DESARROLLO DEL LABORATORIO NRO 1. BOOTCAMP DE CIBERSEGURIDAD

JHON DAVID DAZA GARCIA

Título del Laboratorio: Creación de Contraseñas Seguras y Uso de Gestores de Contraseñas

Objetivos del Laboratorio.

1. Desarrollar habilidades para crear contraseñas seguras y complejas
2. Familiarizar a los participantes con el uso de gestores de contraseñas
3. Promover prácticas de seguridad en la gestión de contraseñas

1. Introducción a la Importancia de las Contraseñas Seguras

El uso de contraseñas seguras es importante porque ayuda a proteger cuentas y datos personales de accesos no autorizados.

- Protección contra ataques de fuerza bruta: Las contraseñas seguras son más difíciles de adivinar para los atacantes que utilizan técnicas de fuerza bruta para intentar acceder a tus cuentas.
- Prevención de accesos no autorizados: Las contraseñas seguras ayudan a prevenir que personas no autorizadas accedan a tus cuentas y datos personales.
- Protección de la identidad: Las contraseñas seguras ayudan a proteger tu identidad y prevenir que los atacantes utilicen tu información personal para cometer fraude o robo de identidad.
- Seguridad de los datos: Las contraseñas seguras ayudan a proteger tus datos personales y financieros de accesos no autorizados.

Características de las contraseñas seguras

- Longitud: Las contraseñas seguras deben tener una longitud mínima de 12 caracteres.
- Complejidad: Las contraseñas seguras deben incluir una combinación de letras mayúsculas y minúsculas, números y caracteres especiales.
- Unicidad: Las contraseñas seguras deben ser únicas y no repetirse en diferentes cuentas.
- No deben ser obvias: Las contraseñas seguras no deben ser obvias ni fáciles de adivinar, como fechas de nacimiento o nombres de familiares.

Mejores prácticas para el uso de contraseñas seguras

- Utilizar un administrador de contraseñas: Utilizar un administrador de contraseñas para generar y almacenar contraseñas seguras.
- Cambiar contraseñas regularmente: Cambiar contraseñas regularmente, especialmente para cuentas sensibles.
- No compartir contraseñas: No compartir contraseñas con nadie, ni siquiera con amigos o familiares.

- Utilizar autenticación multifactor: Utilizar autenticación multifactor para agregar una capa adicional de seguridad a tus cuentas.

1.1. Actividad:

Discusión: Preguntarles a los participantes si alguna vez han tenido una cuenta comprometida debido a una contraseña débil y qué aprendieron de esa experiencia.

2. Creación de Contraseñas Seguras

2.1. Explicación:

Ejemplo práctico de creación de una contraseña segura:

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.

2.2. Actividad Práctica

Link: https://www.joydeepdeb.com/tools/find-replace.html

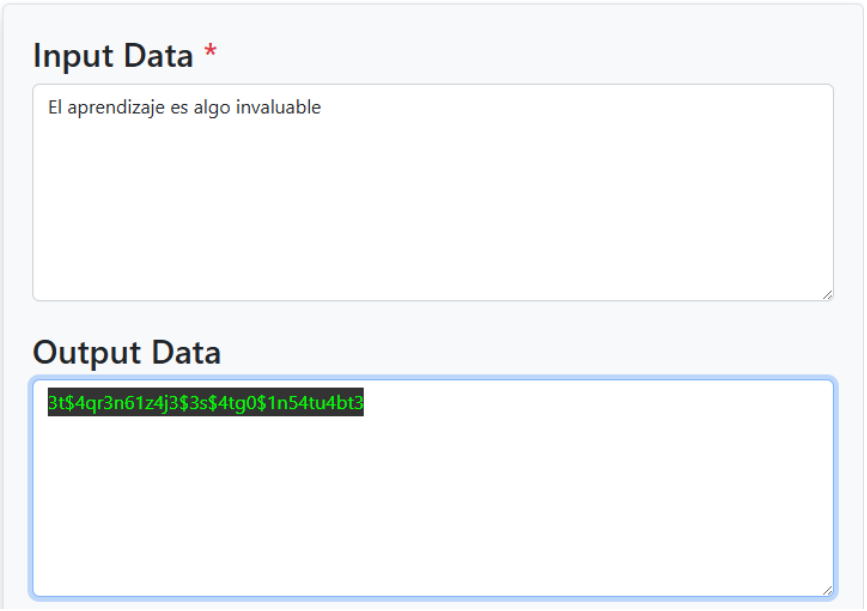
Paso 1: Piensa en una frase u oración significativa para ti.

