**DESARROLLO DEL LABORATORIO NRO 1. BOOTCAMP DE CIBERSEGURIDAD**

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

1. Introducción a la Importancia de las Contraseñas Seguras

* Protección de datos personales: Las contraseñas seguras son esenciales para proteger tus cuentas y datos contra accesos no autorizados.
* Prevención del robo de identidad: Si un atacante accede a tus cuentas, puede suplantarte, hacer compras, enviar correos maliciosos o cometer delitos en tu nombre.
* Prevención de ataques: Contraseñas débiles facilitan ataques como fuerza bruta, phishing o ingeniería social.
* Confidencialidad y privacidad: Mantienen tus comunicaciones y transacciones seguras.
* Cumplimiento normativo y legal: En organizaciones, el uso de contraseñas seguras es parte de políticas de seguridad exigidas por normas como ISO 27001, NIST o la Ley de Protección de Datos Personales.
* Evita el acceso lateral: Si usas la misma contraseña en varios servicios y uno de ellos se ve comprometido, un atacante puede usarla para acceder a otras cuentas (efecto dominó).
  1. Riesgos de contraseñas débiles:
* Robo de identidad: Los atacantes pueden hacerse pasar por ti.
* Pérdida financiera: Acceso no autorizado a cuentas bancarias.
* Compromiso de información sensible: Acceso a correos electrónicos, documentos y datos personales.
  1. Características de una contraseña segura:
* Longitud adecuada: Al menos 12 caracteres; más larga es mejor.
* Combinación de caracteres: Uso de mayúsculas, minúsculas, números y símbolos.
* No usar palabras del diccionario ni patrones comunes: Evita cosas como password, admin123, qwerty, abcd1234.
* No incluir información personal: Nada de nombres, fechas de nacimiento, cédula, placa del carro, nombre del perro, etc.
* Única para cada cuenta o servicio: no reutilices la misma contraseña en varios sitios.
* Fácil de recordar pero difícil de adivinar
* Puedes usar una frase secreta con algunas sustituciones: Ejemplo: MisPerros4Son@Unicos!
* Evita patrones del teclado: Ejemplos débiles: asdfgh, zxcvbn, 1234567890.

Buenas prácticas adicionales:

* Usa un gestor de contraseñas como Bitwarden, 1Password o KeePass para crear y almacenar contraseñas complejas sin tener que memorizarlas todas.
* Activa la autenticación multifactor (MFA) donde sea posible, especialmente en cuentas críticas (correo, bancos, nube).
* Cambia las contraseñas predeterminadas de dispositivos y servicios tan pronto como los configures.
* No compartas tus contraseñas, y si lo haces, usa medios seguros y cámbiala luego.
  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.

1. Creación de Contraseñas Seguras
   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.

* 1. **Actividad Práctica**

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

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

• Ejemplo personal: "Mi comida favorita es la pizza de pepperoni".

Paso 2: Aplica sustituciones y variaciones:

• Reemplazos:

o "M1C0m1d@F@v0r1t@3$L@P1zz@D3P3pp3r0n1!"

Paso 3: Verifica la seguridad de la contraseña:

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

Paso 4: Comparte métodos (opcional):

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

1. **INTRODUCCIÓN A LOS GESTORES DE CONTRASEÑAS.**
   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:

