TECNOLOGICO NACIONAL DE MÉXICO.

INSTITUTO TECNOLÓGICO DE TLAXIACO.

CARRERA: INGENIERÍA EN SISTEMAS COMPUTACIONALES

SEGURIDAD Y VIRTUALIZACION.

ACTIVIDAD: REPORTE DE PRACTICA 1.

SEMESTRE: SEPTIMO **GRUPO:** 7 US

INTEGRANTES DEL EQUIPO:

NELSY ORTIZ LÓPEZ.	21620165
JEANETTE ARLET SALAZAR NICOLÁS.	21620202
LUCERO ZÚÑIGA MARIBEL	21620139

ASESOR: EDWARD OSORIO SALINAS.

TLAXIACO, OAX, A 30 DE AGOSTO DE 2024.

CONTENIDO

TABLA DE ILUSTRACIONES.

Instrucciones.

1. Crea un programa en Python que permita al usuario ingresar una contraseña y que valide si la contraseña es segura o no. Una contraseña segura debe cumplir con los siguientes criterios basados en las recomendaciones de Google:

- Tener al menos 8 caracteres.
- Tener al menos una letra mayúscula (A-Z).
- Tener al menos una letra minúscula (a-z).
- Tener al menos un número (0-9).
- Tener al menos un carácter especial (!, @, #, $, %, ^, &, *, (,), -, _, =, +, [,], {, }, |, \, ;, :, ', ", ,, ., <, >, /, ?, ~, `).
- No debe contener espacios en blanco.
- No debe tener más de 2 caracteres iguales consecutivos.
- Si la contraseña cumple con los criterios, el programa deberá mostrar un mensaje indicando que la contraseña es segura, de lo contrario, deberá mostrar un mensaje indicando que la contraseña no es segura.

En esta ocasión, decidimos implementar el programa utilizando HTML y hojas de estilo, siguiendo los criterios mencionados anteriormente. En la siguiente captura de pantalla se muestra un ejemplo de cómo el programa genera un mensaje de error cuando la contraseña ingresada no es segura. Por ejemplo, al ingresar la contraseña "1234567", el programa indica que la contraseña debe tener al menos 8 caracteres, ya que no cumple con los requisitos mínimos, como el uso de caracteres especiales y mayúsculas.

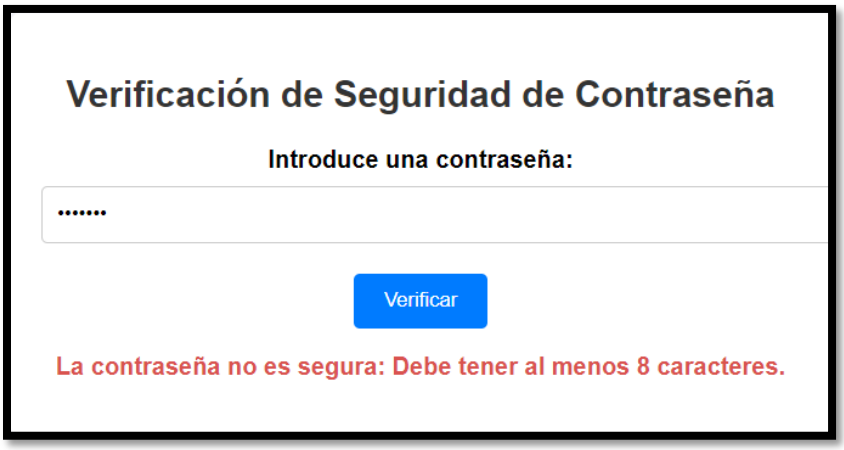


Ilustración 1: La contraseña no es segura.

En el siguiente ejemplo, analizamos otra contraseña utilizando el programa desarrollado. En esta ocasión, probamos con "Contraseñasegura123/", que cumple con todos los criterios de una contraseña segura. Al verificarla, observamos que el programa la acepta como válida.

