Tecnológico Nacional de México
Instituto Tecnológico de Tlaxiaco

Carrera: **Ingeniería en Sistemas Computacionales**

Materia: **Seguridad Y Virtualización**

Tema: **Introducción a la seguridad de la información**

Actividad: **Reporte de Practica**

Alumnos: Feria Ortiz Eduardo Tomas **21620095**
Reyes Peña Isaí **21620053**
Zárate Reyes Irving **20620166**

Grupo: **6US**

Catedrático: **Ing. Osorio Salinas Edward**

Heroica Ciudad de Tlaxiaco.
Viernes, 30 de agosto de 2024.

índice

Actividad 1.

Crea un programa en Python que permita al usuario ingresar una contraseña y que valide si la contraseña es segura o no.

```
#include <iostream>
#include <string>
#include <cctype>

bool esSegura(const std::string& contrasena) {
    if (contrasena.length() < 8) {
        return false;
    }

    bool tieneMayuscula = false, tieneMinuscula = false;
    bool tieneNumero = false, tieneEspecial = false;

    for (size_t i = 0; i < contrasena.length(); ++i) {
        if (isspace(contrasena[i])) {
            return false;
        }
        if (isupper(contrasena[i])) {
            tieneMayuscula = true;
        }
        if (islower(contrasena[i])) {
            tieneMinuscula = true;
        }
        if (isdigit(contrasena[i])) {
            tieneNumero = true;
        }
        if (ispunct(contrasena[i])) {
            tieneEspecial = true;
        }

        if (i > 1 && contrasena[i] == contrasena[i-1] && contrasena[i] == contrasena[i-2]) {
            return false;
        }
    }

    return tieneMayuscula && tieneMinuscula && tieneNumero && tieneEspecial;
}

int main() {
```

```
    std::string contrasena;

    std::cout << "Ingrese una contraseña: ";
    std::getline(std::cin, contrasena);

    if (esSegura(contrasena)) {
        std::cout << "La contraseña es segura.\n";
    } else {
        std::cout << "La contraseña no es segura.\n";
    }

    return 0;
}
```

