UNIVERSIDAD CENTRAL DEL ECUADOR

CRIPTOGRAFÍA Y SEGURIDAD DE LA INFORMACIÓN

Grupo 6

Integrantes:

- Condolo Narvaez Byron Paul
- Lascano Puruncajas Angelo Damian
- Loya Cadena Bryan Eduardo
- Rosero Lema Ruth Estefania
- Tapia Rea Freddy Xavier
- Trujillo Vistin Dennis Adrian

SSL/TLS: Asegurando Comunicaciones en la Web

SSL/TLS (Secure Sockets Layer / Transport Layer Security) es el pilar fundamental para la seguridad en internet. Este protocolo criptográfico garantiza la privacidad e integridad de la información transmitida a través de redes.

1

Definición de la Tecnología

Un protocolo criptográfico para comunicaciones seguras en red, con TLS como su evolución moderna y estándar de facto.

2

Implementación en el Proyecto

Utilizamos **HTTPS** (HTTP sobre TLS) con **Node.js** y **Express.js** , empleando certificados **X.509 autofirmados** y claves **RSA 2048 bits** .

Algoritmos Criptográficos Clave en SSL/TLS

La seguridad de SSL/TLS se sustenta en una combinación estratégica de algoritmos criptográficos que garantizan confidencialidad, integridad y autenticación en cada etapa de la comunicación.

1

Algoritmos de Clave Pública (Asimétricos)

- **RSA (Rivest-Shamir-Adleman) - 2048 bits:** Claves para certificados digitales, verificando la identidad del servidor.
- **ECDHE (Elliptic Curve Diffie-Hellman Ephemeral):** Intercambio de claves de sesión seguro para el secreto hacia adelante (TLS handshake).

2

Algoritmos de Cifrado Simétrico

- **AES-256-GCM (Advanced Encryption Standard - Galois/Counter Mode):** Cifrado y autenticación de datos para la sesión HTTPS.

3

Funciones Hash Criptográficas

- **SHA-256:** Firma digital de certificados, asegurando autenticidad e integridad.
- **SHA-384:** Mayor resistencia para certificados de alta seguridad.
- **HMAC (Hash-based Message Authentication Code):** Integridad y autenticación de mensajes en el flujo TLS.

Protocolos Criptográficos Fundamentales

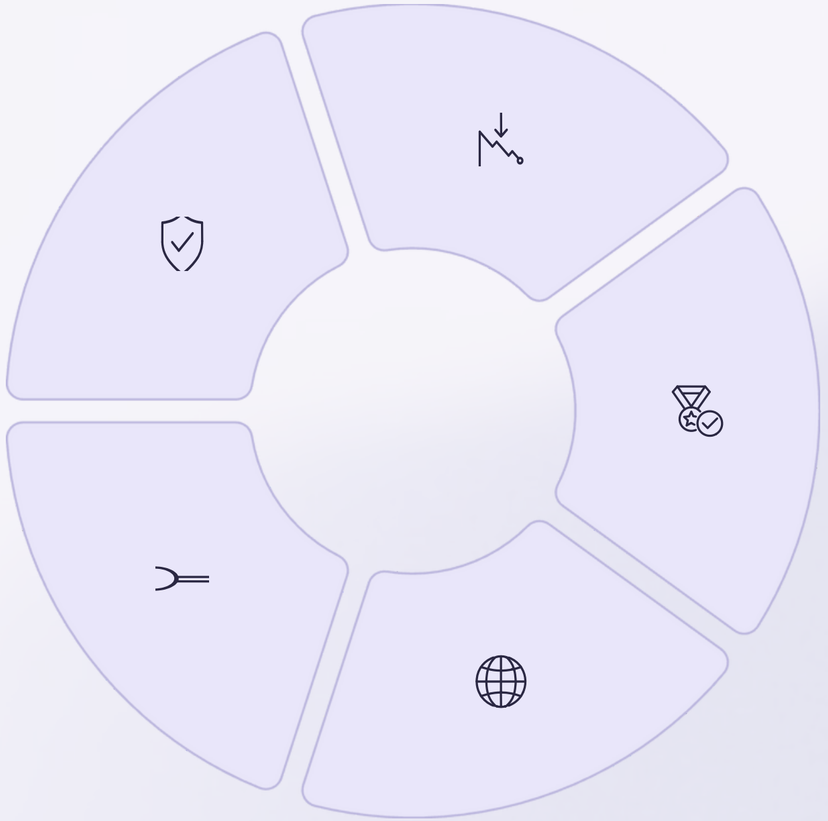
Además de los algoritmos, una serie de protocolos trabajan en conjunto para construir la infraestructura de seguridad que pro tege nuestras interacciones en línea.

TLS 1.3

La versión más reciente y segura del protocolo, ofreciendo mejoras significativas en rendimiento y seguridad.