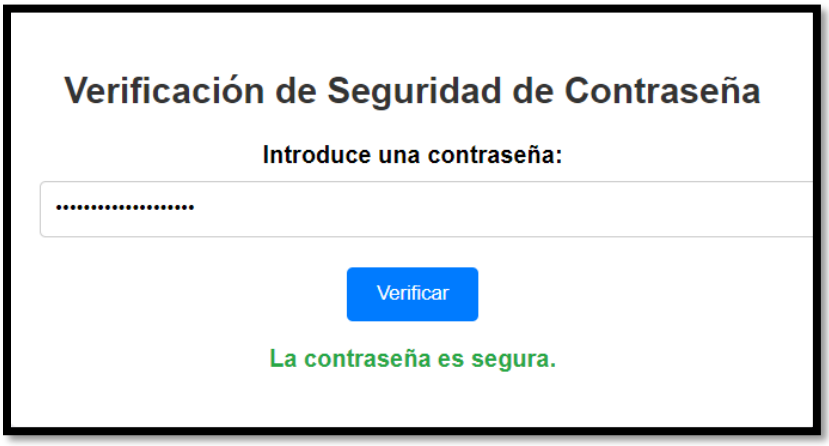


Ilustración 2: Contraseña segura.

2. Crea un programa que me recomiende una contraseña segura. La contraseña debe cumplir con los criterios de la instrucción anterior.

El segundo programa desarrollado genera automáticamente una contraseña segura que cumple con todos los criterios establecidos anteriormente. En el ejemplo siguiente, se puede observar cómo la contraseña generada incluye una

combinación de letras, números, caracteres especiales, y símbolos, garantizando así un nivel óptimo de seguridad.

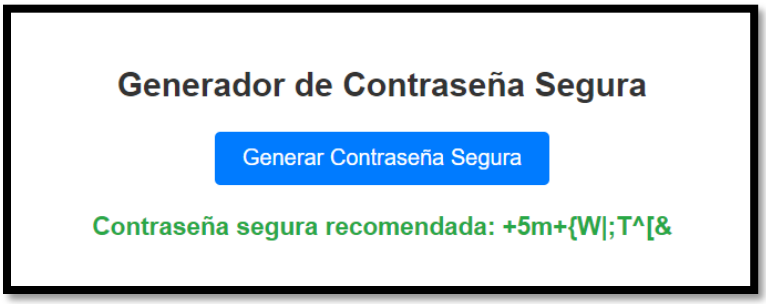


Ilustración 3: Generador de contraseña ejemplo 1.

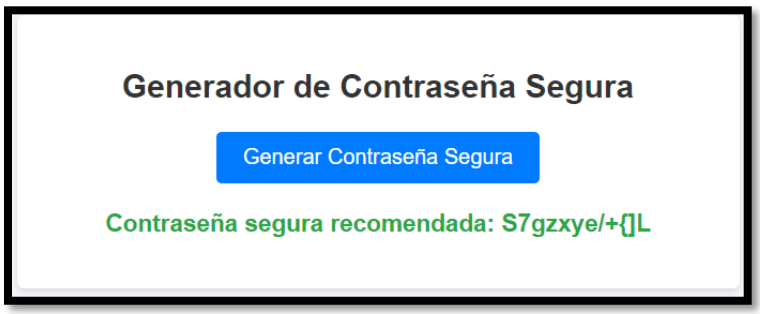


Ilustración 4: Generador de contraseña ejemplo 2.

3. Crea un certificado SSH, clave pública y clave privada, añade el certificado SSH a tu cuenta de GitHub y realiza un git clone de un repositorio nuevo utilizando la ruta SSH del repositorio.

Para crear el certificado SSH realizamos los siguientes pasos:

1. Para comenzar los primero que verificamos que tuviéramos alguna terminal adecuada para el sistema en este caso se hizo el uso de Git Bash, posteriormente ejecutamos el comando para generar la clave SSH:

ssh-keygen -t ed25519 -C "tu_correo_ejemplo@example.com"

2. Iniciamos el agente SSH ejecutando el siguiente comando:

eval "$(ssh-agent -s)"