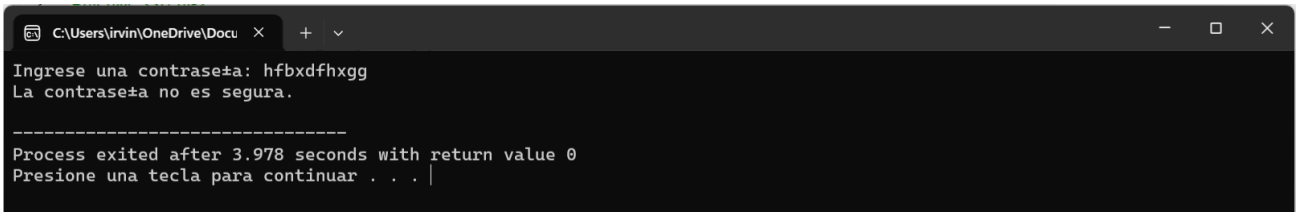


Ilustración 1 - Contraseña no segura

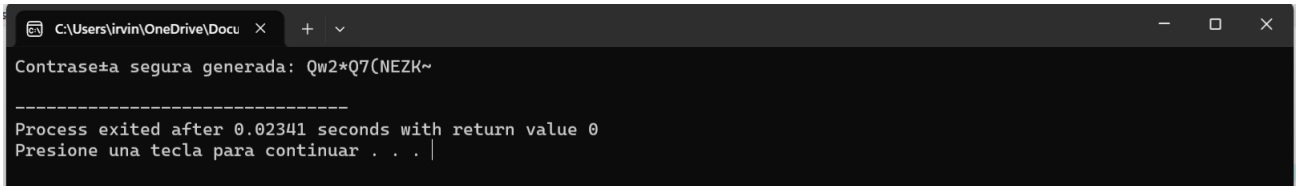
Ilustración 2 - Contraseña Segura

Actividad 2.-

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

```
#include <iostream>
#include <string>
#include <cstdlib>
#include <ctime>

std::string generarContrasenaSegura() {
    const int longitud = 12;
    const std::string mayusculas = "ABCDEFGHIJKLMNOPQRSTUVWXYZ";
    const std::string minusculas = "abcdefghijklmnopqrstuvwxyz";
    const std::string numeros = "0123456789";
    const std::string especiales = "!@#$%^&*()-_=+[]{}|\\;:'\",.<>/?~";

    std::string contrasena;
    contrasena += mayusculas[rand() % mayusculas.size()];
    contrasena += minusculas[rand() % minusculas.size()];
    contrasena += numeros[rand() % numeros.size()];
    contrasena += especiales[rand() % especiales.size()];


    const std::string todos = mayusculas + minusculas + numeros + especiales;
    while (contrasena.size() < longitud) {
        char nuevoCaracter = todos[rand() % todos.size()];


        if (contrasena.size() > 1) {
            char penultimoCaracter = contrasena[contrasena.size() - 1];
            char antepenultimoCaracter = contrasena[contrasena.size() - 2];
            if (nuevoCaracter == penultimoCaracter && nuevoCaracter == antepenultimoCaracter) {
                continue;
            }
        }

        contrasena += nuevoCaracter;
    }

    return contrasena;
}
```

```
int main() {
    srand(time(0));

    std::string contrasenaSegura = generarContrasenaSegura();
    std::cout << "Contraseña segura generada: " << contrasenaSegura << std::endl;

    return 0;
}
```



Actividad 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.

