Tecnicatura Superior en Telecomunicaciones. **Año 2025**
Profesor Ing. Jorge Morales.
Grupo 2 - Alumna: Emma Gutiérrez

Eje 1- TP Nro. 2

Protocolos de Comunicación HTTPS

El protocolo HTTPS (Hypertext Transfer Protocol Secure) es una versión segura del protocolo HTTP que cifra la información entre el navegador y el servidor. Esto protege los datos de la interceptación por terceros.

¿Qué representa HTTPS?

El significado de HTTPS es “Protocolo **Seguro de Transferencia de Hipertexto**”, y te permite enviar datos a páginas de Internet a la vez que evita que los hackers los roben. Tu navegador te indica si una página utiliza HTTPS. Por ejemplo, el navegador Google Chrome muestra un candado.

¿Quién creó el protocolo HTTPS?

Tim Berners-Lee, HTTP es el protocolo en el que se basa la Web. Fue inventado por **Tim Berners-Lee** entre los años 1989-1991, HTTP ha visto muchos cambios, manteniendo la mayor parte de su simplicidad y desarrollando su flexibilidad.

¿Qué es HTTPS y cuáles son sus características?
Características del protocolo HTTPS
Utiliza la tecnología SSL y TLS
Requiere un certificado SSL/TLS de una autoridad de certificación (CA) independiente
Compara el certificado con el navegador antes de intercambiar datos
Encripta todos los datos
Utiliza un servidor totalmente autentificado
Envía una clave de sesión que solo es legible para el servidor
HTTPS combina las solicitudes y respuestas HTTP con la tecnología SSL y TLS. Los sitios web HTTPS deben obtener un certificado SSL/TLS de una autoridad de certificación (CA) independiente. Estos sitios web comparten el certificado con el navegador antes de intercambiar datos para generar confianza.
Cómo saber si un sitio web usa HTTPS
La URL del sitio web empieza por https
El navegador muestra un candado en la barra de URL
Importancia del protocolo HTTPS
Es especialmente importante cuando se transmiten datos confidenciales, como al iniciar sesión en una cuenta bancaria, un servicio de correo electrónico o un proveedor de seguros médicos.
Tipos de certificados
Existen diferentes niveles de validación de certificados, como: Certificados de Validación de Dominio (DV), Certificados de Validación de Organización (OV), Certificados de Validación Extendida (EV).

¿Qué es el protocolo de seguridad web HTTPS?
Qué es el protocolo HTTPS y su importancia

El protocolo HTTPS (Hypertext Transfer Protocol Secure) es una versión mejorada y segura del protocolo HTTP. Su objetivo es proteger la información que se transfiere entre el navegador de un usuario y el servidor de un sitio web mediante el cifrado de datos.

¿Qué es y cómo implementar la seguridad https en tu página web?
https://www.apd.es › seguridad-https-en-tu-pagina-web
¿Qué es el protocolo seguro HTTPS?
El protocolo de transferencia de hipertexto seguro (HTTPS) es la versión segura de HTTP, que es el principal protocolo utilizado para enviar datos entre un navegador web y un sitio web. El HTTPS está encriptado para aumentar la seguridad de las transferencias de datos.

¿Cuáles son las características de un protocolo de investigación?
Los elementos fundamentales de un protocolo incluyen el título, antecedentes, planteamiento del problema, marco teórico, objetivos, diseño metodológico y cronograma. Además, un protocolo debe expresar claramente los objetivos y plan de la investigación para que otros puedan replicarla o evaluar su validez.

¿Cómo implementar el protocolo HTTPS?
Para usar HTTPS, es necesario obtener un certificado de servidor y vincularlo al sitio web donde se aloja ArcGIS Web Adaptor. Cada servidor web tiene su propio procedimiento para cargar un certificado y vincularlo a un sitio web.

¿Qué garantía ofrece el protocolo HTTPS?
Con el protocolo HTTPS se consigue que los datos de la web queden encriptados y que nadie pueda tener acceso a los mismos, aunque encontrase la manera de acceder. También debemos tener en cuenta que no solo se protege el sitio web, sino también la URL

¿Cuáles son los puertos seguros para HTTPS?
Puerto 443: HTTP seguro (HTTPS). HTTPS es la versión segura y encriptada de HTTP. Todo el tráfico web HTTPS va al puerto 443. Los servicios de red que utilizan HTTPS para la encriptación, como DNS sobre HTTPS, también se conectan en este puerto.

¿Qué es el puerto 443 y para qué se utiliza?