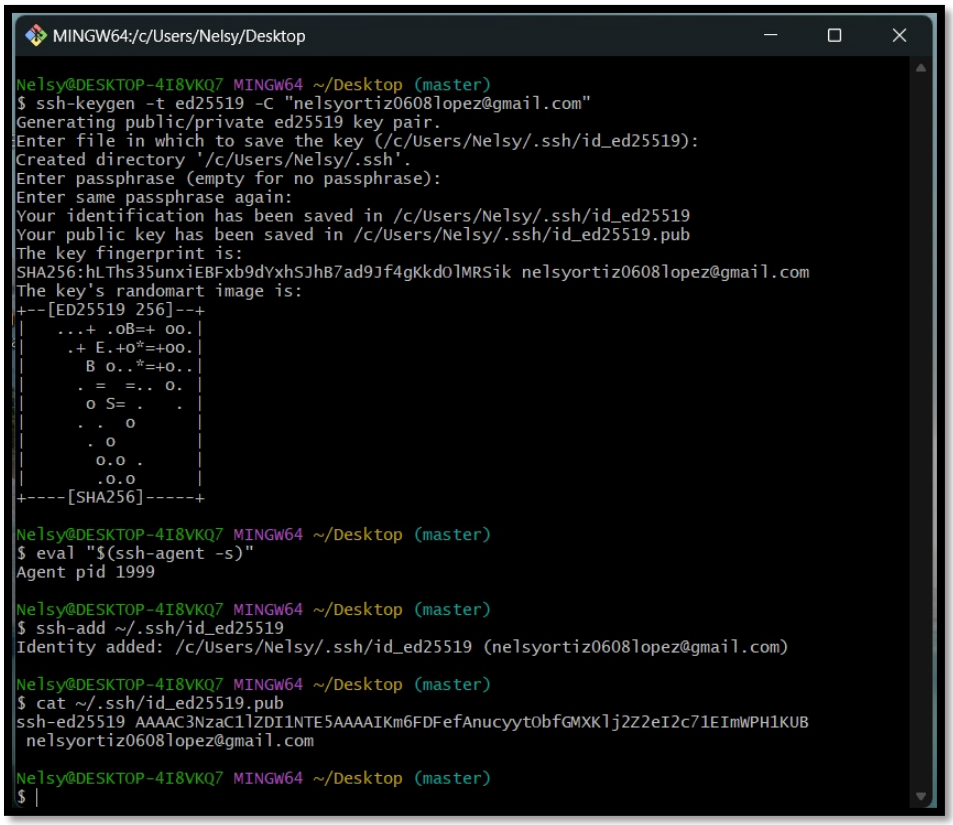


Ilustración 5: Código para crear SSH usuario 1.

3. Paso 3: Añadir la Clave Pública a la Cuenta de GitHub

Copiar la clave pública generada: Utiliza el siguiente comando para mostrar la clave pública en la terminal y cópiala al portapapeles:

4. Una vez realizado eso accedemos a nuestro perfil de de GitHub para acceder a la configuración ssh, en donde se añade la clave ssh.

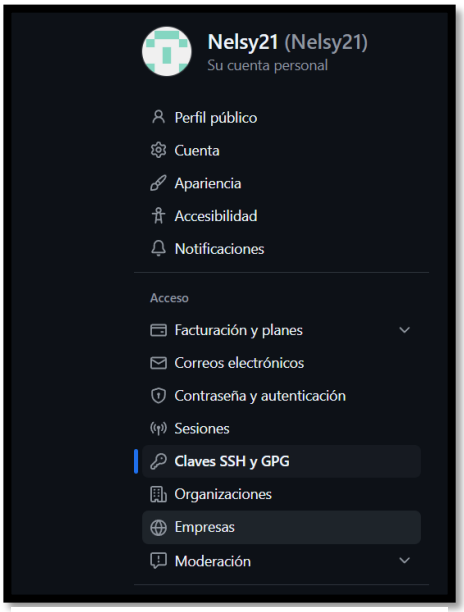


Ilustración 6: Perfil de GitHub.

RESULTADO:

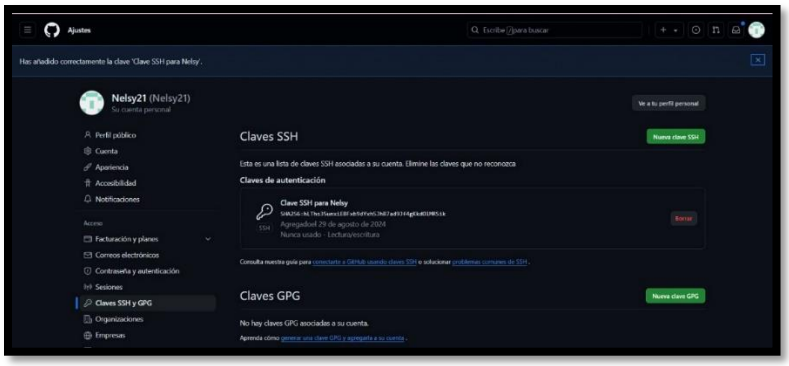


Ilustración 7: SSH usuario 1

INTEGRANTE 2.

A continuación, se presentan las capturas de pantalla que demuestran la ejecución del procedimiento por parte de cada miembro del equipo de trabajo. Estas evidencias visuales muestran cómo cada usuario completó correctamente los pasos descritos para la configuración de la clave SSH y la clonación del repositorio desde GitHub.