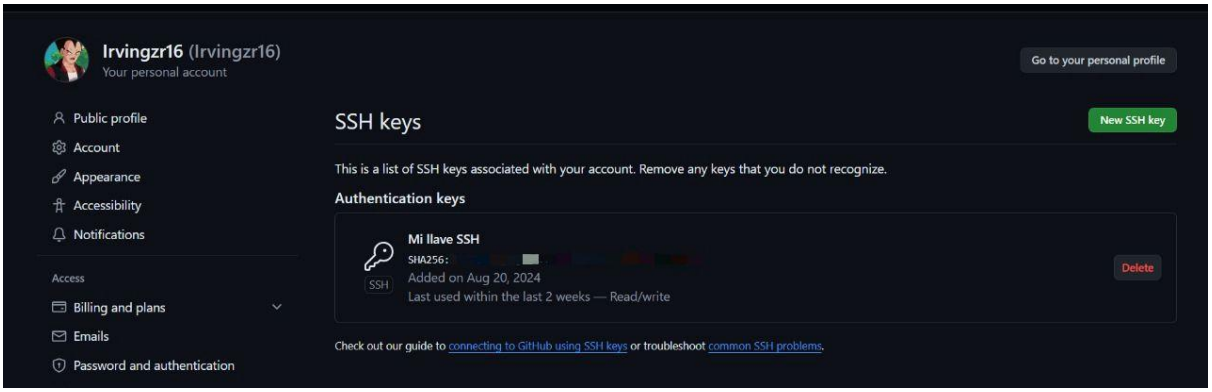


Ilustración 3 - Creación de la clave SSH - Irving

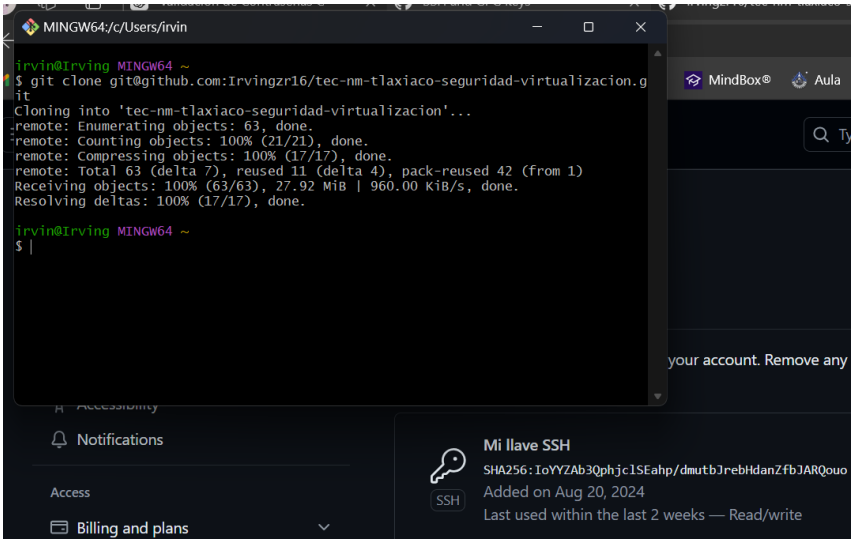


Ilustración 4 - - Comprobación de la clave SSH - Irving

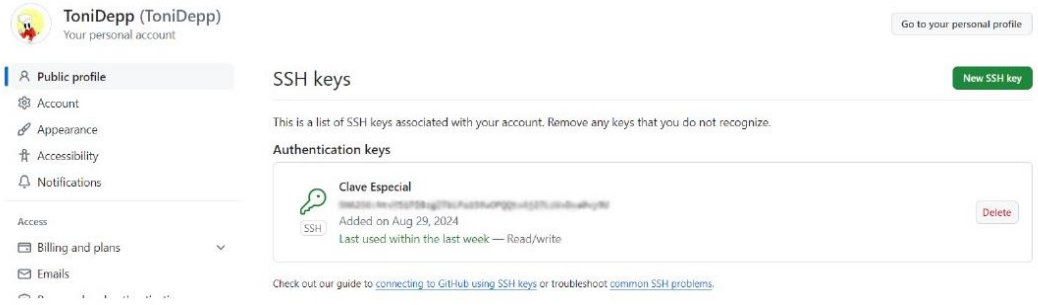


Ilustración 5 - - Creación de la clave SSH - Eduardo

