Actividad 1 Lección 1

- **Paso 1: Introducción a la importancia de las contraseñas seguras (10 minutos)**
  - 📘 **Actividad Teórica**:

1. Explicar la importancia de las contraseñas seguras.
2. Describir los riesgos de contraseñas débiles.
3. Enumerar las características de una contraseña segura.

  - 🗣️ **Actividad Práctica**:
    - Realizar una discusión grupal: ¿Alguna vez han tenido una cuenta comprometida? ¿Qué aprendieron?

Actividad Teórica

1.Son la línea de defensa contra el acceso no autorizado de archivos, dispositivos y cuentas en línea. Ayudan a proteger los datos de usuario y software malintencionado previniendo ataques o robos de datos sin tu consentimiento.

2.El riesgos de contraseñas débiles puede causar estragos como robo de información confidencial suplantaciones, correos electrónicos e entidades bancarias también buscando formas mas fáciles de descifrar las para tener el control total de los datos.

3.Primero tener una longitud larga al menos de 12 a 15 caracteres, Segundo usar combinaciones de símbolos y utilizar menos números y letras entre mas mayúsculas y minúsculas, Tercero evita utilizar frases simples que encuentres por ahí o repeticiones simples como admin1234 o santi2340 o ABCD1234 también no utilices como tu numero de identificación o numero celular o el nombre de tu abuela 😊. Mejor opta por una contraseña combinada será mas seguro y será mas difícil descifrar para los hackers.

Actividad en practica

Pues la verdad si mis redes sociales ya que fue un diciembre en el cual vi en Messenger un pocotón de mensajes a personas que no conocían y después vi en la administración de dispositivos registrados y vi que alguien de otra parte del país entro a mi cuenta haciendo que por poco robe información mía y se adueñe de mi cuenta la pregunta que fue para mi en ese momento es como supo mi cuenta de Facebook.

- **Paso 2: Creación de contraseñas seguras (15 minutos)**

- 📘 **Actividad Teórica**:
    - Explicar cómo transformar una frase memorable en una contraseña segura.
    - Ejemplificar la creación paso a paso (como “M3Gu$t@EIC@f3!...”).
- 📝 **Actividad Práctica**:
    1. Pensar una frase memorable personal.
    2. Convertirla en una contraseña segura usando mayúsculas, minúsculas, números y símbolos.
    3. Compartir métodos de creación (sin decir la contraseña real) y debatir su seguridad.

Actividad teórica

Paso 1: Selecciona una frase memorable.

• Ejemplo: "Me encanta ver películas los fines de semana".

Paso 2: Transforma la frase utilizando sustituciones:

• Reemplaza letras por números y símbolos similares:

o "a" por "@"

o "e" por "3"

o "i" por "1"

o "o" por "0"

o "s" por "$"

Paso 3: Aplica mayúsculas y minúsculas y agrega símbolos:

• "M3Enc@nt@V3rP3lícul@$L0$F1n3$D3$3m@n@"

Paso 4: Verifica la complejidad y longitud:

• Asegúrate de que la contraseña tenga al menos 12 caracteres y una

combinación diversa.

ACTIVIDAD DE PRACTICA

1.Pues podemos utilizar una frase por ejemplo “me gusta el malecón” ahora usamos una serie de combinaciones con numero y símbolos y letras mayus y minus.

2.vamos ejemplificar el primer paso para que sea una contraseña combinada

Me gusta el malecón <<< COMBINADO >>> **M3gu$taElMalecón!**

En este caso estamos utilizando cualquier clase de combinación utilizando las formas que dicen en el punto anterior. aquí muestro de como fue el remplazo de cada una de las letras.

M=M

E=3

G=g

U=u

S=$ o 5

T=t

A=a

E=e

L=l

M=M

A=a

L=l

E=e

C=c

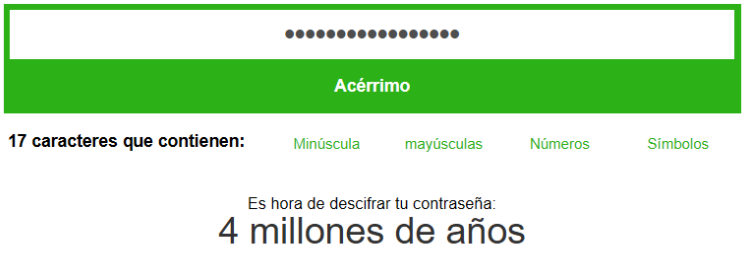
O=o

N=n

!=!

Se ve muy simple pero vamos puedes crear una mas aun difícil.