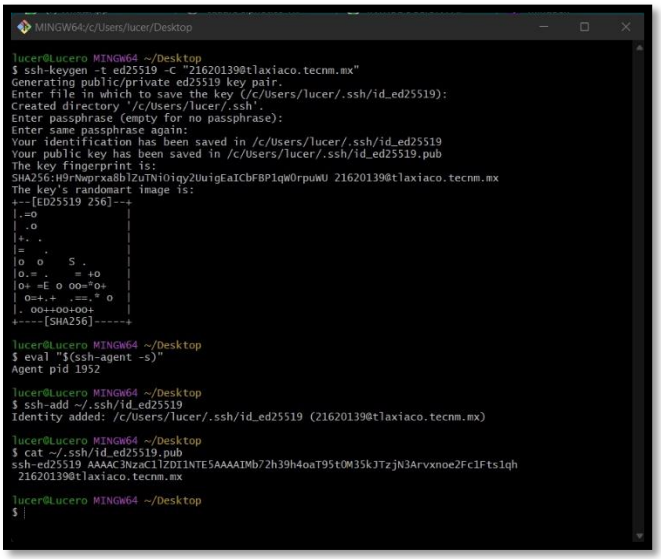


Ilustración 8: Código para crear SSH usuario 2.

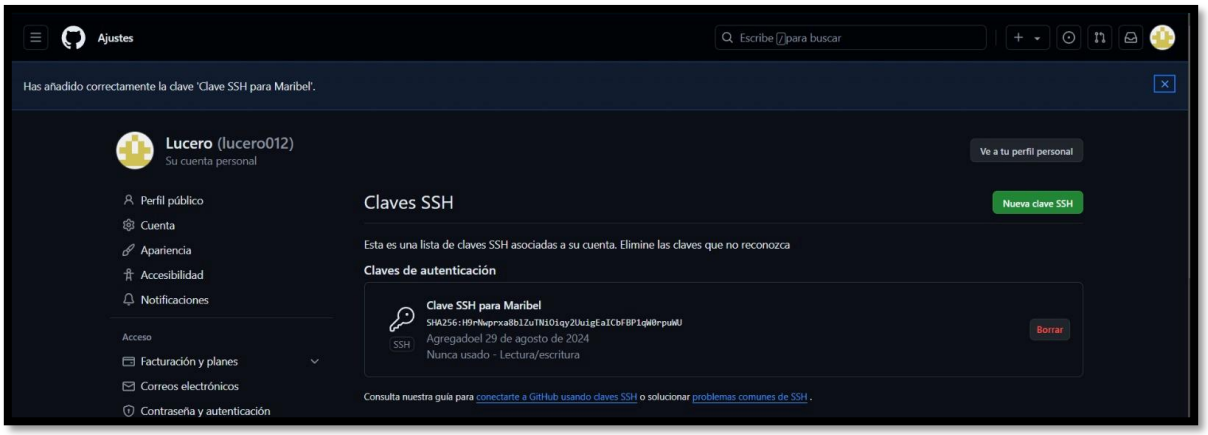


Ilustración 9: SSH usuario 2

INTEGRANTE 3.