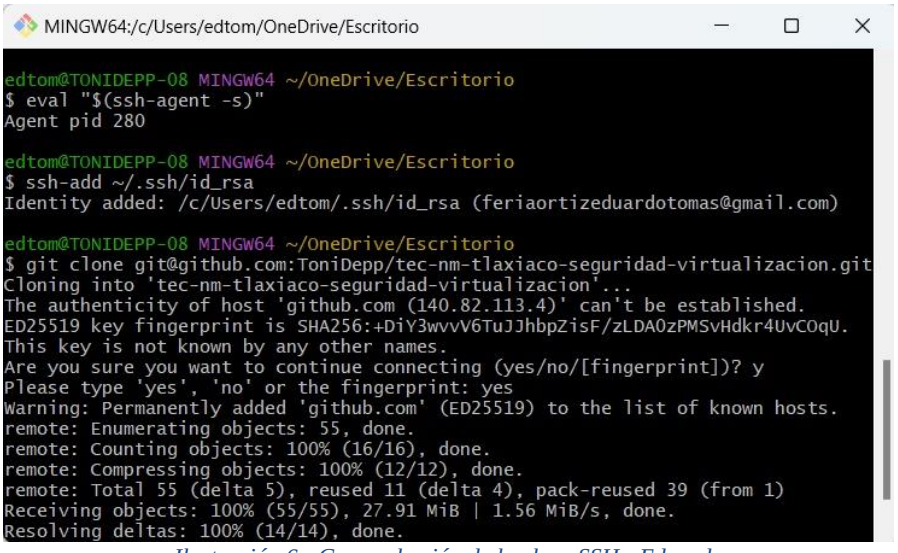


Ilustración 6 - Comprobación de la clave SSH - Eduardo

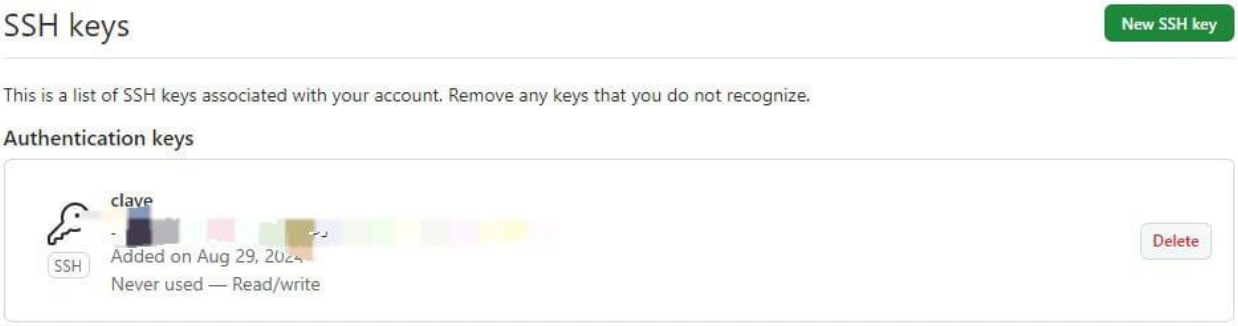


Ilustración 7 - Creación de la clave SSH - Isaí

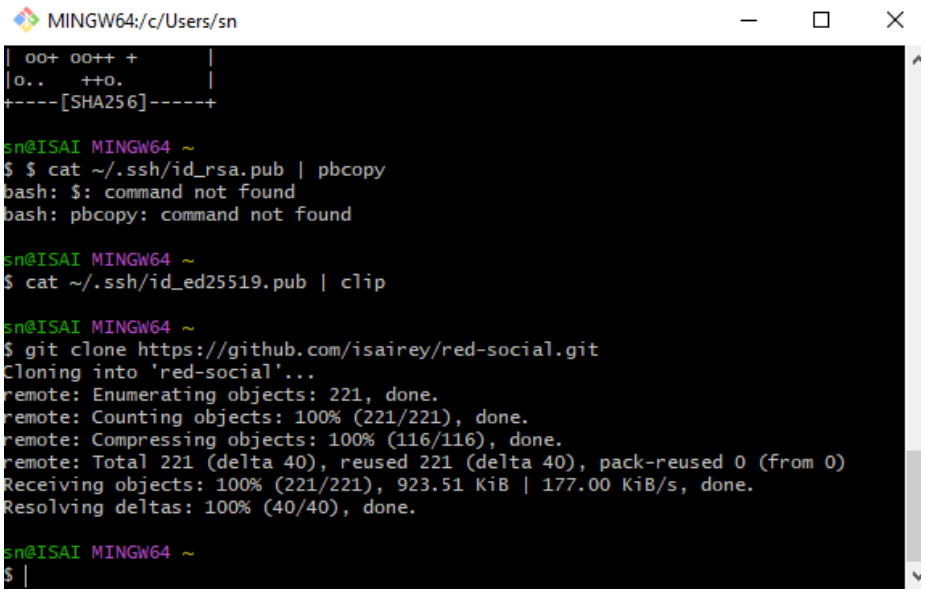
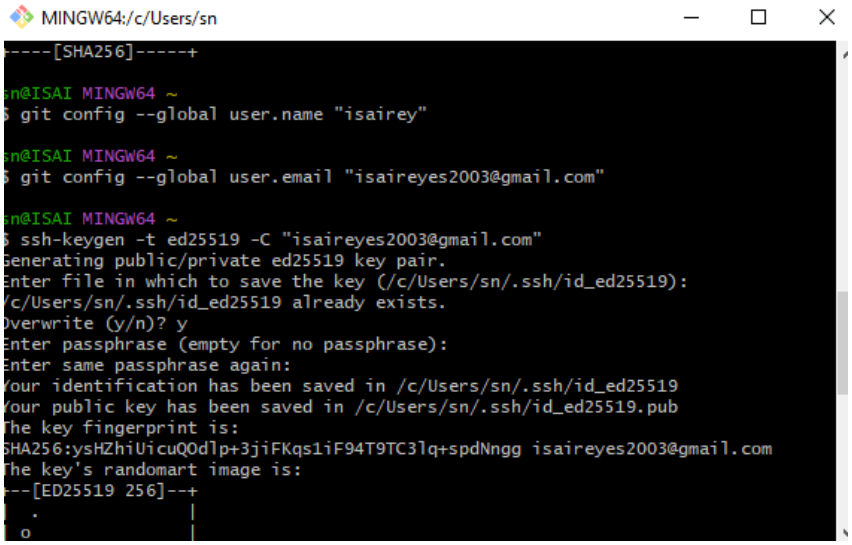
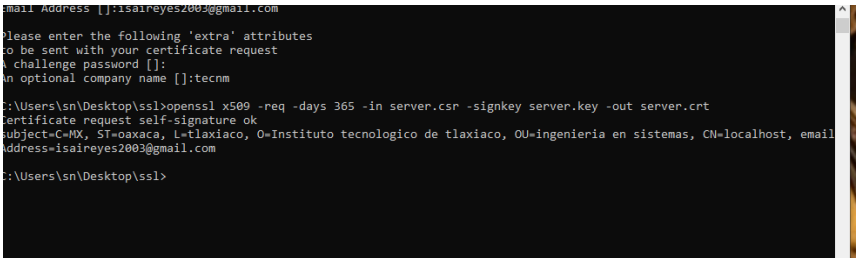