3.Ahora Veremos que longitud tiene y su dificultad y que segura es nuestra clave en este caso usare una pagina que es: https://www.passwordmonster.com/



Se puede ver en el resultado que es una contraseña muy segura con pocos caracteres pero funciona para asegurar nuestras cuentas 😊.

🔹 **Paso 3: Introducción a los gestores de contraseñas (10 minutos)**

- 📘 **Actividad Teórica**:

  a) Explicar qué es un gestor de contraseñas.

  b) Mencionar ventajas: seguridad, comodidad, accesibilidad.

  c) Destacar la importancia de una contraseña maestra fuerte.

- 🖥️ **Actividad Práctica**:

1.Demostrar cómo instalar y configurar un gestor de contraseñas (como Bitwarden).

2.Mostrar cómo crear una contraseña maestra segura.

ACTIVIDAD TEORICA

a) ¿Qué es un gestor de contraseñas?

• Definición: Aplicación que almacena y gestiona tus contraseñas de forma segura y encriptada. Algunos gestores como Bitwarden encriptan las contraseñas, lo que las protege contra el acceso no autorizado. O tambien como Smart Lock que es de Google o Otros servicios

• Funcionalidad: Genera contraseñas fuertes y autocompleta credenciales en sitios web.

b) Ventajas:

Seguridad: Almacenamiento encriptado y protección

contra accesos no autorizados.

Comodidad: No necesitas recordar múltiples contraseñas

complejas.

Organización: Centraliza la gestión de todas tus

contraseñas y notas seguras.

c) Importancia de la contraseña maestra:

Una contraseña maestra es esencial porque simplifica la gestión de contraseñas en múltiples cuentas, mejorando la seguridad y reduciendo el riesgo de hackeo. En lugar de recordar varias contraseñas, solo se necesita una clave maestra para acceder a todas. Esto no solo ahorra tiempo, sino que también hace que sea más difícil para los ciberdelincuentes comprometer la seguridad de tus cuentas.

• Clave principal: Es la única contraseña que debes recordar.

• Seguridad crítica: Debe ser extremadamente fuerte y única

• Consejos: Utiliza una frase de paso largo y aplica las técnicas de

creación de contraseñas seguras.

Ejemplo de contraseña maestra:

• Frase: "La seguridad es mi prioridad número uno".

• Transformación: "L@$3gur1d@d3$M1Pr10r1d@d#1"

ACTIVIDAD EN PRACTICA

1. Demostrar cómo instalar y configurar un gestor de contraseñas (como Bitwarden).
2. Mostrar cómo crear una contraseña maestra segura.

LA DEMOSTRACION FUE EN VIVO Y EN DIRECTO POR MICROSOFT TEAMS POR LO TANTO SE PUEDE VOLVER A VER LA GRABACION DE ESA CLASE DE COMO SE INSTALO EL PROGRAMA.

- 🔹 **Paso 4: Uso práctico de un gestor de contraseñas (15 minutos)**
  - 🖥️ **Actividad Práctica**:
    1. Instalar un gestor de contraseñas.
    2. Crear una cuenta y configurar una contraseña maestra.
    3. Generar y guardar una contraseña en el gestor (por ejemplo, para el correo).
    4. Usar la función de autocompletar para iniciar sesión en un sitio web.

Actividad en practica

Debido a la seguridad que yo ya tengo implementada descarto ese punto porque yo tengo muchas extensiones de seguridad en mi computadora y en mis cuentas no quisiera hacer mas cambios ya que la ultima vez que hice cambios de generador de autenticación perdí acceso a muchos sitios que ya que no estaban bien sincronizados con la parte principal que es google.

Yo se de tecnología pero si todo esta funcionando bien prefiero dejarlo tal y tal como esta.

- 🔹 **Paso 5: Conclusión y mejores prácticas (10 minutos)**
  - 🧠 **Actividad de Cierre**:
    - Reflexión grupal: compartir un consejo o práctica que aplicarán después del taller.

Pues el consejo que yo doy es que utilizan gestores de contraseñas muy seguros para que puedan administrar su contraseñas de sus sitios y que además usar contraseñas bien combinadas para obtener la mayor seguridad posible para evitar vulneraciones. Y pues las practicas replicarlas como ellos dicen pero si ya tienes todo configurado a tu manera mejor no mover ni tocar algo que esta funcionando bien como debe ser.

SESION 1 ACTIVIDAD 1 COMPLETADO POR EL ESTUDIANTE SANTIAGO ENRIQUE NORIEGA GARCIA TALENTO TECH CIBERSEGURIDAD.

BUEN DIA 😊