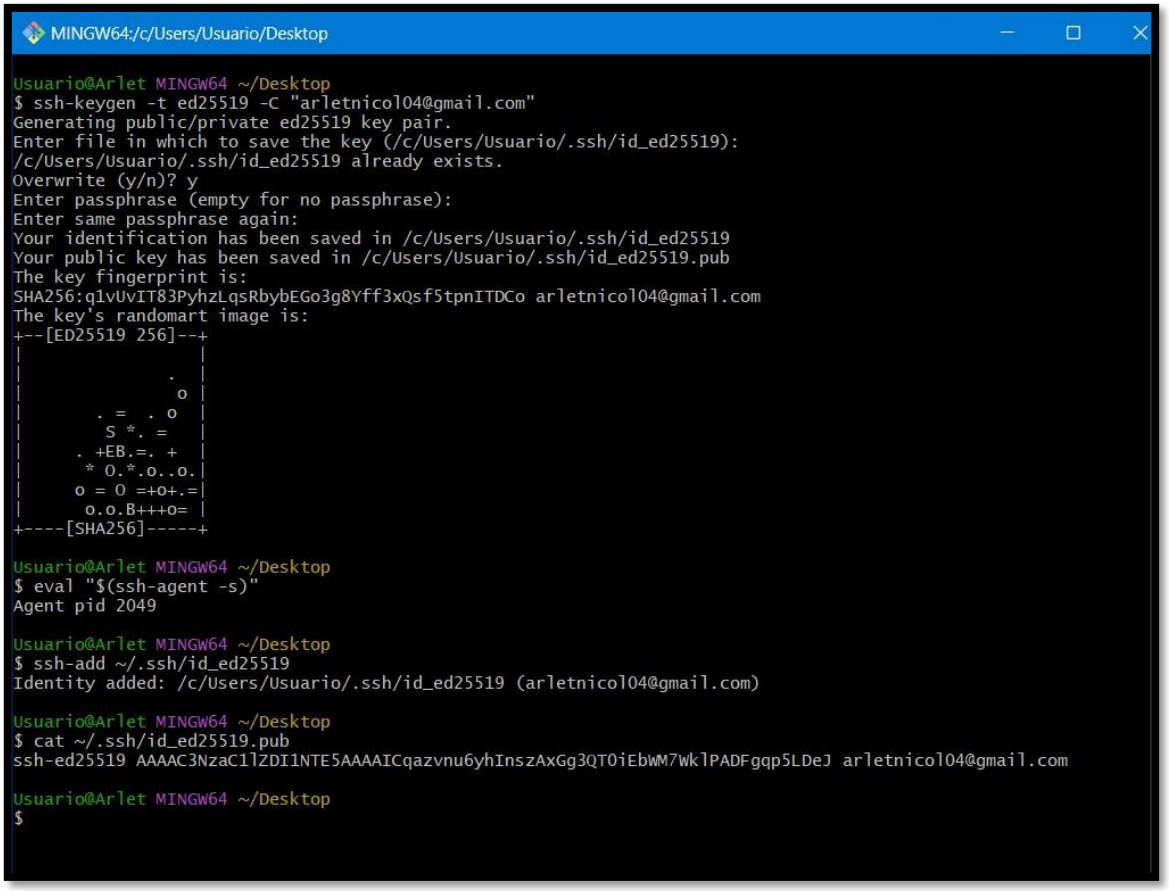


Ilustración 10: Código para crear SSH usuario 3.