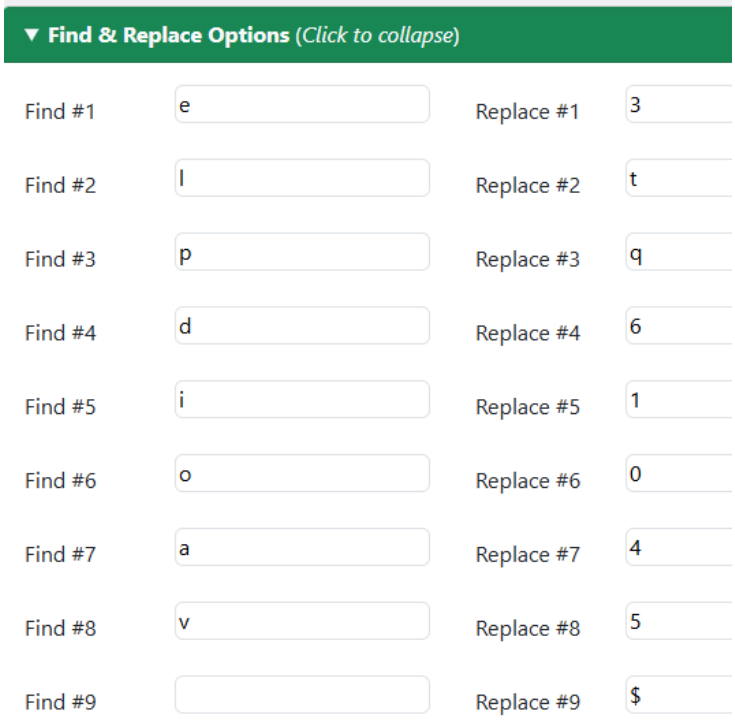
• Ejemplo personal: " **El aprendizaje es algo invaluable**"

Paso 2: Aplica sustituciones y variaciones:

• Reemplazos:

3t$4qr3n61z4j3$3s$4tg0$1n54tu4bt3





Paso 3: Verifica la seguridad de la contraseña:

• Comprueba que tenga una longitud adecuada y diversidad de caracteres.

Paso 4: Comparte métodos (opcional): Este método utiliza la sustitución, lo cual la hace bastante segura.

• Discute con compañeros sobre técnicas utilizadas sin revelar la contraseña.

3. INTRODUCCIÓN A LOS GESTORES DE CONTRASEÑAS.

3.1. Explicación

¿Qué es un gestor de contraseñas?