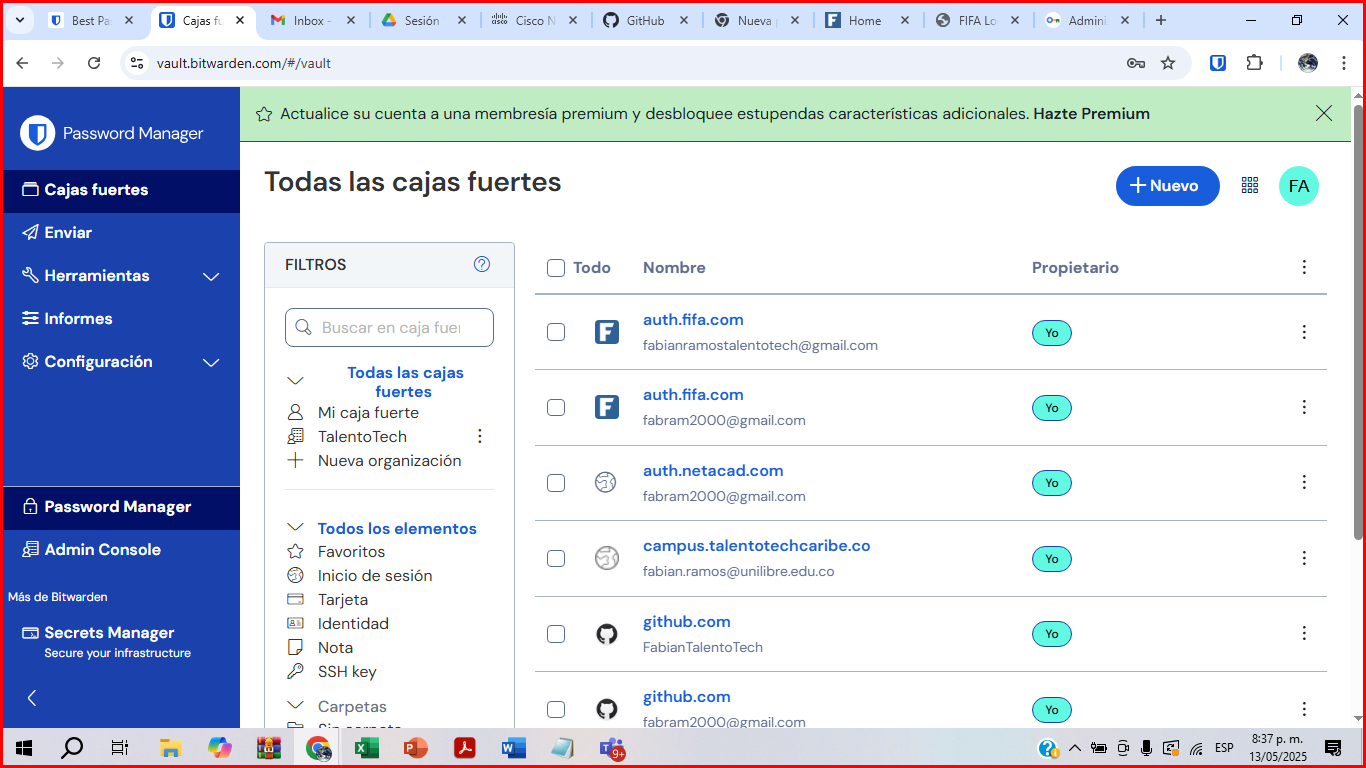
* Clave principal: Es la única contraseña que debes recordar.
* Seguridad crítica: Debe ser extremadamente fuerte y única
* Consejos: Utiliza una frase de paso larga y aplica las técnicas de creación de contraseñas seguras.

Ejemplo de contraseña maestra:

* Frase: "La seguridad es mi prioridad número uno".
* Transformación: "L@$3gur1d@d3$M1Pr10r1d@d#1"
  1. 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.



1. Uso Práctico de un Gestor de Contraseñas (15 minutos)
   1. Actividad Práctica

Paso 1: Instala y configura el gestor de contraseñas.