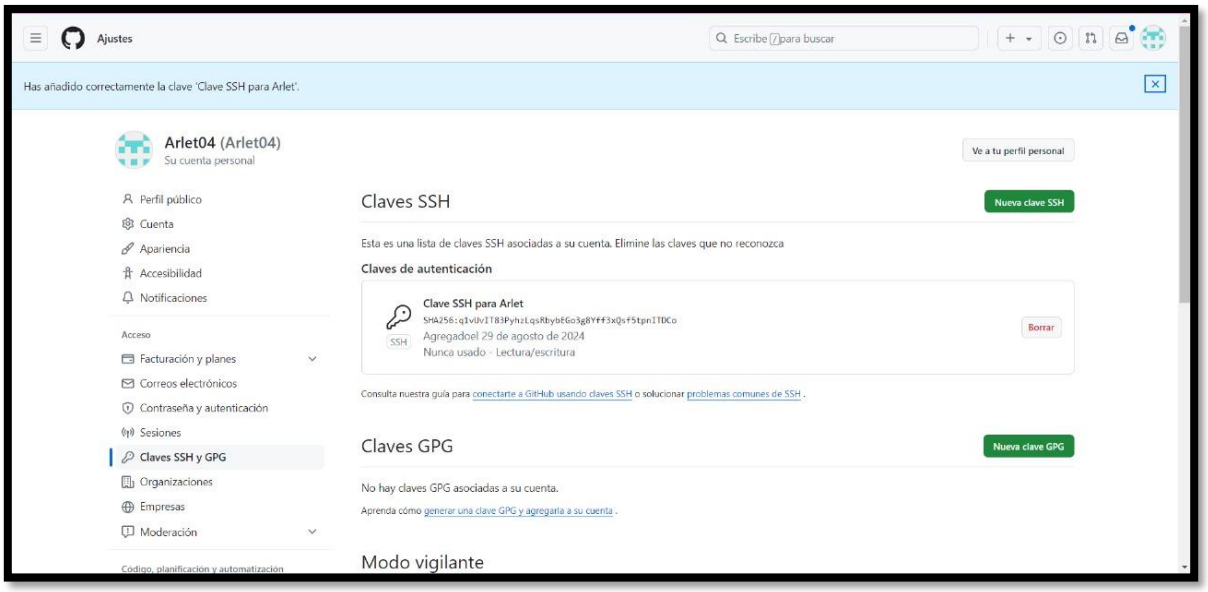
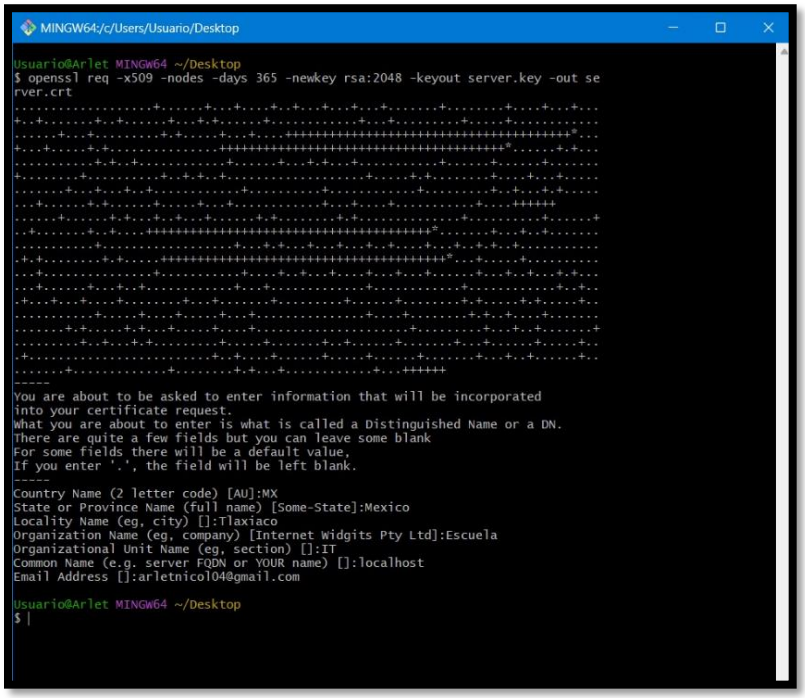
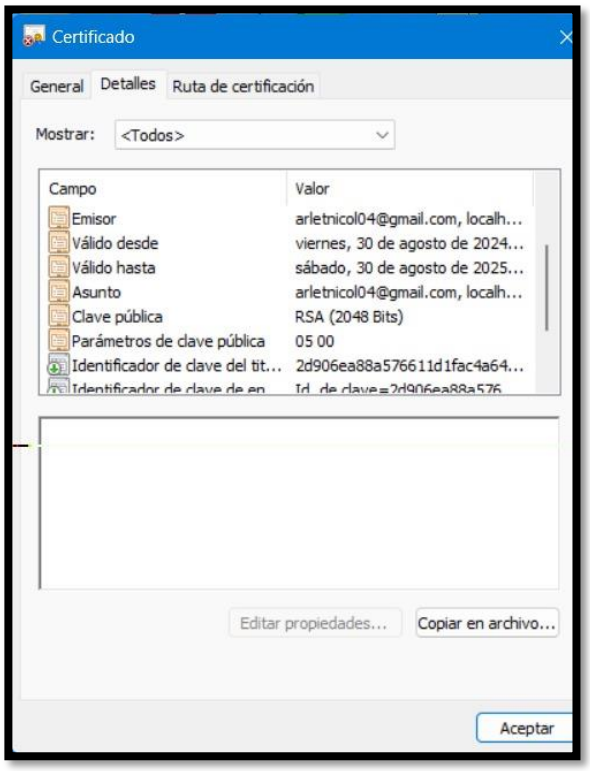


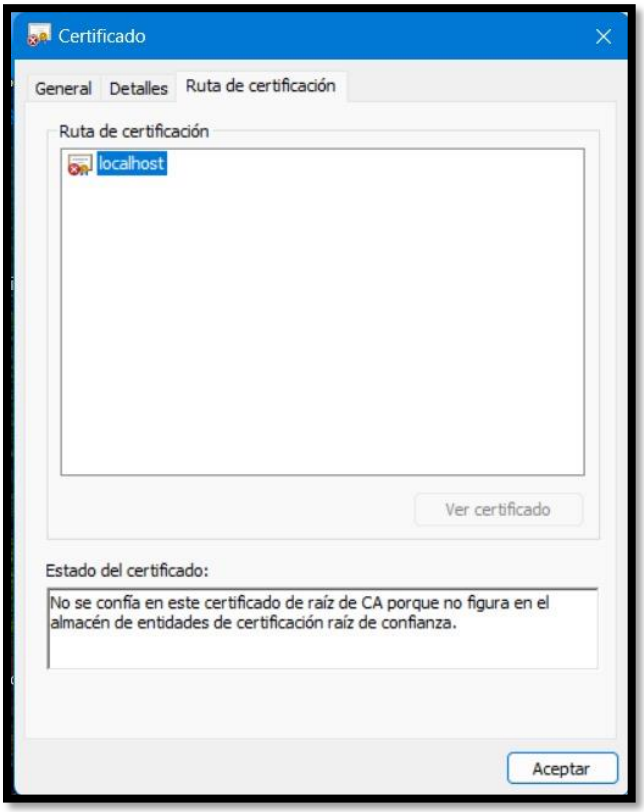
Ilustración 11: SSH usuario 3.