PKI

La **P**ublic **K**ey **I**nfrastructure es el marco que gestiona los certificados digitales, desde su emisión hasta su revocación.



TLS 1.2

Aún ampliamente utilizada por su compatibilidad con sistemas existentes, aunque se recomienda la migración a TLS 1.3.

X.509 v3

El estándar universal para los certificados digitales, pieza clave de la infraestructura de clave pública (PKI).

HTTPS

La implementación de HTTP sobre TLS, garantizando que la navegación web sea cifrada y segura.

Escenarios Comunes de Uso de SSL/TLS

SSL/TLS es omnipresente en el mundo digital, protegiendo una gran variedad de interacciones cotidianas y críticas.

Comercio Electrónico y Banca en Línea

Plataformas como Amazon, MercadoLibre y los servicios bancarios usan SSL/TLS para cifrar transacciones financieras y datos personales, protegiéndolos de ciberataques.

Correo Electrónico Seguro

Servicios como Gmail, Outlook o ProtonMail implementan TLS (SMTP/IMAP/POP3 sobre TLS) para asegurar la comunicación entre clientes y servidores de correo, resguardando la privacidad de los mensajes.

APIs RESTful y Microservicios

Las arquitecturas modernas dependen de APIs REST sobre HTTPS para la comunicación segura entre servicios, aplicaciones móviles y backends, como en Google Maps API o Stripe API.

Generar certificado y clave privada (RSA 2048 bits)

Este comando genera automáticamente:

- `server.key` → Clave privada
- `server.crt` → Certificado digital autofirmado

```
openssl req -x509 -nodes -newkey rsa:2048 -keyout server.key -out server.crt -days 365
```

Llenar la información del certificado

A continuación, se presenta un conjunto de valores **estandarizados, recomendados y orientados a un entorno académico profesional** de la *Universidad Central del Ecuador*.

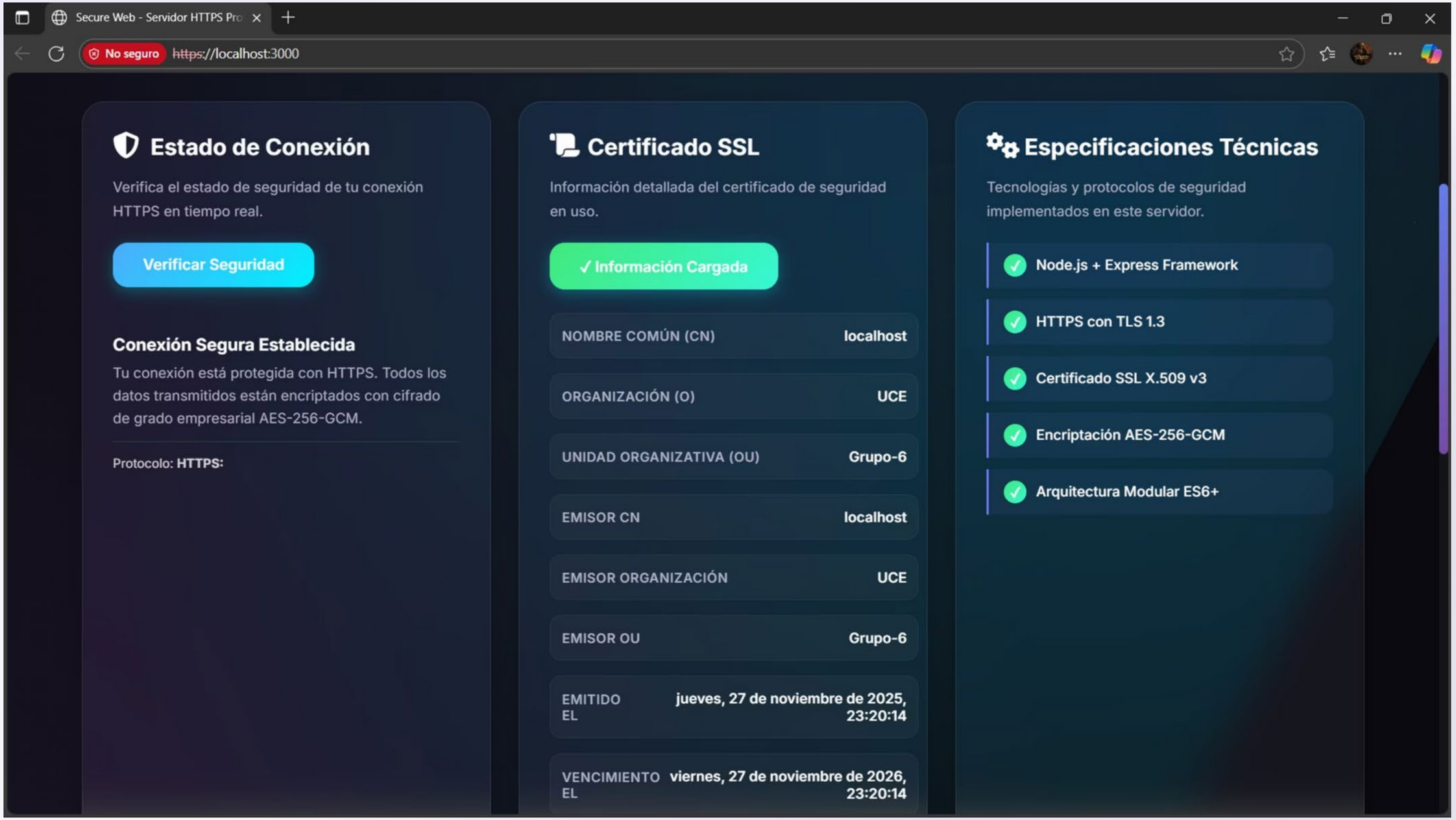
Completa los campos así:

```
Country Name (2 letter code) [AU]: EC
State or Province Name (full name) [Some-State]: Pichincha
Locality Name (eg, city) []: Quito
Organization Name (eg, company) [Internet Widgits Pty Ltd]: Universidad Central del Ecuador
Organizational Unit Name (eg, section) []: Facultad de Ingeniería, Escuela de Computación
Common Name (e.g. server FQDN or YOUR name) []: localhost
Email Address []: criptografia@uce.edu.ec
```