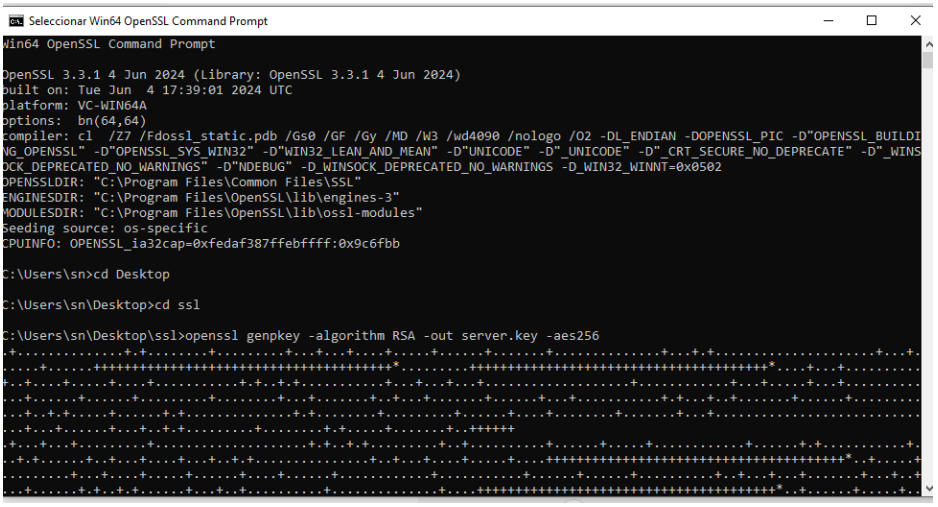
Ilustración 8 - Comprobación de la clave SSH - Isaí

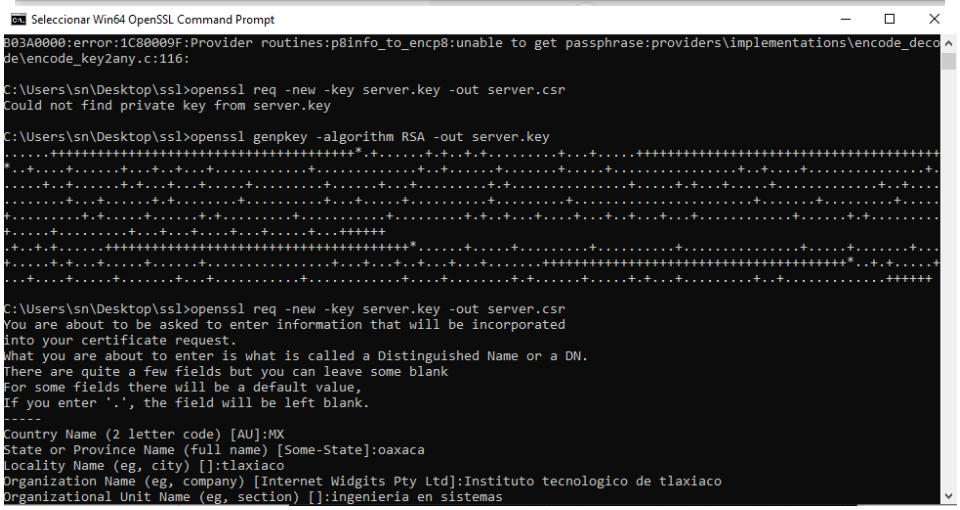
Actividad 4.

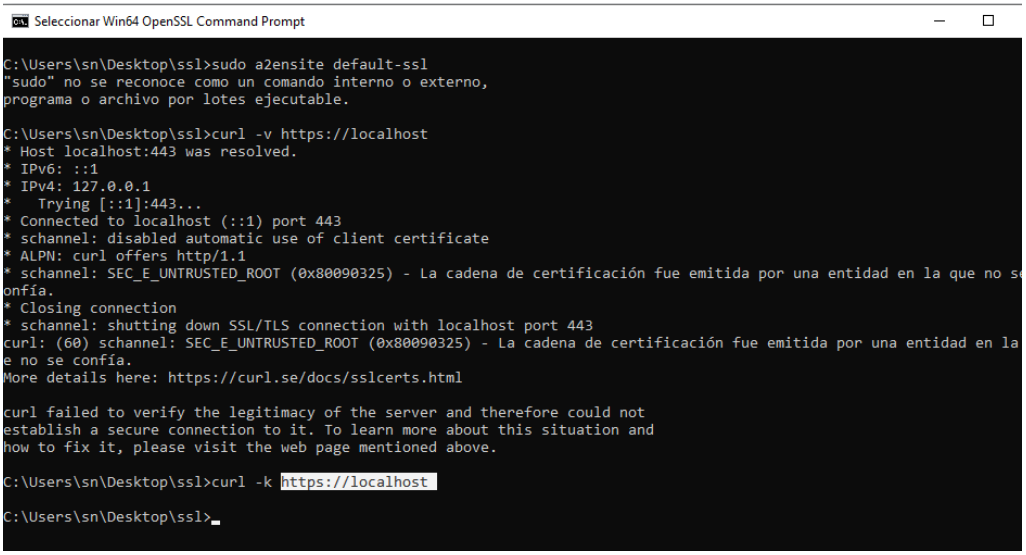
Crea un certificado SSL autofirmado con una validez de 365 días y añádelo a un servidor web local. Realiza una petición GET al servidor web local utilizando curl y muestra el certificado SSL.