4. Crea un certificado SSL autofirmado con una validez de 365 días y añádelo a un servidor web local. Realiza una petición GET al servidor web local utilizando curl y muestra el certificado SSL.




Certificado
General
Detalles
Ruta de certificación
Información del certificado
Este certificado raíz de la entidad de certificación no es de confianza. Para habilitar la confianza, instale este certificado en el almacén de entidades de certificación raíz de confianza.
Emitido para: localhost
Emitido por: localhost
Válido desde 30/08/2024 hasta 30/08/2025
Instalar certificado...
Declaración del emisor
Aceptar


Certificado
General
Detalles
Ruta de certificación
Mostrar: <Todos>
Campo
Valor
Emisor
arletnicol04@gmail.com, localh...
Válido desde
viernes, 30 de agosto de 2024...
Válido hasta
sábado, 30 de agosto de 2025...
Asunto
arletnicol04@gmail.com, localh...
Clave pública
RSA (2048 Bits)
Parámetros de clave pública
05 00
Identificador de clave del tit...
2d906ea88a576611d1fac4a64...
Editar propiedades...
Copiar en archivo...
Aceptar


Certificado
General
Detalles
Ruta de certificación
Ruta de certificación
localhost
Ver certificado
Estado del certificado:
No se confía en este certificado de raíz de CA porque no figura en el almacén de entidades de certificación raíz de confianza.
Aceptar

5. **Investiga y describe los siguientes conceptos:**

Contraseña:

Es una secuencia de caracteres que se utiliza para autenticar o verificar la identidad de un usuario en un sistema o servicio. Las contraseñas deben ser lo suficientemente complejas para proteger el acceso no autorizado y evitar que sean adivinadas fácilmente. (enterprise, s.f.)

Certificado digital:

Es un documento electrónico emitido por una autoridad de certificación que asocia una clave pública con la identidad del propietario del certificado. Los certificados digitales se utilizan para asegurar comunicaciones electrónicas y verificar la identidad de las partes involucradas en transacciones en línea.

Firma digital:

Es un mecanismo criptográfico que se utiliza para verificar la autenticidad e integridad de un mensaje, documento o software. Una firma digital es creada utilizando la clave privada del firmante y puede ser verificada por cualquier persona que tenga acceso a la clave pública correspondiente, garantizando así que el contenido no ha sido alterado y que proviene del firmante indicado.

Cifrado simétrico:

Es un método de cifrado en el cual la misma clave se utiliza tanto para cifrar como para descifrar los datos. Debido a su simplicidad y eficiencia, el cifrado simétrico es adecuado para grandes volúmenes de datos, aunque requiere que ambas partes compartan de forma segura la clave de cifrado.

Cifrado asimétrico:

También conocido como cifrado de clave pública, es un método de cifrado que utiliza un par de claves: una clave pública para cifrar los datos y una clave privada para

descifrarlos. A diferencia del cifrado simétrico, el cifrado asimétrico no requiere compartir una clave secreta entre las partes, lo que mejora la seguridad en las comunicaciones.

Hash:

Es una función que toma una entrada de datos y genera una salida de longitud fija, normalmente una cadena de caracteres alfanumérica. Las funciones de hash se utilizan comúnmente para verificar la integridad de los datos, ya que cualquier cambio en la entrada resulta en una salida de hash completamente diferente. Los hashes son fundamentales en la seguridad informática, especialmente en la gestión de contraseñas y la verificación de archivos.

Encriptación:

Es el proceso de convertir datos en un formato ininteligible para proteger su confidencialidad. La encriptación se utiliza para asegurar la información tanto en tránsito como en reposo, garantizando que solo las partes autorizadas puedan acceder a los datos originales mediante el uso de una clave para descifrar la información. La encriptación puede ser simétrica o asimétrica, dependiendo del método de cifrado utilizado.