Notas importantes:

- **Common Name (CN)** debe ser **localhost**, ya que se trata de un entorno de desarrollo local.
- Los valores institucionales hacen referencia a la UCE y la cátedra correspondiente.
- No se requiere ingresar una contraseña para la clave privada, ya que se usa `-nodes`.

Vista en localhost



Preguntas

Pregunta de Selección Simple

Pregunta 1: ¿Para qué sirve un certificado digital en una página web?

- Para asegurar que la conexión sea privada y segura.
- Para que la página cargue más rápido.
- Para permitir decoraciones visuales.
- Para guardar archivos del usuario.
- Para bloquear anuncios.

Respuesta correcta: Para asegurar que la conexión sea privada y segura.

Pregunta de Selección Múltiple

Pregunta 2: ¿Qué beneficios obtiene un usuario cuando navega en un sitio web con conexión segura (HTTPS)? *(Nota: Esta pregunta tiene 3 respuestas correctas).*

- Su información viaja cifrada.
- Puede verificar que está hablando con el sitio correcto.
- Evita que terceros espíen sus datos.
- Tiene internet más rápido automáticamente.
- Las páginas cambian de diseño.

Respuestas Correctas :

- Su información viaja cifrada.
- Puede verificar que está hablando con el sitio correcto.
- Evita que terceros espíen sus datos.

Pregunta de Emparejamiento

Pregunta 3: Relaciona cada concepto con su significado.

Significado / Definición	Concepto Correcto
Identifica a quién pertenece una página	
Señala que la conexión es segura	
Evita que terceros lean la información	
Programa que muestra páginas web	
Conjunto de prácticas para proteger la información	

Opciones: Certificado digital, HTTPS, Cifrado, Navegador, Seguridad web

Pregunta de Respuesta Corta

Pregunta 4:

¿Cómo se llama el proceso que convierte información en algo ilegible para protegerla?

> Respuesta: Cifrado.

Pregunta de Verdadero o Falso

Pregunta 5: HTTPS ayuda a proteger los datos que envías cuando llenas formularios en una página web?

Respuesta:

Verdadero (true).

Bibliografía

[1] E. Rescorla, “The transport layer security (tls) protocol version 1.3,” RFC 8446 (IETF), 2018, online; available at https://datatracker.ietf.org/doc/html/rfc8446.

[2] B. Dowling, M. Fischlin, F. Günther, and D. Stebila, “A cryptographic analysis of the tls 1.3 handshake protocol,” inProc eedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security (CCS ’15), Denver, CO, USA, 2015, pp. 1197 –1210.

[3] A. Bhargavan, C. Fournet, M. Kohlweiss, A. Pironti, P.-Y. Strub, and S. Zanella-Béguelin, “Proving the tls handshake secure (as it is),” inAdvances in Cryptology – CRYPTO 2014, J. A. Garay and R. Gennaro, Eds. Berlin, Heidelberg: Springer, 2014, pp. 235 –255.

[4] H. Krawczyk and H. Wee, “The optls protocol and tls 1.3,” in2016 IEEE European Symposium on Security and Privacy (EuroS&P), Saarbrücken, Germany, 2016, pp. 81 –96.

[5] Y. Liu, W. Tome, L. Zhang, D. Choffnes, D. Levin, B. Maggs, A. Mislove, A. Schulman, and C. Wilson, “An end-to-end measurement of certificate revocation in the web’s pki,” inInternet Measurement Conference (IMC ’15), Tokyo, Japan, 2015, pp. 183–196