Seleccionar Win64 OpenSSL Command Prompt
Win64 OpenSSL Command Prompt
OpenSSL 3.3.1 4 Jun 2024 (Library: OpenSSL 3.3.1 4 Jun 2024)
built on: Tue Jun 4 17:39:01 2024 UTC
platform: VC-WIN64A
options: bn(64,64)
compiler: cl /Z7 /Fdossl_static.pdb /Gs0 /GF /Gy /MD /W3 /wd4090 /nologo /O2 -DL_ENDIAN -DOPENSSL_PIC -D"OPENSSL_BUILDING_OPENSSL" -D"OPENSSL_SYS_WIN32" -D"WIN32_LEAN_AND_MEAN" -D"UNICODE" -D"_UNICODE" -D"_CRT_SECURE_NO_DEPRECATE" -D"_WINSOCK_DEPRECATED_NO_WARNINGS" -D"NDEBUG" -D_WINSOCK_DEPRECATED_NO_WARNINGS -D_WIN32_WINNT=0x0502
OPENSSLDIR: "C:\Program Files\Common Files\SSL"
ENGINESDIR: "C:\Program Files\OpenSSL\lib\engines-3"
MODULESDIR: "C:\Program Files\OpenSSL\lib\ossl-modules"
Seeding source: os-specific
CPUINFO: OPENSSL_ia32cap=0xfedaf387ffebffff:0x9c6fbb
C:\Users\sn>cd Desktop
C:\Users\sn\Desktop>cd ssl
C:\Users\sn\Desktop\ssl>openssl genpkey -algorithm RSA -out server.key -aes256


Seleccionar Win64 OpenSSL Command Prompt
803A0000:error:1C80009F:Provider routines:p8info_to_encp8:unable to get passphrase:providers\implementations\encode_decode\encode_key2any.c:116:
C:\Users\sn\Desktop\ssl>openssl req -new -key server.key -out server.csr
Could not find private key from server.key
C:\Users\sn\Desktop\ssl>openssl genpkey -algorithm RSA -out server.key
C:\Users\sn\Desktop\ssl>openssl req -new -key server.key -out server.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
Country Name (2 letter code) [AU]:MX
State or Province Name (full name) [Some-State]:oaxaca
Locality Name (eg, city) []:tlaxiaco
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Instituto tecnologico de tlaxiaco
Organizational Unit Name (eg, section) []:ingenieria en sistemas



Actividad 5.

Investiga y describe los siguientes conceptos:

- **Contraseña:** Una contraseña es una combinación de números, letras y símbolos creada para proteger la información y los datos personales que tienes almacenados en tus computadoras, tabletas y celulares. (como crear una contraseña segura, 2024)
- **Certificado digital:** Los certificados digitales son el equivalente digital del DNI, en lo que a la autentificación de individuos se refiere, ya que permiten que un individuo demuestre que es quien dice ser, es decir, que esta en posesión de la clave secreta asociada a un certificado. Para los usuarios proporciona un mecanismo para verificar la autenticidad de programas y documentos obtenidos a través de la red. (Talens-Oliag, 2008)

