EXAMEN PRÁCTICO

Módulo formativo: Sistemas seguros de acceso y transmisión de datos

Certificado de profesionalidad: Seguridad Informática

Examen práctico sobre la creación de un dominio, configuración del router para tener acceso externo y obtención de certificados SSL/HTTPS

Diego Mucci

07/06/2024

CONTENIDO

ENUNCIADOS 2

ACTIVIDAD 1 4

Objetivo: Registra un dominio gratuito y comprobar el registro DNS. 4

ACTIVIDAD 2 7

Objetivo: Instala y configura un servidor web en Windows (alternativamente en Linux) utilizando Internet Information Services (IIS). 7

ACTIVIDAD 3 12

Objetivo: Configura el router para permitir el acceso externo al servidor web. 12

ACTIVIDAD 4 16

Objetivo: Configura HTTPS en el servidor web. 16

ACTIVIDAD 5 22

Objetivo: Explica la importancia de certificar el sitio web y los beneficios de utilizar HTTPS. 22

ENUNCIADOS

Actividad 1 (2 puntos)

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.

Actividad 2 (2 puntos)

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.

Actividad 3 (2 puntos)

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.

Actividad 4 (2 puntos)

Objetivo: Configura 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.

Actividad 5 (2 puntos)

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?

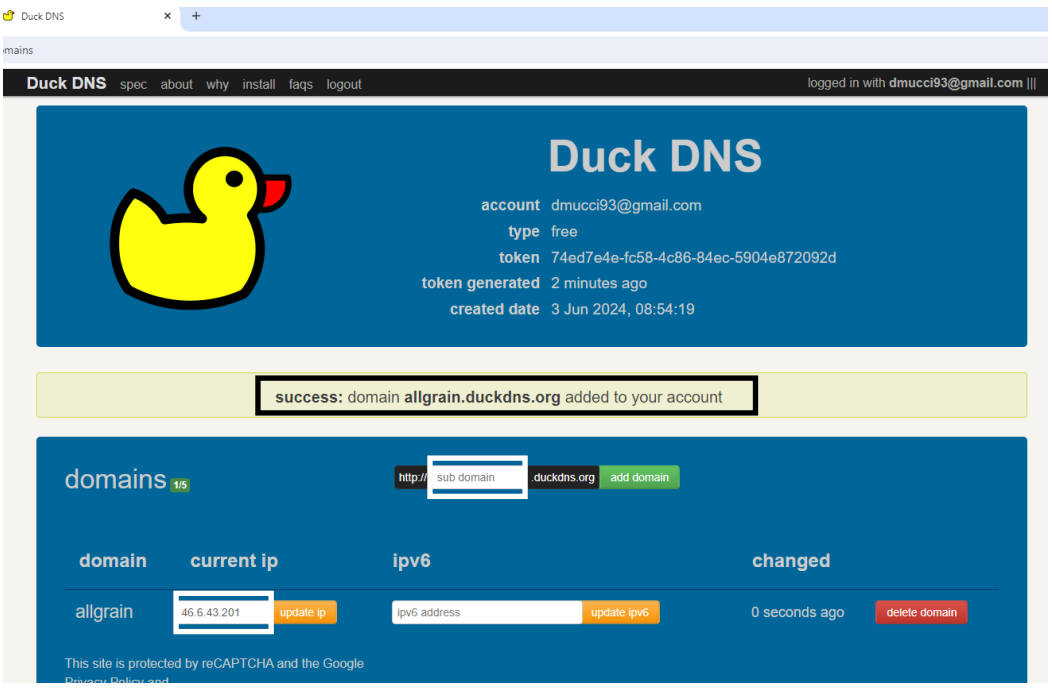
ACTIVIDAD 1 (2 puntos)

Objetivo: Registra un dominio gratuito y comprobar el registro DNS.

Hemos seleccionado Duck DNS como proveedor de registro de dominio de manera gratuita. Para poder hacer uso de él, debemos registrarnos. Una vez creada la cuenta, se nos proporcionará un token, el cual es crucial para la seguridad y el funcionamiento adecuado del servicio Duck DNS. Permite la autenticación de solicitudes de actualización de IP, asegurando que solo usuarios y dispositivos autorizados puedan modificar la configuración del dominio.

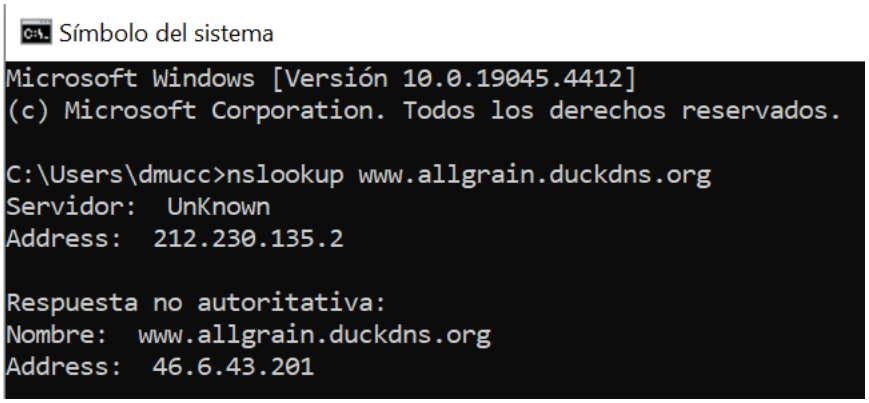
Registraremos el nombre del dominio escribiendo el nombre que le queramos dar a nuestro sitio web en el campo donde dice *sub domain* y después presionamos en *add domain*. ~~Siempre y cuando usemos la versión de pago, aparecerá *duckdns.org* después de nuestro sub dominio.~~

Si ese nombre de dominio no está en uso, nos aparecerá un mensaje satisfactorio de la creación. Más abajo nos aparecerá nuestra IP dinámica asociada a nuestro nombre de dominio:



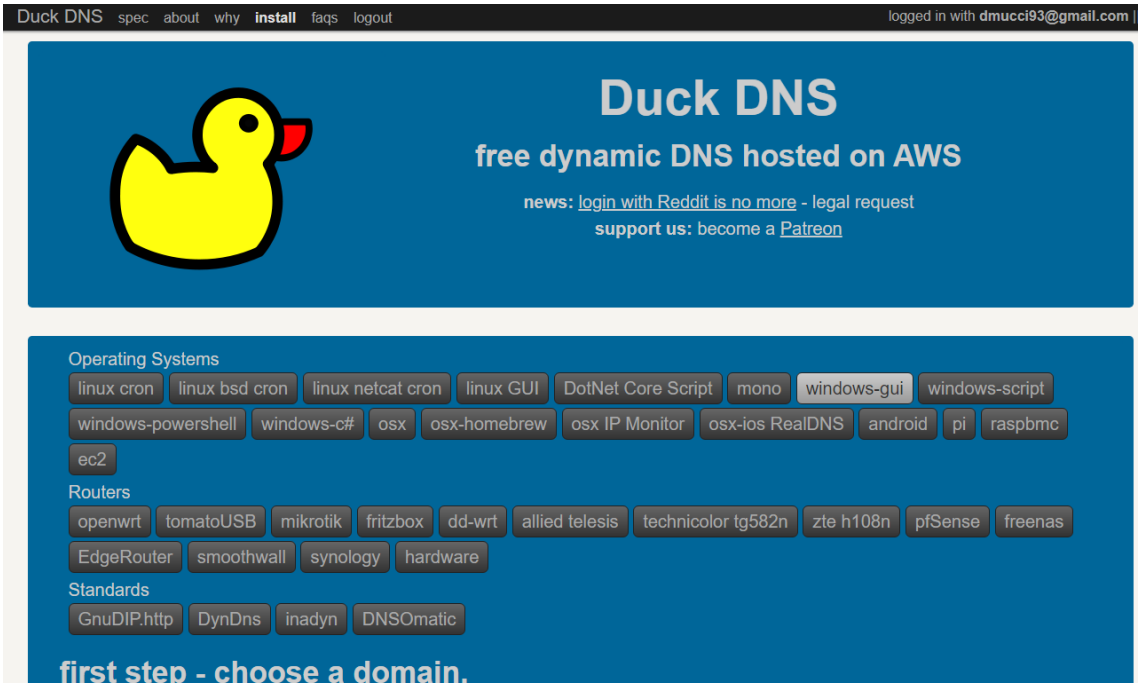
El registro con este proveedor de servicios es inmediato, es una de las ventajas que tiene, ya que normalmente se debe esperar unas 48hs para tener disponible el dominio.

