

Laboratorio 1

Paso 1: Introducción la Importancia de las Contraseñas Seguras (10 minutos)

Importancia de las contraseñas seguras:

Discusión:

De lo discutidos por mis compañeros, hubo una experiencia que fue relevante para mi criterio personal, en varias organizaciones cuando eres vinculado te dan una contraseña genérica compuesta por partes de tu información y uno que otro numero de tu documento de identidad, esta persona no realizo el cambio de contraseña, por esto al haber un ataque de phishing, el atacante pudo identificar el patrón de generación de contraseñas. Afortunadamente el equipo de TI pudo solucionar esta amenaza, a raíz de ello se estableció una política de cambio obligatorio de contraseñas más seguras.

Paso 2: Creación de Contraseñas Seguras (15 minutos)

Actividad práctica

- Primer paso: “Me gusta la música en inglés”
- Segundo paso: M3gU5t4L@Mu61Ç4!3n;NG|35.
- Tercer Paso: Se realizan reemplazos de las vocales por símbolos como @, !, ¡, | y además se incorporan caracteres como Ç, también se alternan entre mayúsculas y minúsculas para romper patrones. Dentro de las ventajas de esta técnica es que al usar de base una frase memorable, es mas sencilla de recordar para la persona que la creó, sin embargo al atacante desconocer la frase se le hará más difícil.

Paso 3: Introducción a los Gestores de Contraseñas (10 minutos)

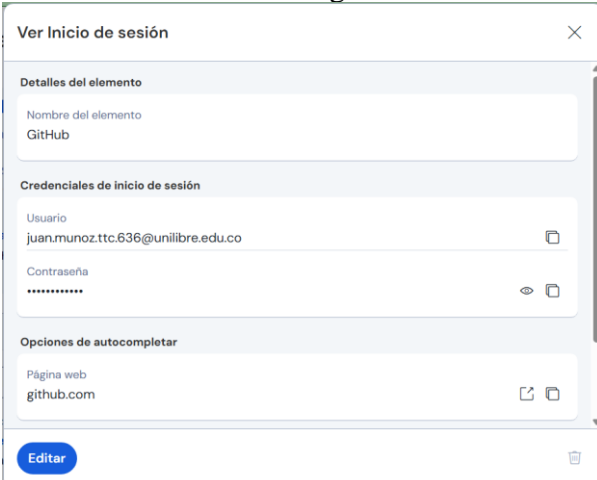
Actividad

- Para instalar Bitwarden simplemente debemos escribir nuestro correo para que nos envíen un email para terminar de configurar la cuenta, establecer una contraseña maestra, verificación de la misma y una pista para ayudar a recordarla.
- Una contraseña maestra fuerte es de suma importancia ya que esta será la llave para acceder al cumulo de contraseñas, y datos de alta confidencialidad, por lo que sí es débil, el atacante tendrá a su disposición todas nuestras credenciales.

Paso 4: Uso práctico de un Gestor de Contraseñas (15 minutos)