- **Firma digital:** Una firma digital es un dato en formato electrónico que sirve como mecanismo para verificar la autenticidad e integridad4 de otro dato también en formato electrónico (a este último, nos referiremos como dato firmado). Una firma digital es un tipo de firma electrónica5 generada por un procedimiento criptográfico que establece una relación única y exclusiva entre el dato firmado y el firmante. (Cuno, 2015)
- **Cifrado asimétrico:** El cifrado asimétrico se lo emplea muy frecuente para pasar con seguridad una clave privada, que posteriormente, será la que se utilice para cifrar y/o descifrar otra información. (Mendoza, 2008)
- **Hash:** Método para convertir una clave dada en una dirección, con el fin de obtener la ruta específica del mismo dentro de un conjunto superior de datos. Dicha ruta se obtiene mediante el uso de procedimientos matemáticos traducidos a algoritmos con el propósito de ser aplicados en sistemas de seguridad, mensajería, banca, administración de datos y otros. (Tejedor-Morales)
- **Encriptación:** La encriptación o cifrado es un mecanismo de seguridad que permite modificar un mensaje de modo que su contenido sea ilegible, salvo para su destinatario. De modo inverso, la desencriptación o descifrado permitirá hacer legible un mensaje que estaba cifrado. (electrónica, s.f.)

Actividad 6.

Investiga y describe los siguientes algoritmos de cifrado:

- **AES:** AES es un algoritmo de cifrado por bloques, inicialmente fue diseñado para tener longitud de bloque variable pero el estándar define un tamaño de bloque de 128 bits, por lo tanto los datos a ser encriptados se dividen en segmentos de 16 bytes (128 bits) y cada segmento se lo puede ver como un bloque o matriz de 4x4 bytes al que se lo llama estado. (Pousa, 2011)
- **RSA:** RSA es un algoritmo de cifrado asimétrico que se utiliza ampliamente para la transmisión segura de datos. Fue desarrollado en 1977 por Ron Rivest, Adi Shamir y Leonard Adleman, de quienes toma su nombre. RSA se

basa en la dificultad de factorizar grandes números primos, lo que hace que la criptografía RSA sea segura y eficiente para el cifrado y la firma digital. El proceso de RSA implica la generación de una clave pública para encriptar datos y una clave privada para desencriptarlos. (Rivest, 1978)

- **SHA-256:** SHA-256 es un algoritmo de hash criptográfico que pertenece a la familia de funciones hash seguras (SHA). Fue desarrollado por la Agencia de Seguridad Nacional de los Estados Unidos (NSA) y se publicó en 2001 como parte del estándar SHA-2. SHA-256 produce un resumen de mensaje (hash) de 256 bits a partir de una entrada de cualquier longitud, lo que lo hace adecuado para aplicaciones de seguridad como la verificación de integridad de datos y la firma digital. A diferencia de los algoritmos de cifrado, SHA-256 no es reversible, lo que significa que no se puede obtener la entrada original a partir del hash generado. (Technology., 2002)

Actividad 7.

Investiga y describe los siguientes estándares de cifrado:

- **SSL:** SSL (Secure Sockets Layer) es un protocolo criptográfico diseñado para proporcionar seguridad en la comunicación a través de redes como Internet. Fue desarrollado por Netscape en 1994 y se utiliza para asegurar la transmisión de datos entre un cliente y un servidor, garantizando que la información intercambiada esté cifrada y, por lo tanto, protegida contra intercepciones y alteraciones. SSL opera mediante el uso de certificados digitales, que permiten verificar la identidad del servidor y establecer un canal seguro. Aunque SSL ha sido reemplazado en gran parte por su sucesor, TLS (Transport Layer Security), el término SSL aún se utiliza comúnmente para referirse a la seguridad en las conexiones web. (Mozilla., 2021)
- **TLS:** TLS (Transport Layer Security) es un protocolo criptográfico que se utiliza para garantizar la privacidad e integridad de los datos transmitidos a través de redes como Internet. TLS es el sucesor de SSL (Secure Sockets

Layer) y se introdujo en 1999 para corregir las vulnerabilidades y mejorar la seguridad de su predecesor. TLS opera mediante el cifrado de los datos intercambiados entre un cliente y un servidor, y utiliza certificados digitales para autenticar la identidad de los servidores. Es ampliamente utilizado para asegurar las comunicaciones web, como en el protocolo HTTPS, y es esencial para la protección de datos sensibles como información personal y financiera. (España., 2019)

Actividad 8.

