***Francisco Javier Otero Herrero***

***Grupo ATU***

***10-4-2025***

***Certificados de Servidores***

# Actividad 2:

## Responder a las siguientes preguntas:

### ***¿Qué son los certificados de servidores seguros? ¿Para qué sirven? Indica sus principales características.***

***Un certificado de servidor seguro*** es un archivo digital que se utiliza en la comunicación cifrada entre un cliente (por ejemplo, un navegador web) y un servidor (por ejemplo, un sitio web). Este certificado actúa como una ***"credencial"*** que verifica la identidad del servidor y habilita el uso de conexiones seguras mediante el protocolo ***HTTPS.***

Estos certificados son emitidos por entidades de confianza ***llamadas Autoridades de Certificación (CA),*** que validan la identidad del propietario del servidor antes de emitir el certificado.

Los certificados de servidores seguros tienen dos funciones principales:

***Autenticación:***

* + Verifican que el servidor al que te estás conectando es quien dice ser.
  + Esto previene ataques como el ***phishing,*** donde un atacante podría suplantar la identidad de un sitio web legítimo.

***Cifrado:***

* + Habilitan el uso de cifrado en las comunicaciones entre el cliente y el servidor.
  + Esto asegura que los datos intercambiados ***(como contraseñas, información personal o detalles de pago)*** no puedan ser interceptados ni leídos por terceros.

En resumen, los certificados garantizan que:

* El servidor es auténtico.
* La comunicación entre el cliente y el servidor es segura.

Sus características principales son:

1. ***Basados en criptografía asimétrica***

* Los certificados utilizan un par de claves: una clave pública y una clave privada.
* La clave pública está incluida en el certificado y se utiliza para cifrar los datos.
* La clave privada se mantiene en secreto en el servidor y se utiliza para descifrar los datos.

1. ***Estructura jerárquica***

Los certificados están organizados en una cadena de confianza:

* Certificado raíz: Emitido por una Autoridad de Certificación (CA) de confianza.
* Certificado intermedio: Actúa como intermediario entre el certificado raíz y el certificado del servidor.
* Certificado del servidor: Específico para el dominio del servidor.

1. ***Protocolo SSL/TLS***

* Los certificados son fundamentales para implementar los protocolos SSL (Secure Sockets Layer) y su sucesor, TLS (Transport Layer Security)
* Estos protocolos permiten establecer una conexión cifrada entre el cliente y el servidor.

1. ***Vida útil limitada***

* Los certificados tienen una fecha de vencimiento (generalmente de 1 a 2 años).
* Una vez vencido, el certificado debe renovarse para seguir siendo válido.

1. ***Validación de identidad***

Existen diferentes niveles de validación según el tipo de certificado:

* ***DV (Domain Validation):*** Verifica solo que el solicitante tiene control sobre el dominio.
* ***OV (Organization Validation):*** Verifica la identidad de la organización que solicita el certificado.
* ***EV (Extended Validation):*** Ofrece la validación más rigurosa, incluyendo auditorías exhaustivas.

1. ***Formato estándar***

* Los certificados generalmente siguen el estándar ***X.509,*** que define su estructura y contenido.

1. ***Información contenida***

Un certificado incluye los siguientes datos:

* ***Nombre del titular:*** Identidad del propietario del certificado (por ejemplo, el nombre del dominio).
* ***Clave pública:*** La clave pública del servidor.
* ***Fecha de emisión y expiración:*** Período de validez del certificado.
* ***Firma digital:*** Emitida por la Autoridad de Certificación (CA) para verificar la autenticidad del certificado.

### ***¿En qué circunstancias debemos utilizar un certificado SSL?***

***Los certificados SSL (Secure Sockets Layer), o sus sucesores TLS (Transport Layer Security),*** son esenciales en cualquier situación donde la seguridad de las comunicaciones entre un cliente y un servidor sea importante. A continuación, detallamos las circunstancias clave en las que se debe utilizar un certificado ***SSL:***

1. ***Sitios web con transmisión de datos sensibles:***

* ***Circunstancia:*** Si tu sitio web maneja información sensible, como contraseñas, números de tarjetas de crédito, datos personales o información médica.
* ***Ejemplo:***
* Tiendas en línea (ecommerce) que procesan pagos.
* Plataformas de banca en línea.
* Formularios de registro o inicio de sesión.