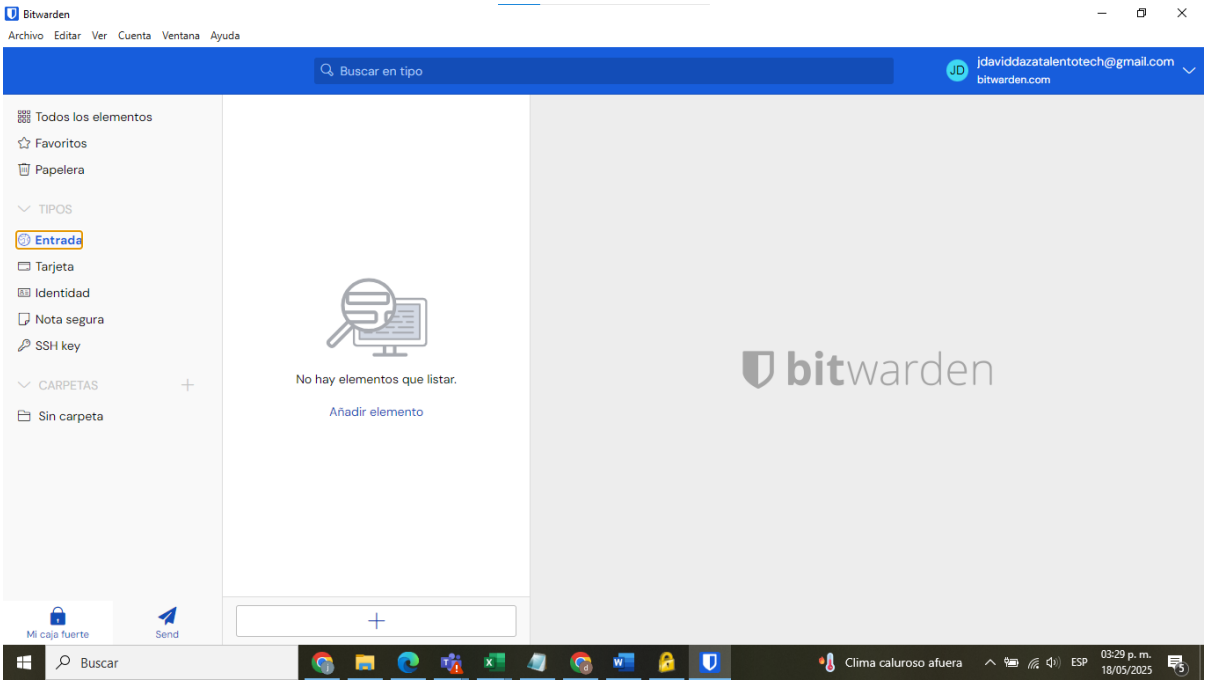
- Definición: Aplicación que almacena y gestiona tus contraseñas de forma segura y encriptada. Algunos gestores como Bitwarden encriptan las contraseñas, lo que las protege contra el acceso no autorizado.
- Funcionalidad: Genera contraseñas fuertes y autocompleta credenciales en sitios web.
- Ventajas:
    - 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.

Importancia de la contraseña maestra:

- Clave principal: Es la única contraseña que debes recordar.
- Seguridad crítica: Debe ser extremadamente fuerte y única
- Consejos: Utiliza una frase de paso larga y aplica las técnicas de creación de contraseñas seguras.

Ejemplo de contraseña maestra:

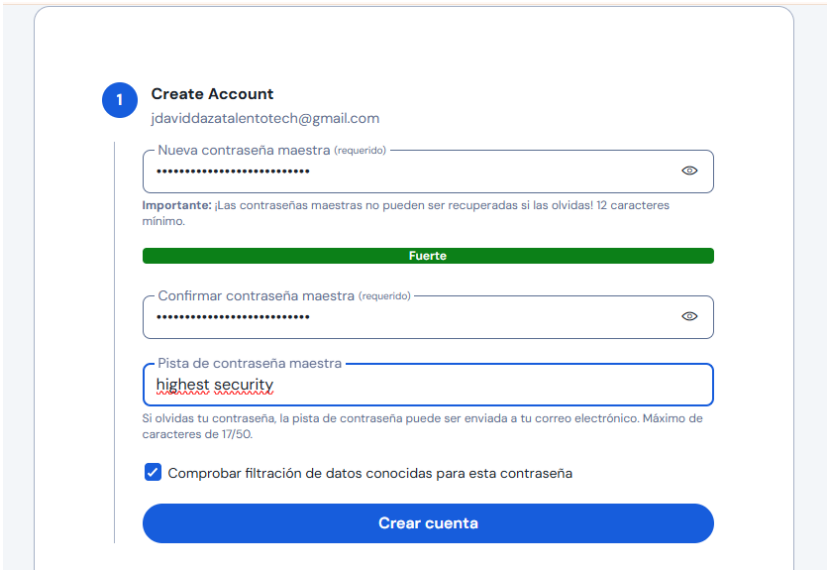
- Frase: " Seguridad al más alto nivel".
- Transformación: " S3gur1d4d$4l$m4s$4lt0$n1v3l "