Investiga y describe los siguientes protocolos de seguridad:

- **HTTPS:** HTTPS (HyperText Transfer Protocol Secure) es una versión segura del protocolo HTTP, que se utiliza para la transferencia de datos en la web. HTTPS cifra la comunicación entre el navegador del usuario y el servidor, utilizando protocolos como SSL o TLS, para proteger la información sensible contra interceptaciones y ataques. Es esencial para transacciones en línea, acceso a cuentas personales, y cualquier situación en la que se maneje información confidencial. (Datos., 2020)
- **SFTP:** SFTP (Secure File Transfer Protocol) es un protocolo de red que permite la transferencia segura de archivos entre sistemas, utilizando el protocolo SSH (Secure Shell) para cifrar tanto los comandos como los datos. A diferencia de FTP, SFTP garantiza que la información intercambiada no sea vulnerable a ataques, proporcionando autenticación y encriptación. Es comúnmente utilizado para transferir datos sensibles y realizar copias de seguridad de manera segura. (España., SFTP: Transferencia segura de archivos, 2018)
- **SSH:** SSH (Secure Shell) es un protocolo de red que permite la administración y transferencia segura de datos entre dispositivos remotos. SSH proporciona autenticación sólida y encriptación de la información transmitida, lo que asegura que las comunicaciones y los comandos

enviados entre el cliente y el servidor estén protegidos contra ataques. Es ampliamente utilizado para la administración remota de servidores y sistemas, así como para la transferencia segura de archivos. (Mozilla., SSH: Seguridad en las comunicaciones remotas. , 2020)

Conclusión.

Después de esta serie de investigaciones y prácticas, podemos concluir que la seguridad de la información es un aspecto fundamental en el ámbito de la tecnología y la computación. A lo largo de las actividades realizadas, hemos repasado conceptos clave como la creación de contraseñas seguras, la generación y uso de certificados digitales y algoritmos de cifrado, y la implementación de protocolos de seguridad en la comunicación y transferencia de datos. Estas prácticas nos han permitido recordar y comprender mejor los mecanismos que protegen la integridad y confidencialidad de la información, sino también adquirir habilidades técnicas para aplicarlos en entornos reales.

Bibliografía

como crear una contraseña segura. (Junio de 2024). Obtenido de Argentina.gob.ar: https://www.argentina.gob.ar/justicia/convosenlaweb/situaciones/como-crear-una-contrase%C3%B1a-segura

Cuno, Á. L. (2015). Conceptos de firma digital. *IDENTIDAD DIGITAL*.

Datos., A. E. (2020). *HTTPS: Navegación segura en Internet.* Obtenido de Agencia Española de Protección de Datos.: https://www.aepd.es/charlas/https-navegacion-segura

electrónica, S. (s.f.). *1024 - ¿Qué es la Encriptación o Cifrado?* Obtenido de Real Casa de la Moneda - Fabrica Nacional de Moneda y Tiembre: https://www.sede.fnmt.gob.es/preguntas-frecuentes/otras-preguntas/-/asset_publisher/1RphW9IeUoAH/content/1024-que-es-la-encriptacion-o-cifrado-

España., I. N. (2018). *SFTP: Transferencia segura de archivos*. Obtenido de Instituto Nacional de Ciberseguridad de España.: https://www.incibe.es/sftp

España., I. N. (2019). *Protocolo TLS: Seguridad en las comunicaciones*. Obtenido de Instituto Nacional de Ciberseguridad de España. : https://www.incibe.es/protocolo-tls

Mendoza, J. C. (2008). Demostración de cifrado simétrico y asimétrico. *Ingenius: Revista de Ciencia y Tecnología*, pág. 8.

Mozilla., F. (2020). *SSH: Seguridad en las comunicaciones remotas.* . Obtenido de Fundación Mozilla.: https://developer.mozilla.org/es/docs/Glossary/SSH

Mozilla., F. (2021). *¿Qué es SSL y cómo funciona?* Obtenido de Mozilla.org: https://developer.mozilla.org/es/docs/Glossary/SSL

Pousa, A. (Diciembre de 2011). ALGORITMO DE CIFRADO SIMÉTRICO AES. . pág. 3.

Rivest, R. S. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*.

Talens-Oliag, S. (2008). *Introducción a los certificados digitales*. Obtenido de Universidad de Valencia, España: https://www. uv. es/sto/articulos/BEI-2003-11/certificados_digitales. html.[Accessed: 28-Enero-2018].

Technology., N. I. (2002). Secure Hash Standard (SHS). *Federal Information Processing Standards Publication*.

Tejedor-Morales, M. Y. (s.f.). HASHING. UN CONCEPTO. UNA REALIDAD. *Universidad Tecnológica de Panamá*.