*Razón: El cifrado SSL/TLS garantiza que los datos no puedan ser interceptados ni leídos por terceros malintencionados.*

1. ***Sitios web públicos para generar confianza:***

* ***Circunstancia:*** Si deseas que los usuarios confíen en tu sitio web, incluso si no manejas datos sensibles.
* ***Ejemplo:***
* Blogs, portafolios o sitios informativos.
* Cualquier sitio que busque mejorar su reputación y profesionalidad.

1. ***Cumplimiento legal y normativo:***

* ***Circunstancia:*** Si tu sitio debe cumplir con regulaciones legales o estándares de seguridad específicos.
* ***Ejemplo:***
* ***GDPR (Reglamento General de Protección de Datos):*** Obliga a proteger los datos personales de los usuarios europeos.
* ***PCI DSS (Payment Card Industry Data Security Standard):*** Requiere cifrado para sitios que manejan pagos con tarjetas de crédito.
* ***HIPAA (Health Insurance Portability and Accountability Act):*** Exige protección de datos médicos en EE. UU.

*Razón: El uso de SSL/TLS es obligatorio para cumplir con estas regulaciones y evitar multas o sanciones.*

1. ***Mejora del SEO (Posicionamiento en buscadores):***

* ***Circunstancia:*** Si deseas mejorar el posicionamiento de tu sitio en los motores de búsqueda.
* ***Ejemplo:***
* Google prioriza los sitios con HTTPS en sus resultados de búsqueda.

*Razón: Los certificados SSL/TLS no solo aumentan la seguridad, sino que también son un factor de ranking para los algoritmos de búsqueda.*

1. ***Comunicación entre servidores***

* ***Circunstancia:*** Si necesitas asegurar las conexiones entre servidores, APIs o aplicaciones backend.
* ***Ejemplo:***
* Servicios en la nube que se comunican entre sí.
* APIs RESTful o GraphQL que transmiten datos sensibles.

*Razón: El cifrado SSL/TLS protege las comunicaciones internas de ataques como el espionaje o la manipulación de datos.*

1. ***Acceso remoto seguro:***

* ***Circunstancia:*** Si proporcionas acceso remoto a sistemas o aplicaciones.
* ***Ejemplo:***
* Conexiones a servidores mediante SSH o RDP.
* Acceso a intranets o extranets corporativas.

*Razón: El cifrado SSL/TLS asegura que las credenciales y los datos transmitidos durante el acceso remoto no sean interceptados.*

1. ***Correo electrónico seguro:***

* ***Circunstancia:*** Si manejas correos electrónicos que contienen información confidencial.
* ***Ejemplo:***
* Servidores de correo (SMTP, IMAP, POP3) que utilizan cifrado SSL/TLS.
* Servicios de correo web (como Gmail o Outlook) que requieren HTTPS.

*Razón: El cifrado evita que los correos sean interceptados o manipulados durante la transmisión.*

1. ***Redes Wi-Fi públicas:***

* ***Circunstancia:*** Si ofreces acceso a una red Wi-Fi pública o privada.
* ***Ejemplo:***
* Cafeterías, aeropuertos o hoteles que ofrecen Wi-Fi a clientes.
* Redes corporativas que permiten acceso a invitados.

*Razón: El cifrado SSL/TLS protege a los usuarios de ataques como el Man-in-the-Middle (MitM) en redes inseguras.*

1. ***Aplicaciones móviles***

* ***Circunstancia:*** Si desarrollas aplicaciones móviles que se conectan a servidores backend.
* ***Ejemplo:***
* Aplicaciones de banca móvil.
* Apps de mensajería instantánea.

*Razón: El cifrado SSL/TLS asegura que los datos enviados desde la app al servidor estén protegidos.*

1. ***Sitios con autenticación de usuarios:***

* ***Circunstancia:*** Si tu sitio permite a los usuarios iniciar sesión o crear cuentas.
* ***Ejemplo:***
* Plataformas educativas.
* Redes sociales.
* Foros o comunidades en línea.

*Razón: El cifrado protege las credenciales de los usuarios y evita accesos no autorizados.*

Se debe utilizar un certificado***SSL/TLS***siempre que:

1. *Manejes datos sensibles.*
2. *Quieras generar confianza en tus usuarios.*
3. *Necesites cumplir con regulaciones legales.*
4. *Desees mejorar el SEO de tu sitio.*
5. *Asegures comunicaciones entre sistemas*.

En resumen, el uso de certificados ***SSL/TLS*** es prácticamente obligatorio en la mayoría de los escenarios modernos de internet, ya que garantizan la seguridad, la privacidad y la confianza en las interacciones digitales.