3.2. Actividad

Demostración en vivo:

- Instalación de Bitwarden: Accede a Bitwarden y descarga la aplicación para tu sistema operativo o la extensión del navegador.
- Creación de cuenta: Regístrate con tu correo electrónico y establece una contraseña maestra segura.
- Exploración de funciones: Recorre la interfaz para familiarizarte con la creación de entradas, carpetas y opciones de seguridad.



4. Uso Práctico de un Gestor de Contraseñas (15 minutos)

4.1. Actividad Práctica

Paso 1: Instala y configura el gestor de contraseñas.

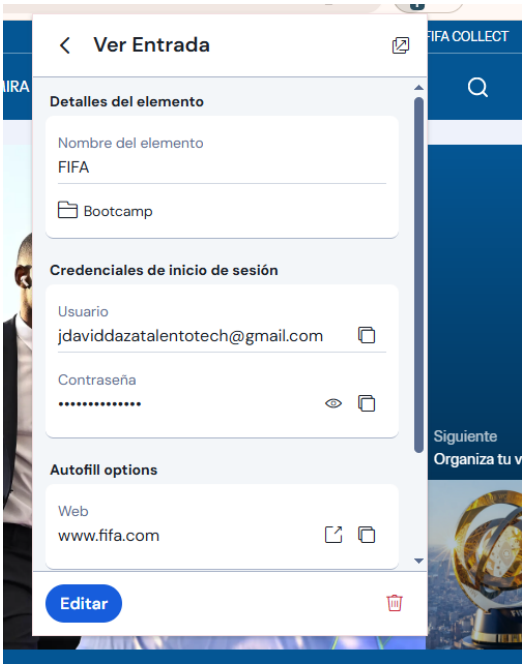
- Si aún no lo has hecho, completa la instalación y creación de tu cuenta.

Paso 2: Configura la autenticación de dos factores (2FA):

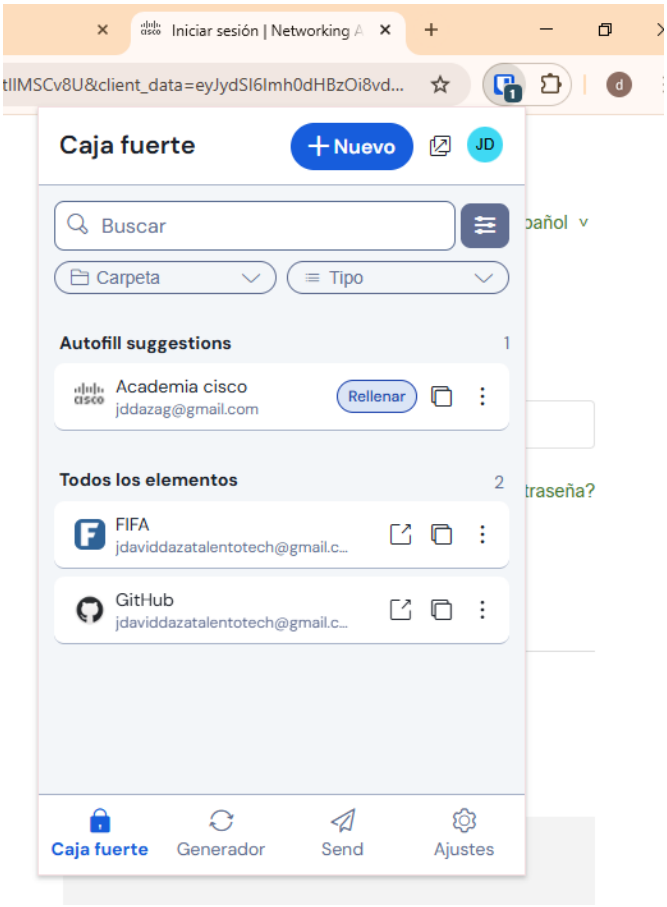
- Opcional pero recomendado: Añade una capa extra de seguridad utilizando una aplicación autenticadora.