El puerto 443 es el puerto estándar para la comunicación segura en la web a través de HTTPS, la versión segura de HTTP. Este puerto se utiliza para cifrar la información que se transmite entre un navegador y un servidor web, asegurando que la información no sea interceptada por terceros, según Hostinger.

El Puerto estándar para HTTPS:
Es el puerto predeterminado para la comunicación segura en la web.

Cifrado de datos:
Asegura que la información intercambiada entre el navegador y el servidor web esté cifrada y protegida.

Uso común:
Se utiliza en una amplia gama de servicios online, incluyendo sitios web de comercio electrónico, bancarios, redes sociales, correo electrónico, almacenamiento en la nube y VPN.

Alternativa a HTTP:
A diferencia del puerto 80 (HTTP), el puerto 443 garantiza una conexión segura y privada.
Cuando un sitio web utiliza HTTPS, el tráfico de datos se encripta mediante un certificado SSL/TLS, como explica Hostinger y luego se transmite a través del puerto 443.
Si el puerto 443 no está abierto o bloqueado, es posible que no puedas acceder a un sitio web que utiliza HTTPS, o que la conexión no sea segura.
Para asegurar la seguridad de la comunicación, es importante utilizar el puerto 443 para HTTPS, y evitar utilizar el puerto 80 (HTTP) para transacciones sensibles.

El puerto 443 es el puerto estándar para HTTPS, la versión segura de HTTP. HTTPS se utiliza para que los sitios web y servicios en línea transmitan datos de forma segura y cifrada.

Puerto 443
El puerto predeterminado para HTTPS, la versión segura de HTTP
Para qué se usa
Para que los sitios web y servicios en línea transmitan datos de forma segura

Cómo se usa
Se utiliza para acceder a recursos web de forma segura
Por qué es importante

Garantiza la seguridad y privacidad de los usuarios en Internet

El **puerto 8443** es un número de puerto alternativo que también representa HTTPS.

Cómo saber si el puerto 443 está abierto

Ejecuta un comando que verifique si el puerto 443 está abierto. Si el comando devuelve “Conectado a <dirección IP o nombre de dominio>“, entonces el puerto 443 está abierto

El Grupo de Trabajo de Ingeniería de Internet (IETF) reconoce el número de puerto TCP 443 como el protocolo HTTPS predeterminado.

¿Qué es el protocolo de transferencia de hipertexto seguro (HTTPS) y cómo funciona?

El protocolo de transferencia de hipertexto seguro (HTTPS, por sus siglas en inglés) es un protocolo de comunicación de internet que se utiliza para cifrar y transmitir información de manera segura entre el navegador web de un usuario y el sitio web al que está conectado.

El protocolo HTTPS (Hypertext Transfer Protocol Secure) es una versión segura del protocolo HTTP que cifra la información entre el navegador y el servidor. Esto protege los datos de la interceptación por terceros.

Características del protocolo HTTPS

Utiliza la tecnología SSL y TLS

Requiere un certificado SSL/TLS de una autoridad de certificación (CA) independiente

Compara el certificado con el navegador antes de intercambiar datos

Encripta todos los datos

Utiliza un servidor totalmente autentificado

Envía una clave de sesión que solo es legible para el servidor

Cómo saber si un sitio web usa HTTPS

La URL del sitio web empieza por https

El navegador muestra un candado en la barra de URL

Importancia del protocolo HTTPS

Es especialmente importante cuando se transmiten datos confidenciales, como al iniciar sesión en una cuenta bancaria, un servicio de correo electrónico o un proveedor de seguros médicos.

Tipos de certificados

Existen diferentes niveles de validación de certificados, como: Certificados de Validación de Dominio (DV), Certificados de Validación de Organización (OV), Certificados de Validación Extendida (EV).

https://www.apd.es/seguridad-https-en-tu-pagina-web/#:~:text=Qu%C3%A9%20es%20el%20protocolo%20HTTPS%20y%20su%20importancia,mediante%20el%20cifrado%20de%20datos.

BIBLIOGRAFIA

- Trigo Aranda, V. (2005). Internet de las cosas: Conectividad y seguridad. [Editorial].
- Cavero Barca, J. M., & Fernández Gómez-Bravo, A. (2005). Arquitectura de sistemas para la Internet de las cosas. [Editorial].
- Aracil, F. J., Simó, J., & Ureña, J. (2005). Internet de las cosas: Tecnología, aplicación y diseño.[Editorial].
- Ramos Melgar, E. (2005). Desarrollo de aplicaciones IoT con Node-RED. [Editorial].
- Campos Magencio, Ó. (2005). Desarrollo de aplicaciones con Arduino para la Internet de las cosas. [Editorial].