6. **Investiga y describe los siguientes algoritmos de cifrado:**

AES (Estándar de Cifrado Avanzado):

Algoritmo de cifrado simétrico que utiliza la misma clave para cifrar y descifrar datos. Es ampliamente utilizado para proteger datos sensibles debido a su alta eficiencia y seguridad.

RSA (Rivest-Shamir-Adleman):

Algoritmo de cifrado asimétrico que utiliza un par de claves (pública y privada) para cifrar y descifrar datos. Es uno de los métodos más seguros para la transmisión de información sensible y para la autenticación digital.

SHA-256 (Algoritmo Hash Seguro de 256 bits):

Algoritmo de hash criptográfico que genera una cadena de 256 bits a partir de una entrada de cualquier longitud. Es utilizado para asegurar la integridad de los datos, como en la verificación de archivos y en blockchain.

7. **Investiga y describe los siguientes estándares de cifrado:**

SSL:

Tecnología estandarizada que permite cifrar el tráfico de datos entre un navegador web y un sitio web (o entre dos servidores web), protegiendo así la conexión, Esto impide que un hacker pueda ver o interceptar la información que se transmite de un punto a otro, la cual puede contener datos personales o financieros.

TLS:

Versión actualizada y más segura de SSL. Aunque seguimos refiriéndonos a nuestros certificados de seguridad como «certificados SSL» porque ese es el término más extendido, todos los certificados de DigiCert utilizan la tecnología TLS más moderna y son de plena confianza.

8. **Investiga y describe los siguientes protocolos de seguridad:**

HTTPS (Protocolo de transferencia de hipertexto seguro):

Se utiliza en internet para proteger la transferencia de datos entre un navegador web y un servidor web. Utiliza cifrado SSL/TLS para garantizar la confidencialidad, integridad y autenticación de los datos transmitidos.

SFTP (Protocolo de transferencia segura de archivos):

Basado en SSH (Secure Shell) que proporciona un método para transferir archivos y gestionar datos de manera segura a través de una conexión encriptada, evitando la interceptación y manipulación de datos.

SSH (Secure Shell):

Protocolo de red utilizado para operar servicios de red de forma segura a través de una red insegura. SSH proporciona una forma segura de acceder a un ordenador remoto y gestionar la transmisión de comandos y datos cifrados, garantizando la confidencialidad e integridad de la comunicación.

CONCLUSION:

Como ingenieros en sistemas, es fundamental tener un conocimiento sólido sobre conceptos de seguridad digital y virtualización. Estos temas son importantes para proteger la información y los sistemas frente a posibles amenazas en un mundo cada vez más digitalizado.

Lo aprendido en esta práctica incluye cómo funcionan las contraseñas, certificados digitales, firmas digitales, y diferentes métodos de cifrado como el simétrico y asimétrico. Además, se estudian algoritmos específicos como AES, RSA y SHA-256, que son esenciales para la protección de datos.

También es importante entender los estándares y protocolos de seguridad como SSL, TLS, HTTPS, SFTP y SSH, que garantizan la seguridad de la información en tránsito y almacenada. Estos conocimientos no solo ayudan a mantener la privacidad y la integridad de los datos, sino que también permiten a los ingenieros diseñar sistemas que resistan ataques y accesos no autorizados.

La importancia de estos conceptos en la vida diaria es evidente. Desde proteger la información personal hasta asegurar transacciones bancarias y comunicaciones corporativas, la seguridad informática es vital para proteger la información sensible y mantener la confianza en las plataformas digitales. Como ingenieros, es nuestra responsabilidad garantizar que los sistemas que desarrollamos sean seguros y confiables para los usuarios.

BIBLIOGRAFÍA.

- docusign. (s.f.). *docusign*. Retrieved 30 de agosto de 2024, from https://www.docusign.com/es-mx/blog/desarrolladores/firma-digital-seguridad-informatica
- *enterprise*. (s.f.). Retrieved 30 de Agosto de 2024, from https://enterprise.arcgis.com/es/web-adaptor/10.3/install/iis/enable-https-on-your-web-server-portal-.htm
- INGENIUS. (s.f.). *Demostración de cifrado simético y asimétrico.* Retrieved 30 de agosto de 2024, from https://dspace.ups.edu.ec/bitstream/123456789/8185/1/Demostraci%C3%B3n%20de%20cifrado%20sim%C3%A9trico%20y%20asim%C3%A9trico.pdf