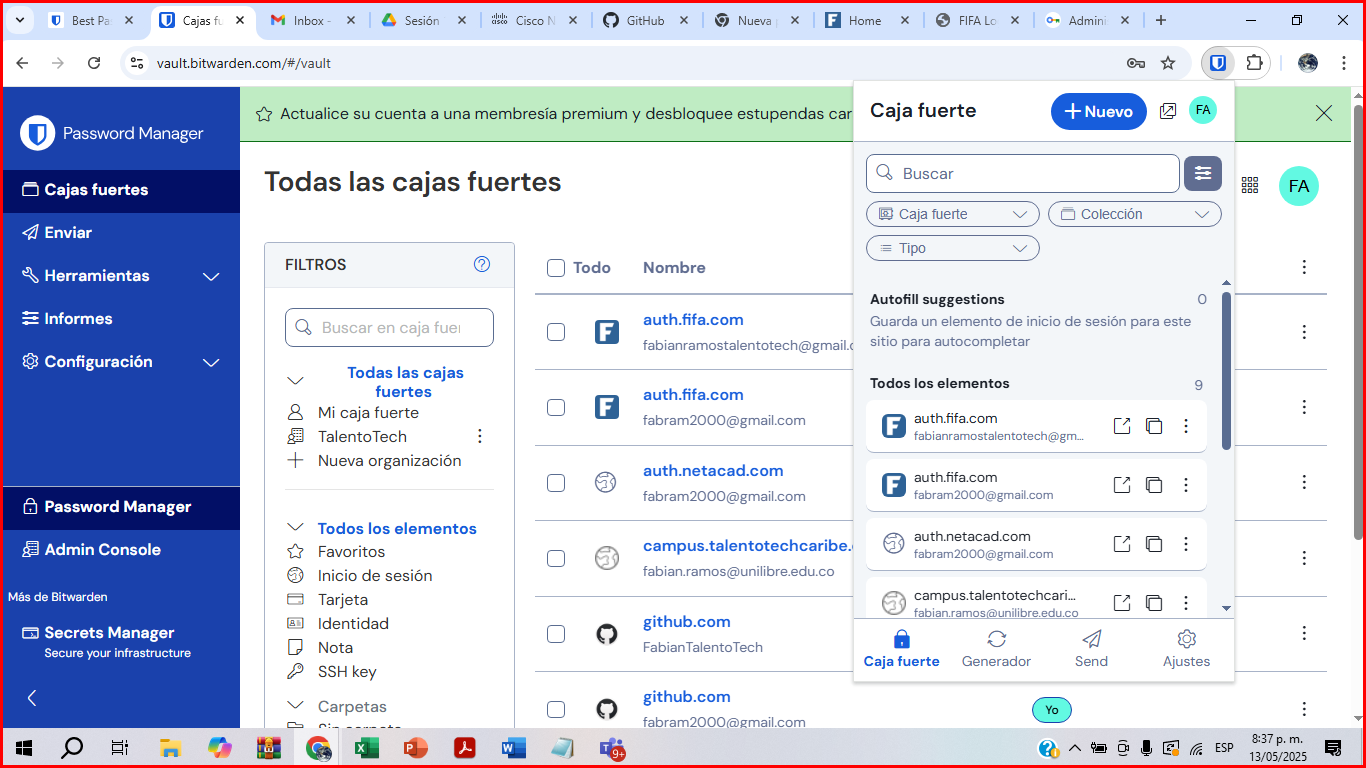
* Si aún no lo has hecho, completa la instalación y creación de tu cuenta.

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.