Paso 3: Genera y guarda una nueva contraseña:

- Ejemplo: Sitio web: Tu cuenta de redes sociales, por ejemplo, Facebook.
- Procedimiento:
    - Abre Bitwarden y selecciona "Agregar elemento".
    - Completa los campos:
        - Nombre: "Facebook Personal".
        - Nombre de usuario: Tu correo electrónico o nombre de usuario.
        - Contraseña: Utiliza el generador de contraseñas: Establece longitud (ej. 16 caracteres). Incluye mayúsculas, minúsculas, números y símbolos.
    - Guarda el elemento.



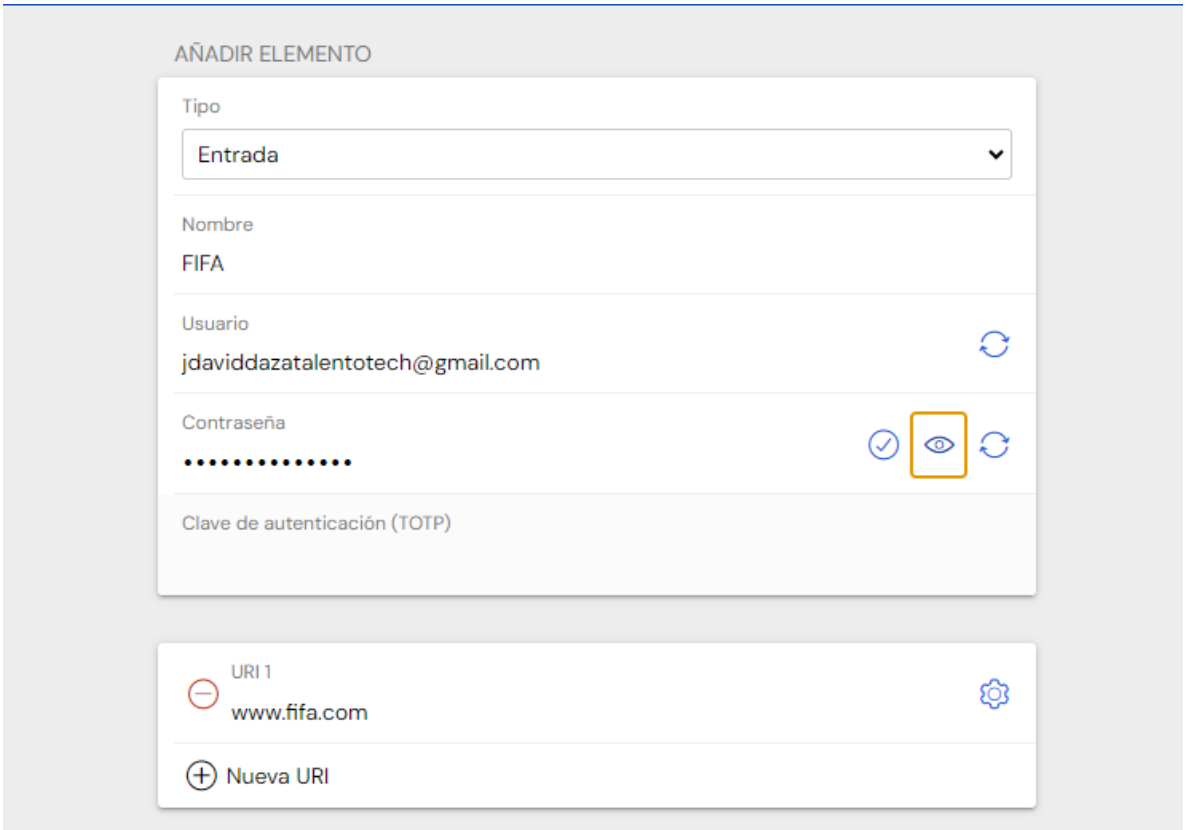
Paso 4: Prueba la función de autocompletar:



- En el navegador:
  - Visita Facebook e intenta iniciar sesión.
  - Cuando se te pida, permite que Bitwarden autocomplete tus credenciales.