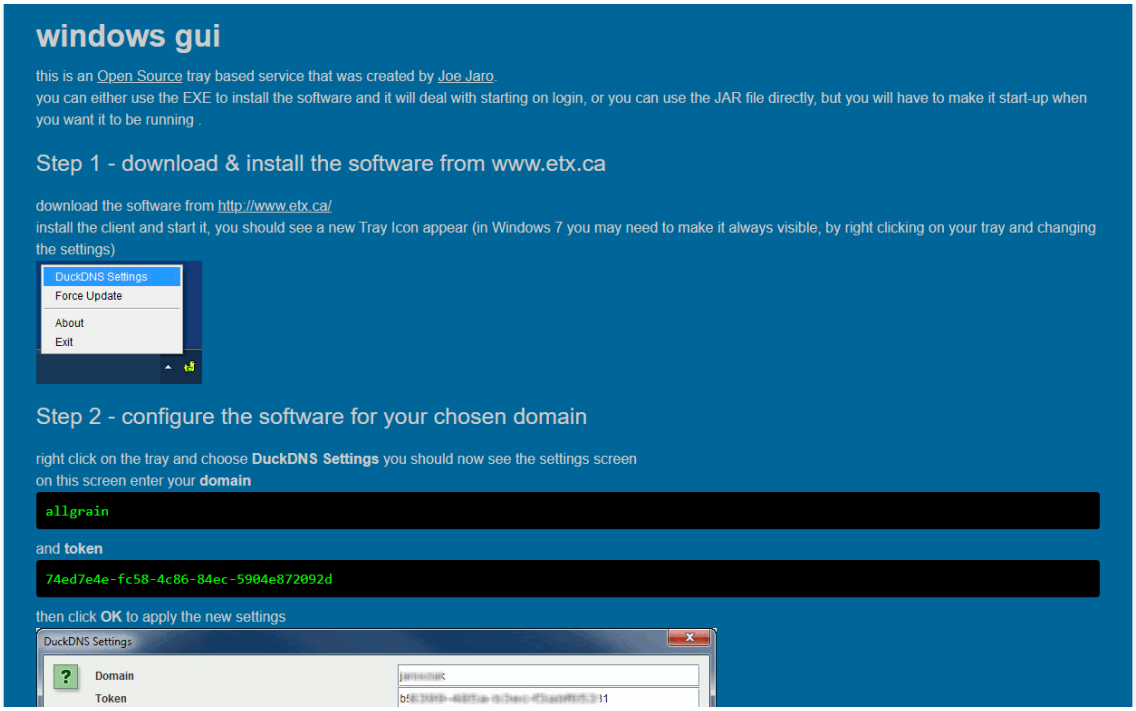
Para comprobar si se ha creado correctamente, abriremos el símbolo del sistema (cmd) y escribiremos el comando *nslookup www.allgrain.duckdns.org* el cual es el nombre de nuestro dominio:



Como vemos, aparece *respuesta no autoritativa* lo cual quiere decir que es un servidor DNS externo. También nos da el nombre del dominio y nuestra IP pública asociada a ese nombre de dominio. Por lo tanto, se puede concluir que ha sido registrado correctamente.

Como nuestra IP pública es dinámica y no fija, si quisiéramos mantener el dominio y que se adapte a estos cambios deberíamos ir a *Install* → *Windows-gui* y ahí se explican los pasos a seguir para llevar a cabo dicho proceso.





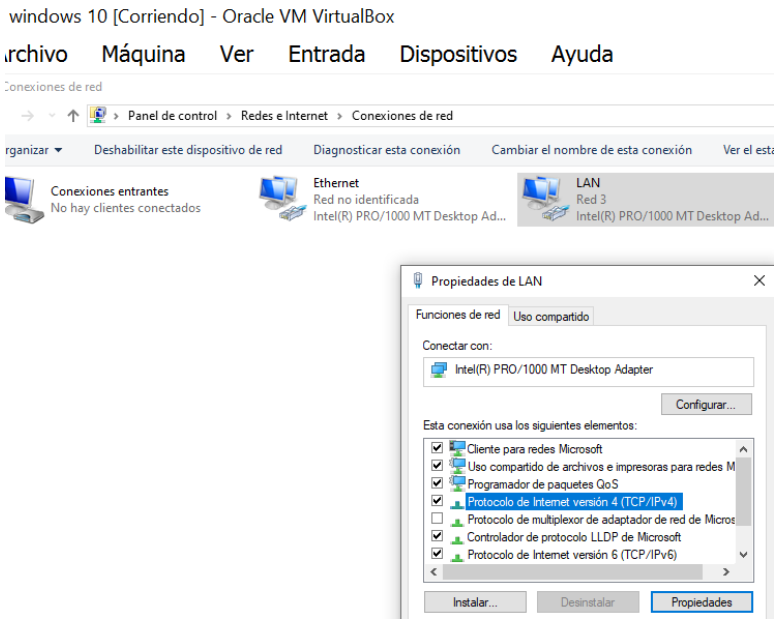
Es importante comprobar que no estamos detrás de ninguna VPN, ya que esto nos daría una IP diferente y afectaría a la asociación del dominio con la IP y, por lo tanto, a su correcto funcionamiento.

ACTIVIDAD 2 (2 puntos)

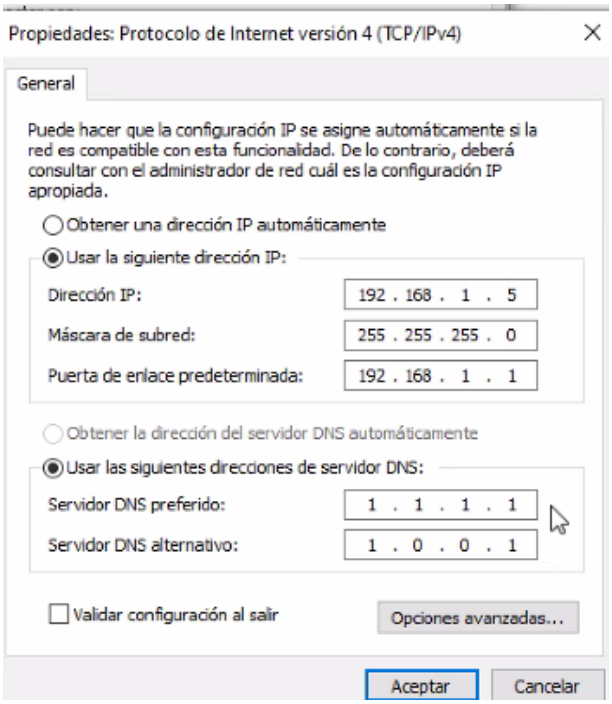
Objetivo: Instala y configura un servidor web en Windows (alternativamente en Linux) utilizando Internet Information Services (IIS).

Como durante la realización de esta práctica vamos a dirigir tráfico externo a un puerto específico, lo primero que deberemos hacer, será establecer una IP fija en nuestra máquina virtual Windows 10. Esto se hace porque si la IP del dispositivo cambia con el tiempo (lo cual puede suceder si se está utilizando una IP dinámica asignada por DHCP), el *router* no sabrá a dónde redirigir el tráfico, lo cual rompería la regla de *port forwarding*. Sin una IP fija, cada vez que el dispositivo reciba una nueva IP, tendríamos que actualizar las reglas de *port forwarding* en la configuración del *router*.

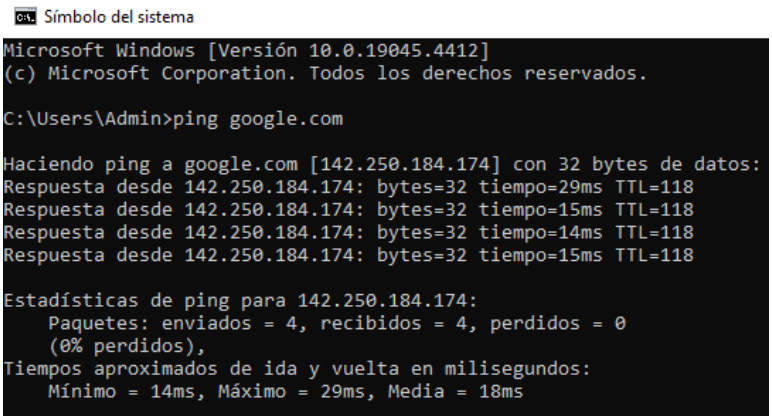
Para modificar esto, presionamos las teclas *Windows + R* para abrir el cuadro de diálogo *Ejecutar*. Escribimos *ncpa.cpl* para ver las conexiones de red y sobre la red LAN, la cual está conectada mediante adaptador puente a nuestra máquina física, pulsamos botón derecho del ratón *Propiedades → Protocolo de Internet versión 4 → Propiedades*:



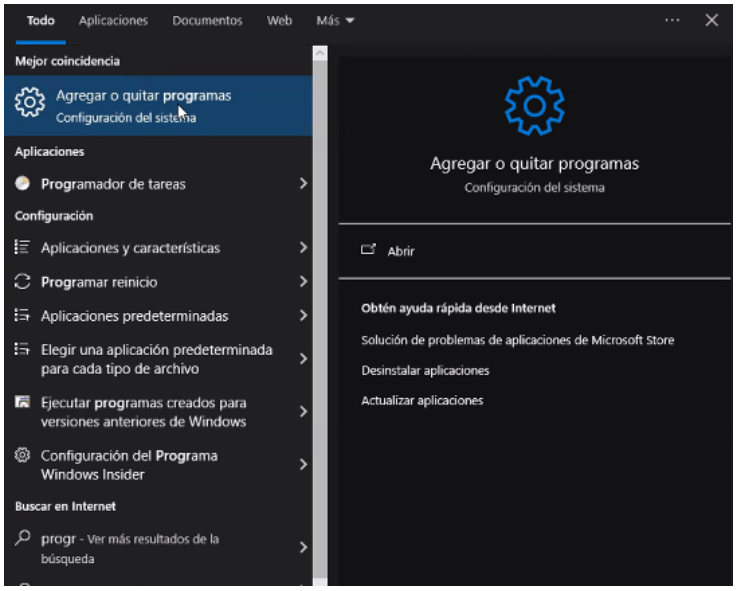
Escribiremos manualmente una dirección de IP fija, una máscara de red, una puerta de enlace predeterminada (la de nuestro *router*) y una dirección DNS primaria y otra secundaria. En nuestro caso le otorgamos ambas del servidor de *Cloudflare*, ya que se trata de un servidor rápido y seguro:



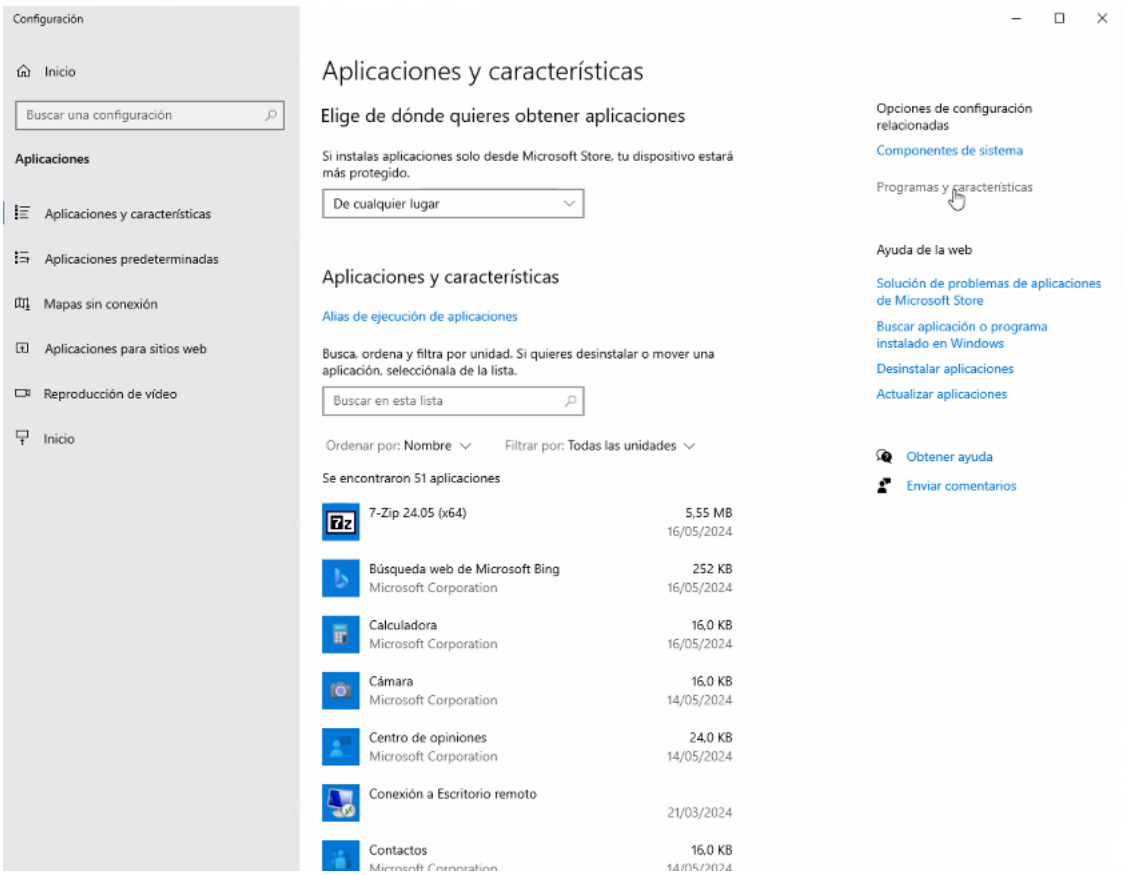
Para comprobar que todo sigue funcionando correctamente y aun disponemos de conexión, podemos hacer *ping* a Google.com:



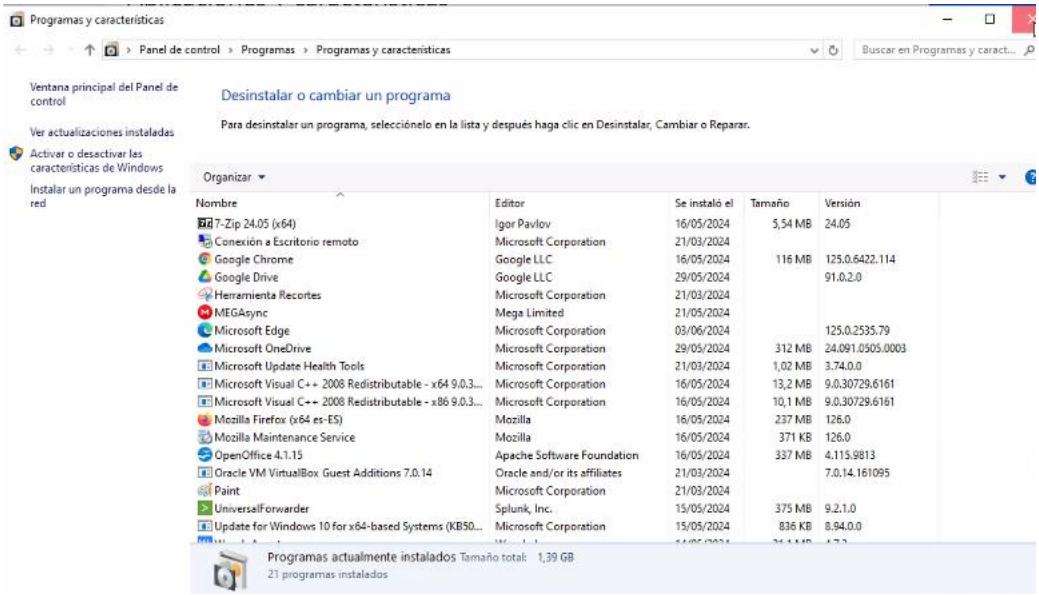
Una vez tenemos la IP fija establecida y comprobado que tenemos conexión a internet, vamos a proceder a activar ***Internet Information Services*.** IIS es un conjunto de servicios de servidores web creado por Microsoft para el sistema operativo Windows. Permite a los usuarios alojar y administrar sitios y aplicaciones web.
En el buscador de Windows escribimos *Agregar o quitar programas*, le damos clic:



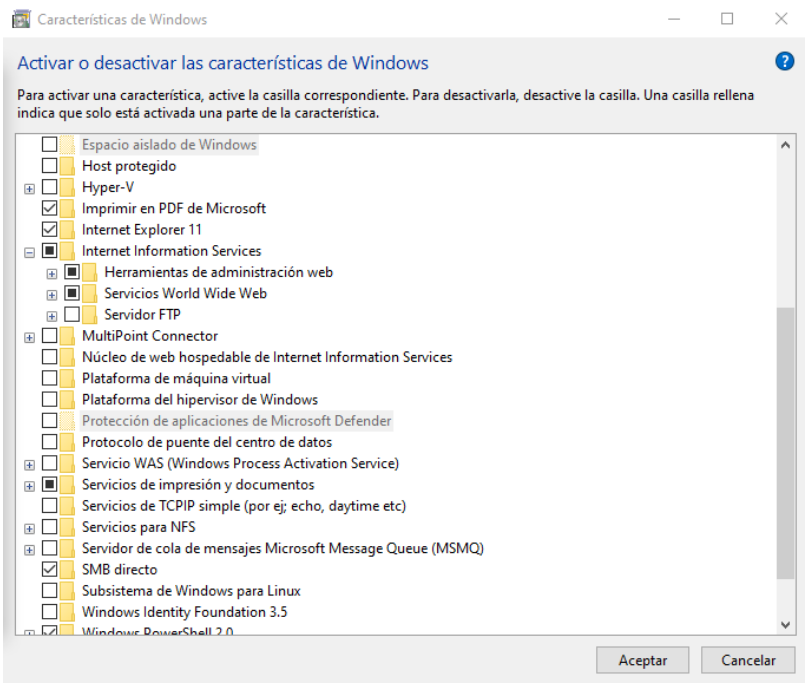
Después nos dirigimos al lado derecho de la ventana que se nos abrirá y le damos a *Programas y características*:



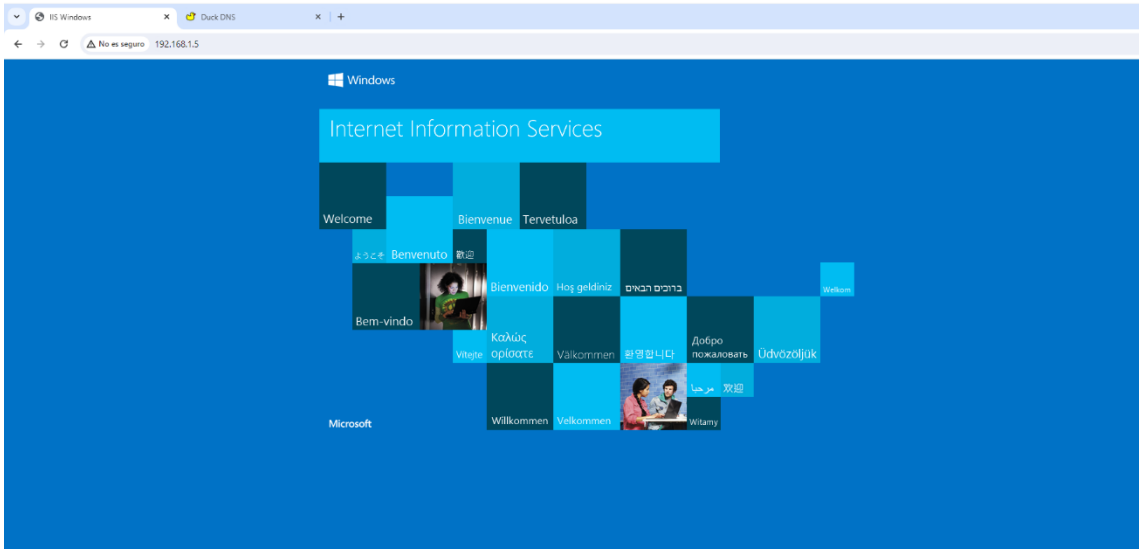
Ahora, en el lado izquierdo de la ventana, clicamos en A*ctivar o desactivar las características de Windows*:



Seleccionamos *Internet Information Services* y lo dejamos tal cual aparece, es decir, todo seleccionado excepto *Servidor FTP*:

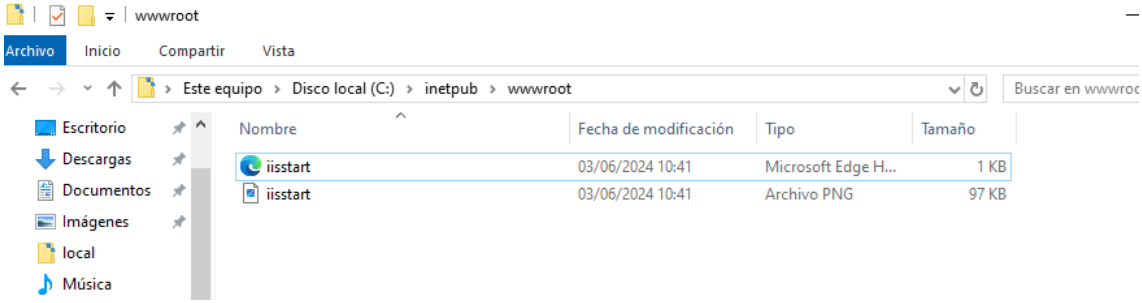


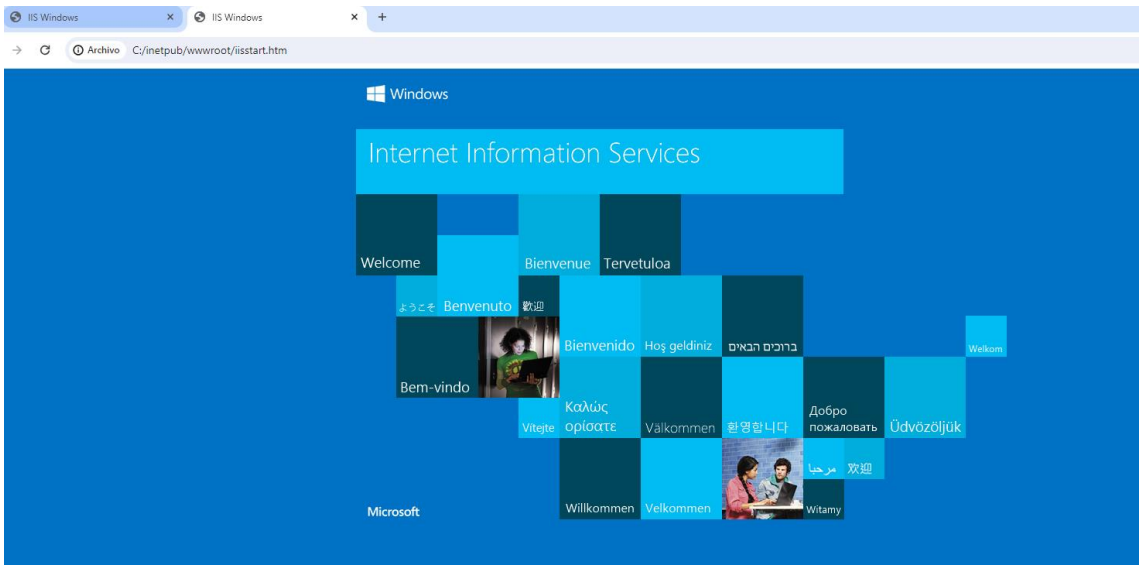
Una vez tengamos listo todo esto, escribimos en la barra de nuestro navegador, la dirección IP fija que le hemos asignado a nuestra máquina virtual, 192.168.1.5, y se nos abrirá la plataforma de *Internet Information Services*. Por el momento nos aparecerá la alerta de que este sitio no es seguro, ya que no contamos con el certificado SSL:



En lugar de abrirlo por IP, también se puede abrir por documento, es decir, yendo a:

Disco C: → inetpub → wwwroot → iisstart

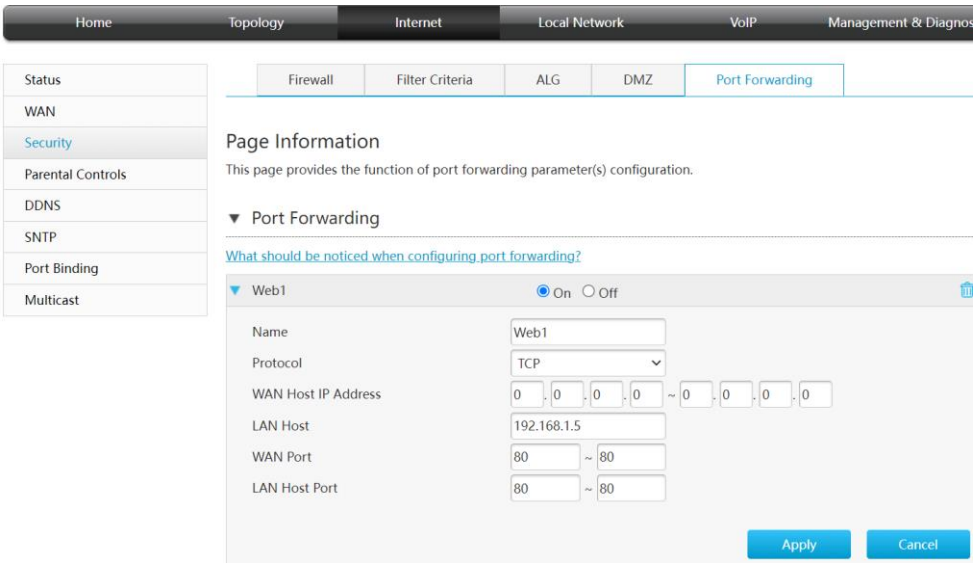




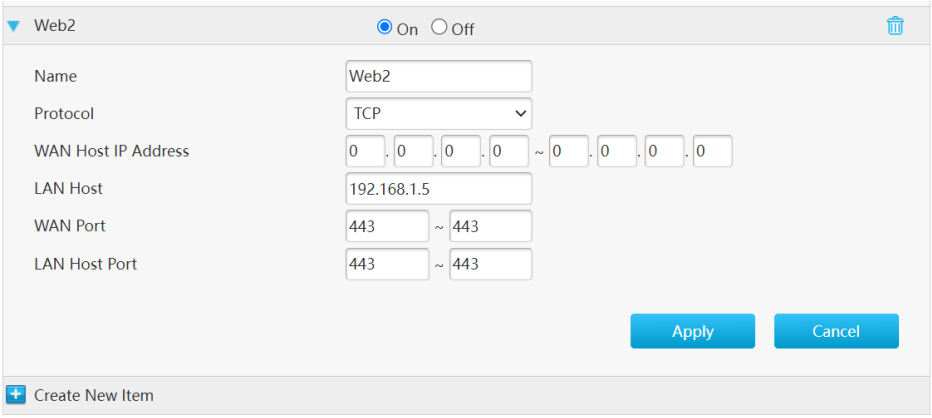
ACTIVIDAD 3 (2 puntos)

Objetivo: Configura el router para permitir el acceso externo al servidor web.