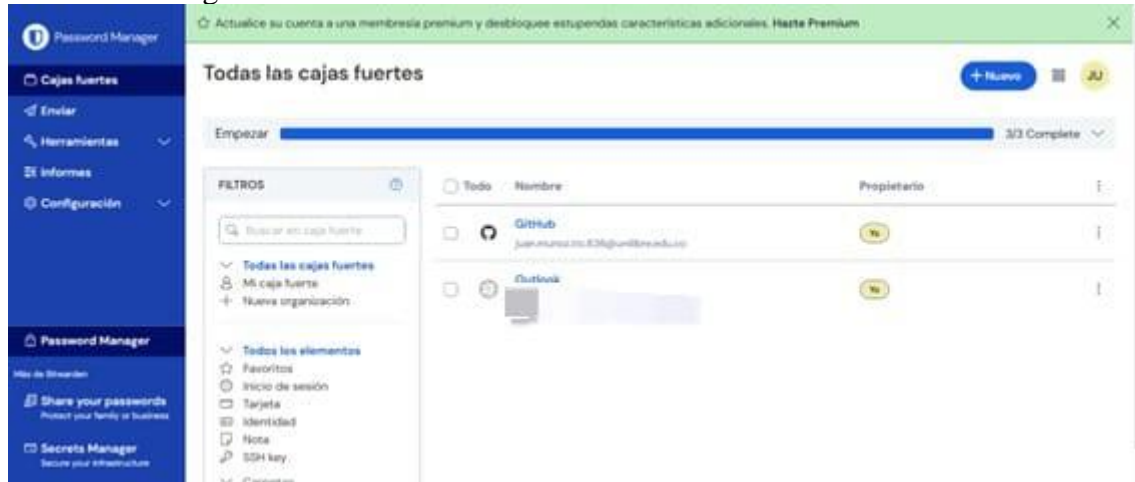
Actividad practica

Añadir una contraseña al gestor de contraseñas



The screenshot shows a mobile application interface for a password manager. At the top, there's a title bar that says "Ver Inicio de sesión" with a close button (X). Below this, the interface is divided into sections: "Detalles del elemento" (Details of the item) showing "Nombre del elemento" (Item name) as "GitHub"; "Credenciales de inicio de sesión" (Login credentials) showing "Usuario" (Username) as "juan.munoz.ttc.636@unilibre.edu.co" and "Contraseña" (Password) as a masked string "*****"; and "Opciones de autocompletar" (Autocomplete options) showing "Página web" (Website) as "github.com". At the bottom left, there is a blue button labeled "Editar" (Edit), and at the bottom right, there is a trash icon.

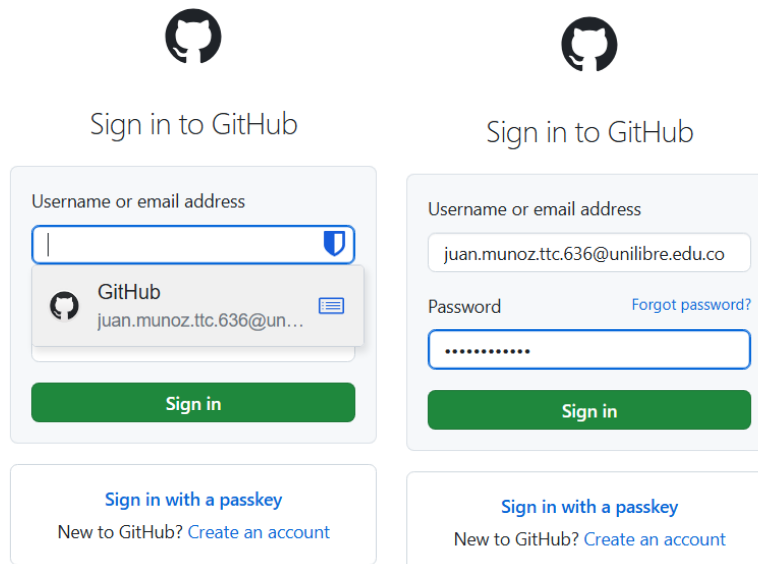
Dashboard del gestor de contraseñas



Sitio web: <https://login.microsoftonline.com>

Contraseña generada por el gestor: A2^IGJ5y6qci1G

Ejemplo de función autocompletar



Paso 5: Conclusión y Mejores Prácticas (10 minutos)

Actividad Final

Como consejo al finalizar el taller podemos decir que debemos ser cautelosos con respecto al nivel de complejidad de las contraseñas para sitios críticos o que sea de un uso muy personal o confidencial, debemos apoyarnos ya sea en un gestor y generador de contraseñas o creando nosotros mismos contraseñas seguras mediante de la combinación de letras mayúsculas y minúsculas con números y caracteres especiales.

Lista de verificación

- ✓ Crear una frase segura
- ✓ Transformar la frase combinando mayúsculas, minúsculas, números, símbolos
- ✓ Instalar un gestor de contraseñas seguro
- ✓ Establecer una contraseña maestra fuerte y segura para nuestro gestor
- ✓ Crear y guardar contraseñas únicas para cuentas de alta importancia en el gestor
- ✓ Hacer uso de la función autocompletar del gestor para hacer inicios de sesión de manera segura

- ✓ No utilizar la misma contraseña para todos los sitios
- ✓ Actualizar regularmente las contraseñas de sitios críticos como bancos o correos