ¿Tú como usuario avanzado te sentirías seguro visitando la web?

Riesgos Mitigados mediante HTTPS:

### Intercepción de Datos (Eavesdropping):

- **Mitigación:** HTTPS cifra los datos transmitidos, lo que impide que un atacante pueda leer la información mientras viaja por la red.
- **Impacto:** Esto protege datos sensibles como credenciales de inicio de sesión, información personal y detalles de pago.

### Manipulación de Datos:

- **Mitigación:** HTTPS asegura la integridad de los datos durante la transmisión, impidiendo que los datos sean modificados sin ser detectados.
- **Impacto:** Protege contra ataques que intentan alterar los datos intercambiados entre el cliente y el servidor.

### Suplantación de Sitios Web (Phishing):

- **Mitigación:** Los certificados SSL/TLS validan la autenticidad del sitio web, dificultando que los atacantes se hagan pasar por el sitio legítimo.
- **Impacto:** Reduce el riesgo de que los usuarios sean engañados para que ingresen información sensible en sitios web falsificados.

### Ataques de Hombre en el Medio (MitM):

- **Mitigación:** HTTPS protege contra MitM al cifrar la comunicación entre el cliente y el servidor.
- **Impacto:** Asegura que la información no pueda ser interceptada y alterada por un atacante que se encuentra en medio de la comunicación.

## Sensación de Seguridad para el Usuario

### Usuario Normal:

- **Sensación de Seguridad:** Un usuario promedio se sentirá más seguro al ver el candado verde y el "https://" en la URL. Estos indicadores de seguridad son ampliamente reconocidos y dan confianza de que la conexión es segura.
- **Confianza:** La mayoría de los usuarios confían en estos indicadores visuales y, como resultado, estarán más dispuestos a interactuar y proporcionar información sensible en el sitio.

### Usuario Avanzado:

- **Sensación de Seguridad:** Un usuario avanzado también se sentirá más seguro visitando un sitio web con HTTPS, pero evaluará otros factores adicionales como la validez y la autenticidad del certificado SSL/TLS, la reputación de la entidad certificadora (CA) y la implementación de otras medidas de seguridad en el sitio.
- **Confianza:** Además de HTTPS, un usuario avanzado buscará prácticas de seguridad adicionales, como el uso de HSTS (HTTP Strict Transport Security), configuraciones adecuadas de seguridad en los headers HTTP, y la ausencia de vulnerabilidades comunes en la aplicación web.

## Conclusiones

Este trabajo ha proporcionado una experiencia práctica y detallada en la gestión de dominios, configuración de servidores web y la implementación de medidas de seguridad, centrándose especialmente en la adopción de HTTPS. A través de una serie de actividades estructuradas, hemos logrado alcanzar los siguientes objetivos:

### 1. Registro de Dominio y Configuración DNS:

- Seleccionamos y registramos un dominio gratuito utilizando DuckDNS, aprendiendo a asociarlo con la IP pública de nuestra red y verificando la resolución DNS. Este proceso nos mostró la importancia de la gestión de DNS dinámico y cómo asegurar la correcta configuración para garantizar la accesibilidad del dominio.

### 2. Instalación y Configuración de IIS:

- Instalamos y configuramos Internet Information Services (IIS) en un servidor Windows, comprobando su funcionamiento desde la red local y desde Internet. Esta actividad nos familiariza con el proceso de configuración de un servidor web y destacó la importancia de la conectividad y accesibilidad para garantizar la disponibilidad del sitio.

### 3. Configuración del Router para Acceso Externo:

- Abrimos los puertos 80 y 443 en el router y los redirigimos a la IP del servidor IIS, permitiendo el acceso externo al servidor web. Este paso demostró la necesidad de configurar adecuadamente la infraestructura de red para permitir el acceso remoto de manera segura.

### 4. Implementación de HTTPS y Certificados SSL:

- Utilizamos herramientas como "Certify the Web" para obtener un certificado SSL y configurar IIS para utilizar HTTPS. Aunque enfrentamos desafíos técnicos durante este proceso, como errores en la generación del certificado, logramos resolverlos y completar la implementación con éxito.

## **5. Importancia de certificar el sitio web y beneficios de HTTPS:**

- Exploramos la importancia de certificar un sitio web y los beneficios asociados, como la seguridad de la información, la confianza del usuario, la mejora del SEO y el cumplimiento normativo. También identificamos los riesgos mitigados mediante la implementación de HTTPS y cómo tanto los usuarios normales como los avanzados se benefician de esta seguridad adicional.

Esta práctica no solo nos proporcionó habilidades técnicas en la configuración de infraestructuras web y la implementación de medidas de seguridad, sino que también nos enseñó valiosas lecciones sobre la resolución de problemas y la importancia de garantizar la seguridad y la confiabilidad de las comunicaciones en línea. Los obstáculos encontrados durante el proceso nos brindaron oportunidades para aprender y mejorar, preparándonos mejor para enfrentar desafíos similares en el futuro y fortaleciendo nuestra comprensión de los principios fundamentales de la seguridad web y la gestión de infraestructuras en línea.