Paso 5: Replicar el proceso para otras cuentas:

- Repite los pasos anteriores para otras cuentas importantes como correo electrónico, banca en línea, etc.



5. Conclusión y Mejores Prácticas (10 minutos)

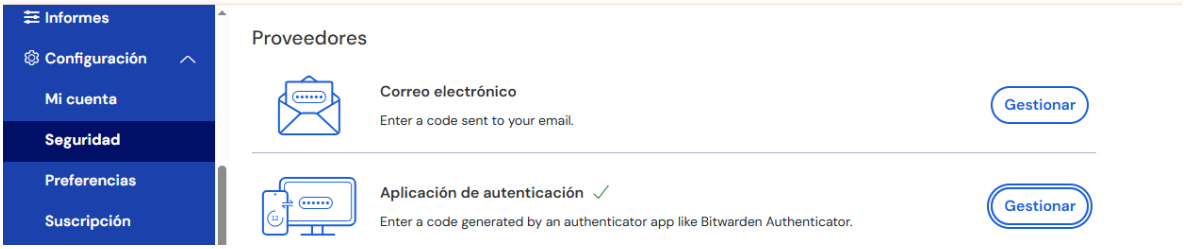
5.1. Repaso de los Puntos Clave

• Crear contraseñas fuertes y únicas para cada cuenta es esencial para la seguridad en línea.

• Los gestores de contraseñas simplifican este proceso al almacenar y generar contraseñas seguras.

• La contraseña maestra es crítica; debe ser fuerte y protegida.

• Autenticación de dos factores (2FA): Añade seguridad adicional a tus cuentas.



Para activar 2FA para bitwarden descargue el Bitwarden Authenticator, luego lei el código QR en la plataforma web de Bitwarden.

Recomiendo mucho utilizar la ayuda de Bitwarden, hay bastante información pertinente https://bitwarden.com/help/

5.2. Actividad Final

Reflexión:

• Compromiso personal: Piensa en una práctica de seguridad que implementarás.

o Ejemplo: "Actualizaré todas mis contraseñas antiguas y las gestionaré con Bitwarden".

Lista de Verificación:

1. Crear una frase memorable y segura.

2. Transformarla en una contraseña compleja.

3. Instalar un gestor de contraseñas confiable.

4. Configurar una contraseña maestra fuerte y habilitar 2FA.

5. Generar contraseñas únicas para todas tus cuentas importantes.

6. Utilizar la función de autocompletar para mayor seguridad y comodidad.

7. Mantener tus contraseñas y gestor actualizados.

8. No compartir tu contraseña maestra ni escribirla en lugares inseguros.

6. Subida del documento PDF a GitHub:

Paso 1: Preparar el documento:

- Crea un documento en Word o similar con todas las actividades realizadas. Incluye:
    - Explicaciones de los pasos que realizaste.
    - Capturas de pantalla (sin revelar informa

Paso 2: Convertir a PDF:

- Guarda el documento en formato PDF para asegurar la compatibilidad.

Paso 3: Subir a GitHub:

- Crear un repositorio: o Accede a tu cuenta de GitHub.

- Haz clic en "New repository".
- Asigna un nombre relevante, por ejemplo, "Laboratorio-Contraseñas-Seguras".
- Agrega una descripción si lo deseas.
- Decide si el repositorio será público o privado.
- Subir el archivo: o En el repositorio, haz clic en "Add file" y luego en "Upload files".
- Arrastra y suelta el archivo PDF o selecciónalo desde tu computadora.
- Añade un mensaje de confirmación (commit) describiendo el archivo.
- Haz clic en "Commit changes" para subir el documento.

Paso 4: Verificación:

- Asegúrate de que el archivo se ha subido correctamente y es accesible.
- Si es un repositorio público, puedes compartir el enlace con quien corresponda.