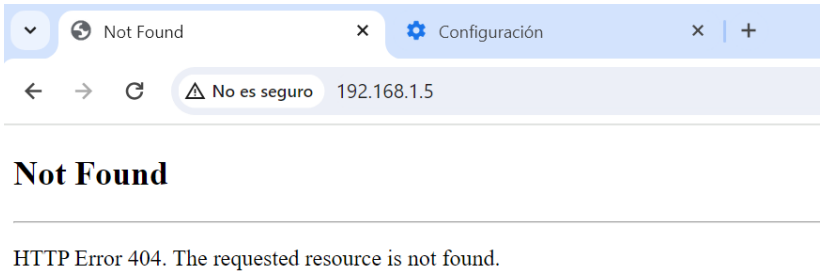
Para permitir el acceso desde el exterior al servidor web, deberemos abrir la configuración del *router* e ir a la configuración de puertos. En mi caso me dirijo a la pestaña de *Internet* → *Security* → *Port Forwarding*. Una vez dentro de la configuración de puertos, creamos dos reglas. Una para poder entrar al servidor web desde el puerto 80:



Y otra regla para poder entrar desde el puerto 443:

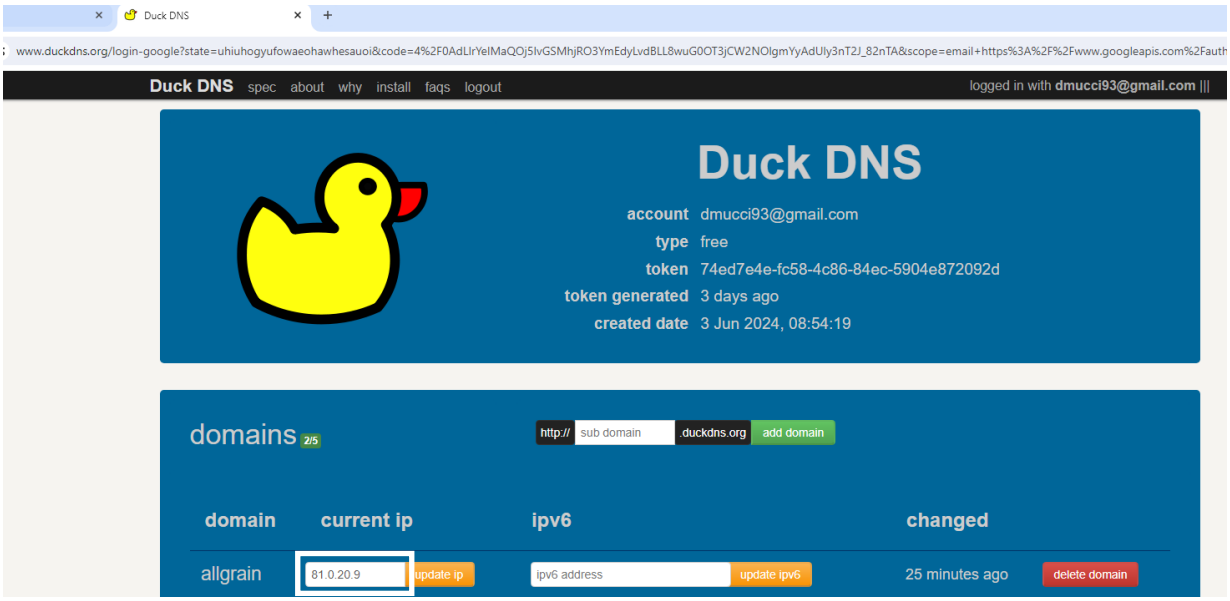


Ahora, escribimos la dirección IP en el navegador de otro dispositivo, en este caso, en el navegador web de mi máquina física y deberíamos ver abrirse nuevamente el servicio de *Internet Information Services*. Pero esto no fue posible de ninguna de las maneras, ni si quiera especificando el número de puerto:



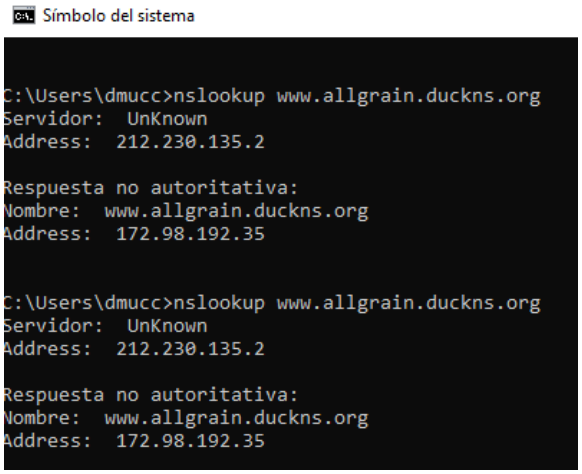
Esto es debido a que tengo activado CG-NAT (Carrier-Grade Network Address Translation) por parte mi proveedor de servicios de Internet (ISP) y eso me está imposibilitando la configuración de puertos de mi router. CG-NAT es una tecnología utilizada por los ISPs para gestionar la escasez de direcciones IPv4. Cuando uno está detrás de un CG-NAT, se comparte una dirección IP pública con otros usuarios, lo que implica varias limitaciones, como por ejemplo, imposibilidad de redirigir puertos o dificultad para acceder a servicios internos desde el exterior. Para remediar esto, llamé a mi ISP y pedí que me desactivaran CG-NAT, 24hs después recibí un *sms* diciendo que se había desactivado correctamente.

Después de esto, se apagó el router durante unos minutos y se volvió a encender para generar otra IP pública y asegurarnos de la desactivación de CG-NAT. Seguidamente, nos dirigimos nuevamente al servidor DuckDNS para actualizar la IP pública de nuestro sitio web y escribir la que tenemos actualmente:

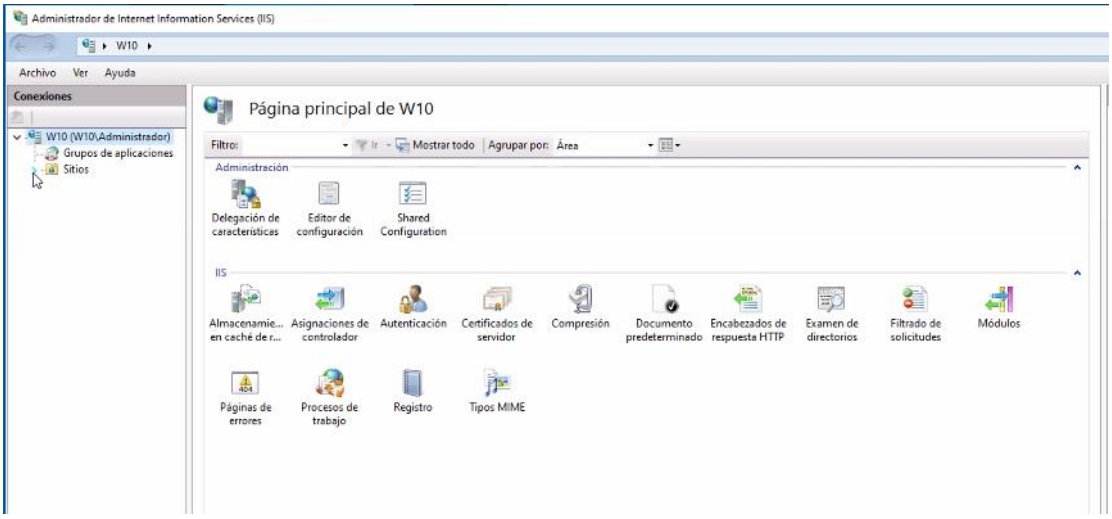


La IP pública la hemos corroborado yendo al sitio web: https://www.cual-es-mi-ip.net/geolocalizar-ip-mapa:

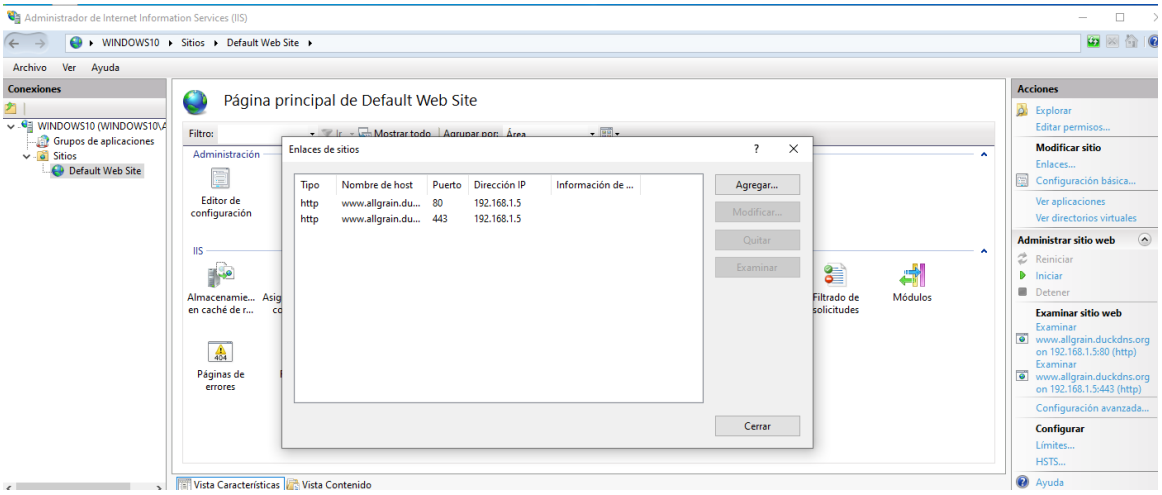
Pero ahora nos encontramos con otro problema y es que, al abrir cmd y escribir nuevamente el comando *nslookup nombredeldominio* nos aparece nuestro dominio creado asociado a otra IP distinta a la nuestra. Esto puede ser debido a que puede llevar un tiempo actualizar el servidor DuckDNS y las IP. Se esperó durante varios minutos, pero seguía apareciendo la IP 172.98.192.35 en lugar de nuestra IP pública 81.0.20.9:



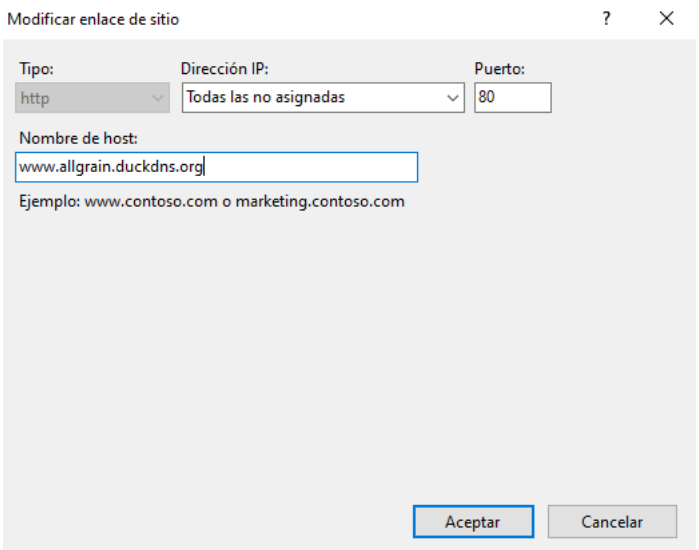
Aunque nosotros no hemos podido acceder al sitio web de ninguna de las maneras, probablemente debido a algún problema aún con mi proveedor de servicios de internet o con los servidores, si quisiéramos poder entrar por dominio deberíamos hacer lo siguiente. Vamos a *Administrador de Internet Information Services → Sitios*:



Después le damos a *Default Web Site* y en el lado derecho de la ventana clicamos en *Enlaces*. Se nos abrirá la siguiente ventana y le damos a agregar:



Escribimos el nombre del dominio que hemos creado, seleccionamos la dirección IP fija que hemos asignado y lo asociamos primero al puerto 80:

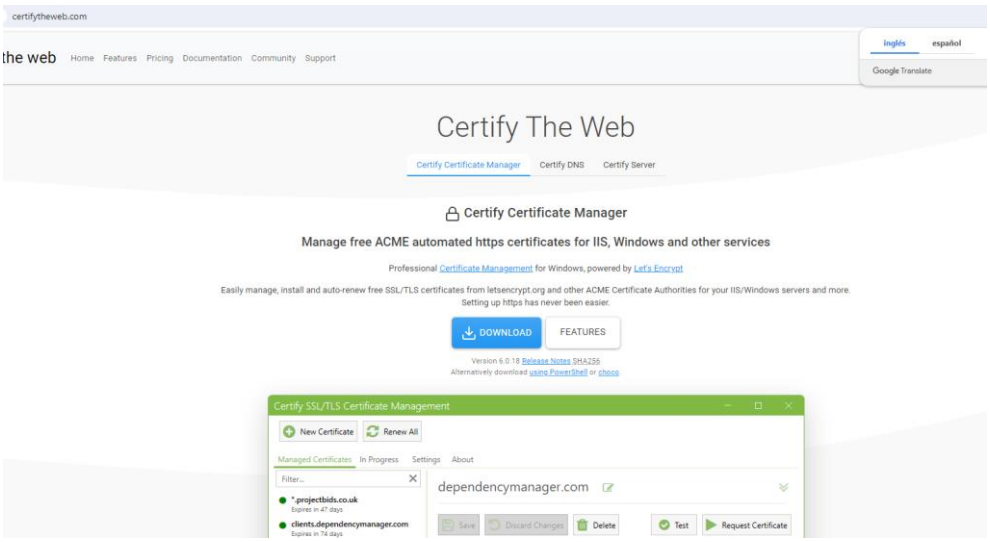


ACTIVIDAD 4 (2 puntos)

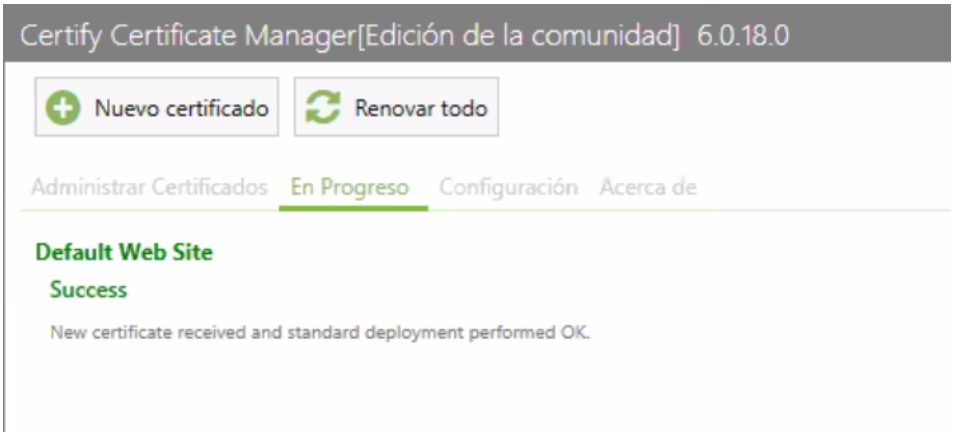
Objetivo: Configura HTTPS en el servidor web.

Ahora, si no se hubieran ocasionado los problemas detallados más arriba, al poner el nombre del dominio o nuestra IP pública en el navegador web, debería de entrar, pero advertirnos de que la página no es segura. Esto es debido a que no tenemos un certificado SSL (*Secure Sockets Layer*), el cual es un archivo de datos que vincula una clave criptográfica a los detalles de una organización. Cuando se instala en un servidor web, activa el candado y el protocolo HTTPS (*Hypertext Transfer Protocol Secure*), que permite conexiones seguras desde un servidor web a un navegador. SSL es esencial para asegurar datos sensibles, proteger la privacidad del usuario, y asegurar que la información transmitida entre el servidor web y el navegador del usuario se mantenga privada e íntegra.
Para obtener dicho certificado haríamos lo siguiente:

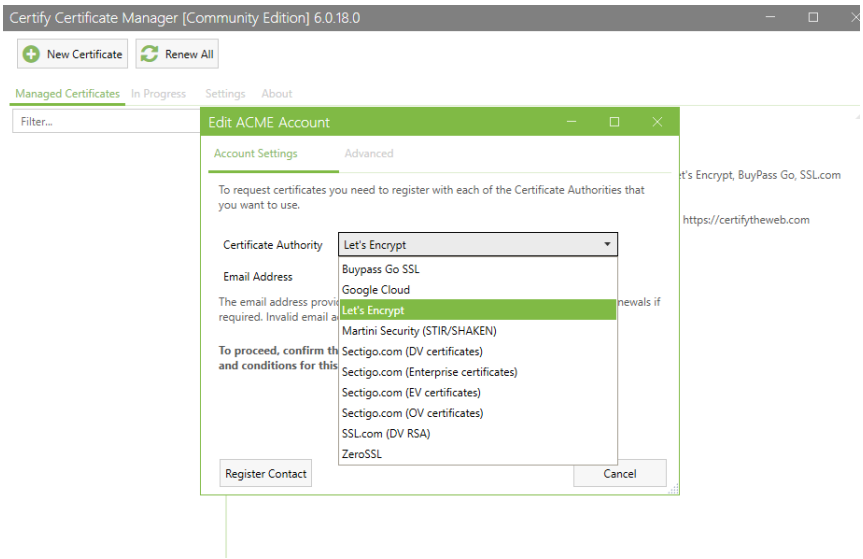
- Vamos a este sitio web y descargamos el software https://certifytheweb.com/



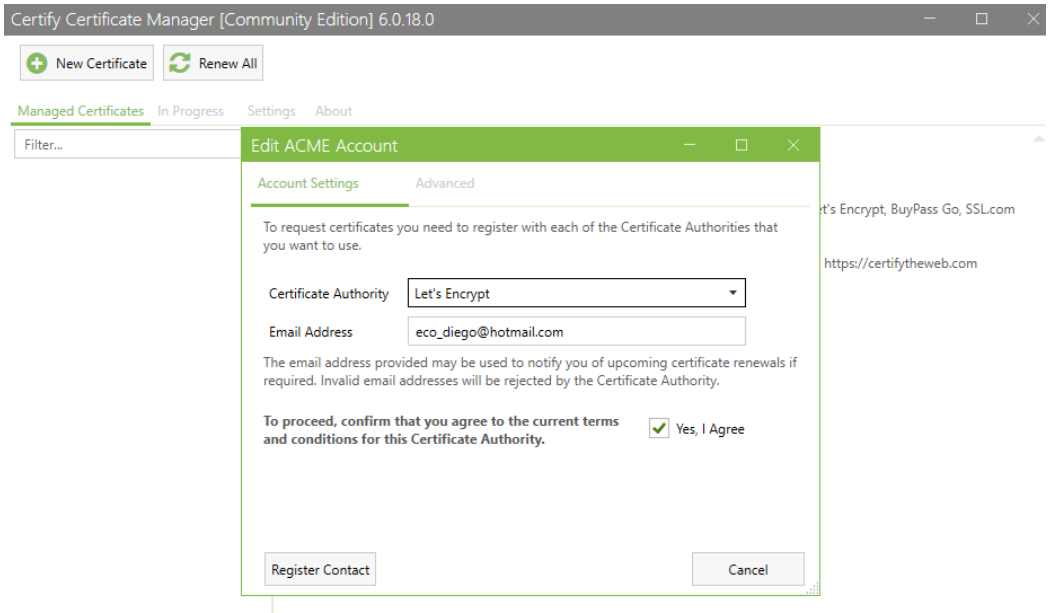
Seguimos el proceso de instalación normal y una vez lo tengamos, le damos *a nuevo certificado*:



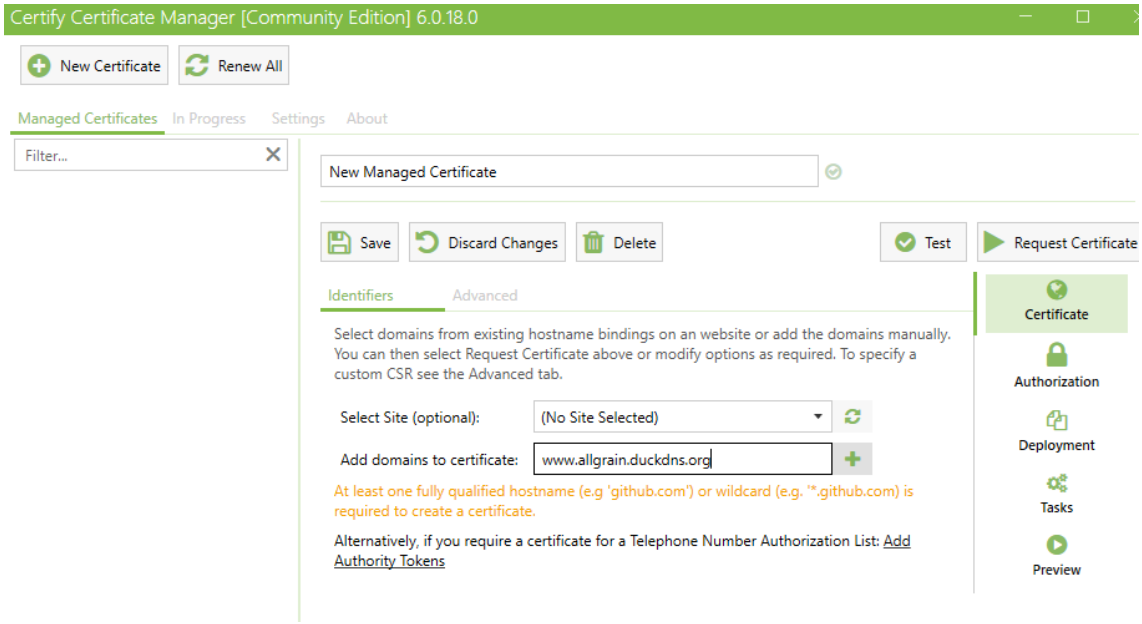
Nos pedirá que nos registremos, escribiendo nuestro email y seleccionando una Autoridad de Certificación. Nosotros dejaremos la que viene por defecto (*Let's Encrypt*):



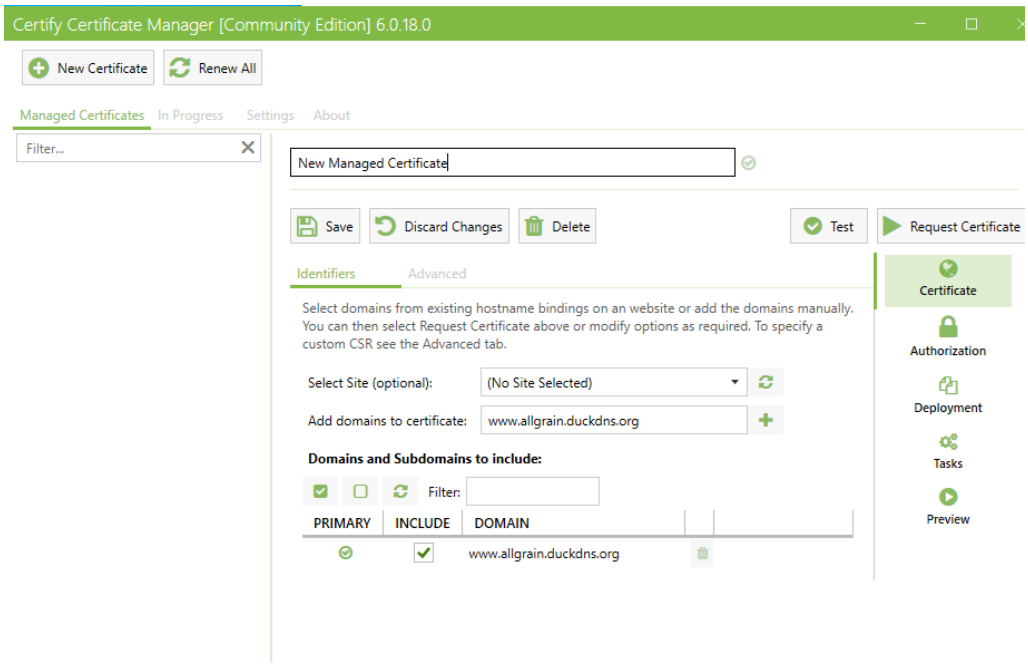
Le damos al botón *Register Contact*:

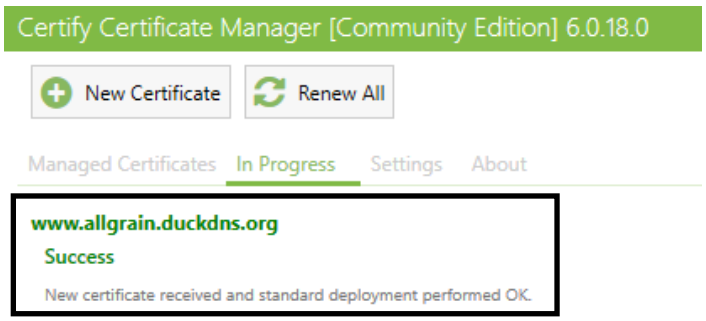


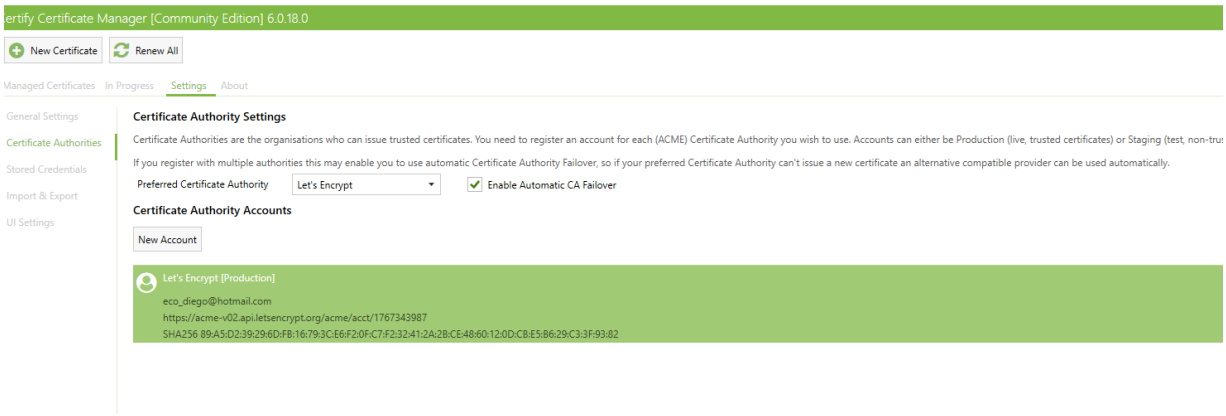
Donde pone *Add domains to certificate* escribimos el nombre de nuestro dominio y le damos al símbolo “+”:



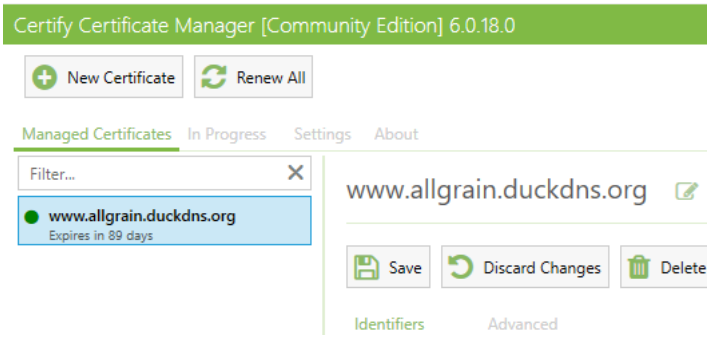
Presionamos en *Request Certificate* y si todo está correcto se generará el certificado:



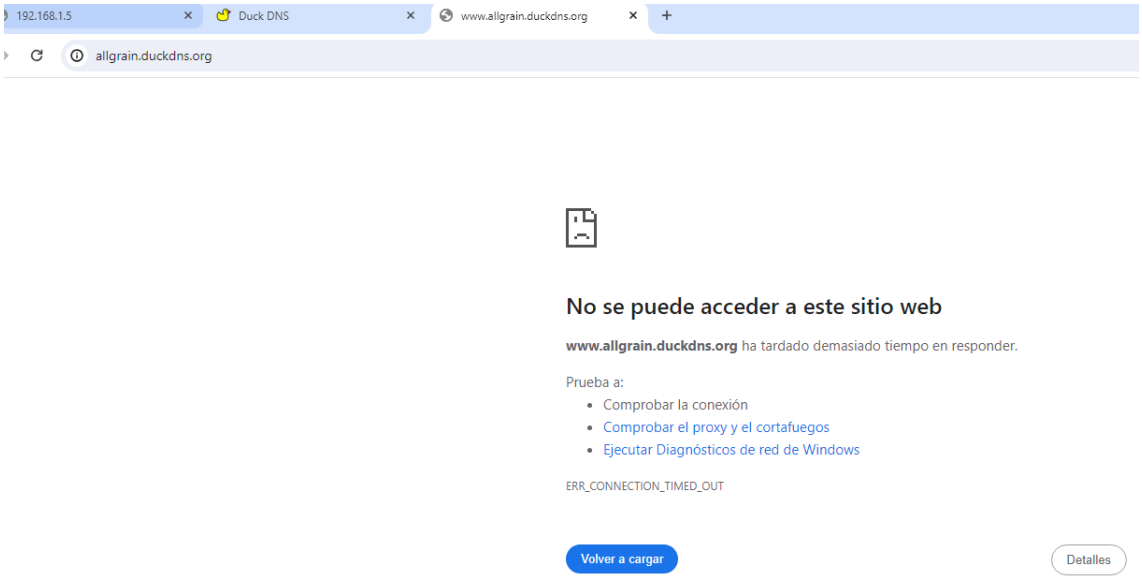




En *Managed Certificates* podemos ver la duración del certificado. Nos dice que expira en 89 días:



Es extraño porque, aunque nos haya dejado generar el certificado para este nombre de dominio, no hemos podido abrir nuestro sitio web de ninguna de las maneras. Probablemente sea debido a que aún no se han generado bien todos los cambios hechos por los problemas que ocurrieron durante esta práctica (detallados más arriba):



Para descartar que sea un problema de servidores DNS. Pusimos tanto en nuestra máquina virtual como en nuestra máquina física el servidor DNS de Cloudflare (1.1.1.1). Pero aun así, nos encontramos con que si hacemos *nslookup www.allgrain.duckdns.org* desde nuestra máquina virtual, la IP que corresponde al dominio es nuestra IP pública:

```
C:\Users\Admin>nslookup www.allgrain.duckdns.org
Servidor:  one.one.one.one
Address:  1.1.1.1

Respuesta no autoritativa:
Nombre:  www.allgrain.duckdns.org
Address:  81.0.20.9
```

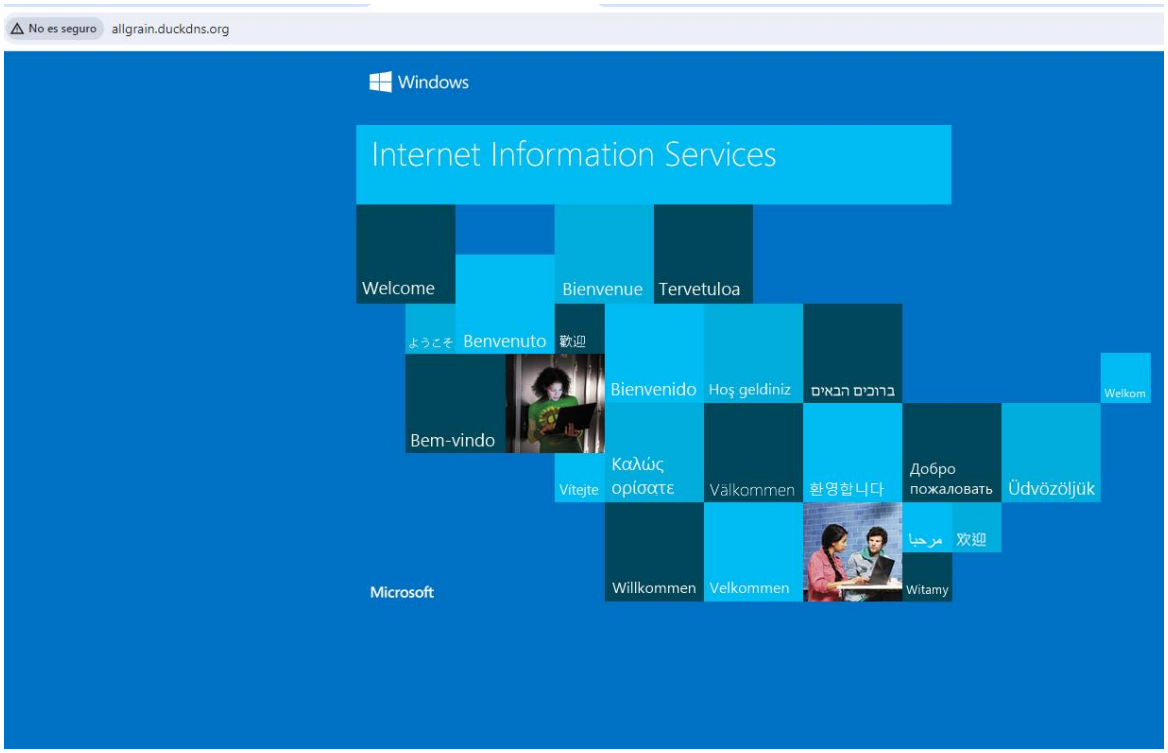
Sin embargo, si hacemos *nslookup www.allgrain.duckdns.org* desde nuestra máquina física, nos aparece otra IP diferente a la IP pública que utilizamos para generar el dominio:

```
C:\Users\dmucc>nslookup www.allgrain.duckns.org
Servidor:  one.one.one.one
Address:  1.1.1.1

Respuesta no autoritativa:
Nombre:  www.allgrain.duckns.org
Address:  172.98.192.35
```

También reiniciamos tanto la máquina virtual como nuestra máquina física, pero el problema siguió persistiendo.

Al cabo de 24hs, justo antes de la entrega de este examen, se volvió a probar, sin realizar ningún tipo de cambio en las configuraciones y ahora sí que se pudo acceder al sitio web a través del nombre del dominio:



Esto probablemente sea debido a algún problema del servidor que requirió más tiempo de lo habitual para actualizarse su configuración. El único problema que persiste es que, el sitio web sigue apareciendo como “no seguro” a pesar de haberse generado correctamente el certificado SSL. Quizás también sea un problema de tiempos y haya que darle más espacio de tiempo de lo normal a *Certify Certificate Manager* para que se genere correctamente dicho certificado.

ACTIVIDAD 5 **(2 puntos)**

Objetivo: Explica la importancia de certificar el sitio web y los 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.

Certificar un sitio web con un certificado SSL y utilizar HTTPS es crucial por diversas razones relacionadas con la seguridad y la confianza, tanto para la empresa como para los usuarios.

Algunos de los beneficios para la empresa son**:**

- **Protección de Datos**: Cifra los datos transmitidos entre el servidor y los navegadores, protegiendo información sensible como contraseñas, datos personales y financieros.
- **Confianza del Cliente**: Un sitio web seguro aumenta la confianza de los usuarios, lo que puede llevar a una mayor conversión y fidelización.
- **Cumplimiento Normativo**: Ayuda a cumplir con normativas y estándares de seguridad como GDPR, PCI DSS, entre otros.
- **Mejor Posicionamiento SEO**: Google y otros motores de búsqueda dan preferencia a los sitios web que usan HTTPS, mejorando el ranking en los resultados de búsqueda.
- **Integridad del Contenido**: Asegura que el contenido enviado al usuario no ha sido alterado por terceros en tránsito.

Por otro lado, algunos de los beneficios que supone utilizar HTTPS para los usuarios son:

- **Seguridad de la Información**: Los datos personales y financieros están protegidos contra interceptaciones y robos.
- **Confianza en la Autenticidad**: Los usuarios pueden estar seguros de que están interactuando con el sitio web legítimo de la empresa.
- **Experiencia de Navegación Mejorada**: Navegar en un sitio seguro reduce el riesgo de ataques como *phishing* y *man-in-the-middle*.

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?

Al implementar HTTPS algunos de los riesgos que se logran mitigar son:

- **Intercepción de Datos (*Sniffing*)**: HTTPS cifra los datos, haciendo que sean incomprensibles para el atacante que los pueda interceptar.
- **Alteración de Datos (*Tampering*)**: HTTPS garantiza la integridad de los datos transmitidos, asegurando que no sean modificados durante la transferencia.
- **Suplantación de Identidad (*Phishing*)**: Un certificado SSL autentica el sitio web, reduciendo el riesgo de que los usuarios sean engañados por sitios falsos.
- **Ataques *Man-in-the-Middle* (MitM)**: HTTPS protege contra los ataques MitM, donde un atacante intercepta y potencialmente altera la comunicación entre el usuario y el servidor.

En cuanto a la seguridad para el usuario, podríamos decir que un usuario normal generalmente se siente más seguro al ver el candado verde y el mensaje "este sitio es seguro" en la barra de direcciones del navegador. Esto visualmente indica que el sitio es seguro y fiable. Un usuario avanzado, considero que también se sentiría seguro visitando un sitio con HTTPS. Dado que, además, puede verificar detalles adicionales del certificado SSL, como la autoridad emisora y la duración, para confirmar la autenticidad y seguridad del sitio. Pero tampoco debería depositar toda la fe en ello, ya que hoy en día existen muchas maneras de que tus datos sean vulnerados incluso contando con la presencia de HTTPS.

La existencia de un certificado SSL no garantiza que quien esté detrás de un servidor haga operaciones con tus datos no autorizadas por tí. Un certificado SSL genera una falsa confianza en el usuario normal, que no debe trasladarse a un usuario avanzado.

Buen trabajo y los tiempos son los tiempos, muchas veces no los controlamos. Veo y me alegro que ahora explicas los por qués y los para qués.

9,5/10