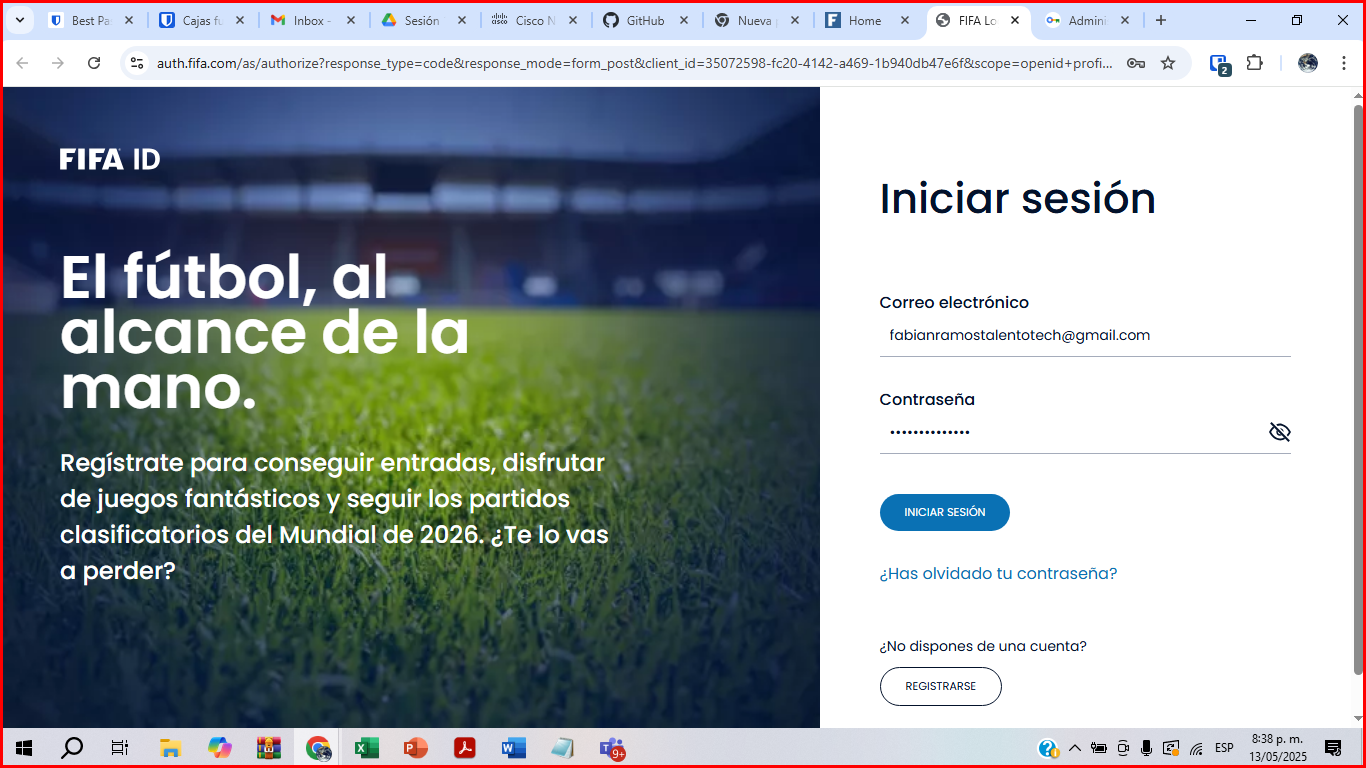


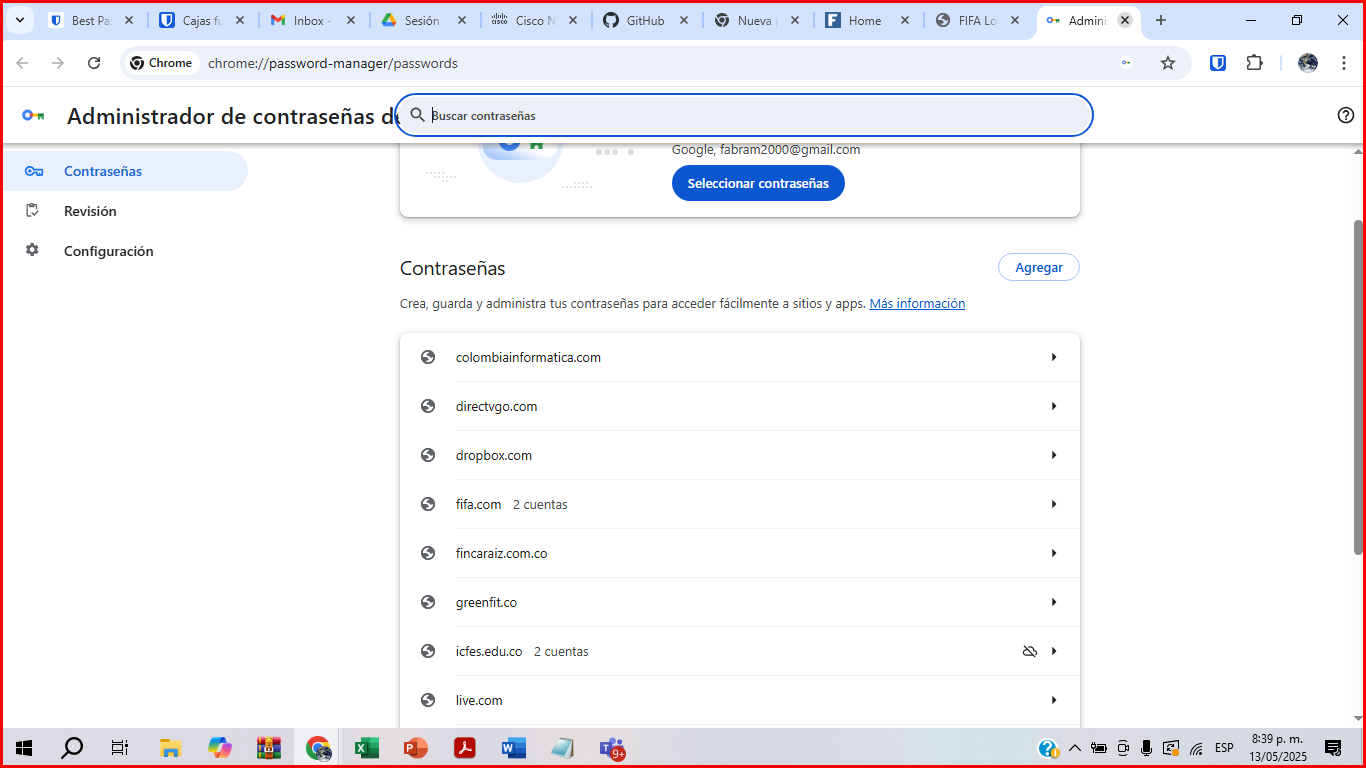
Paso 4: Prueba la función de autocompletar:

* 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.





1. Conclusión y Mejores Prácticas (10 minutos)
   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.

* 1. 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.

1. 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.