Actividad 04. Uso de contraseñas

1. Con toda esta información y la que obtengas por tu cuenta, elabora una política de generación de contraseñas segura
2. Utiliza y muestra un gestor de contraseñas

1. Con toda esta información y la que obtengas por tu cuenta, elabora una política de generación de contraseñas segura

La ***política de generación de contraseñas seguras*** tiene como **objetivo** establecer las pautas claras para la creación y gestión de contraseñas seguras, con el fin de minimizar el riesgo de acceso no autorizado a tus cuentas y proteger la información personal.

Los **Requisitos** que hay que tener para tener contraseñas seguras son:

- ***Longitud***: Mínimo 12 caracteres, aunque lo ideal son 15 o más caracteres. Cuanto más larga sea la contraseña, más segura y más difícil será de descifrar.
- ***Complejidad***: Combinar letras mayúsculas y minúsculas, números y caracteres especiales.
- ***Unicidad***: Cada cuenta debe tener una contraseña única. No hay que reutilizar las contraseñas en diferentes sitios web y/o móvil.
- ***Información Personal***: No utilizar la información personal para las contraseñas (nombres, fechas de nacimiento, dirección, etc.).
- ***Caducidad***: Cambiar las contraseñas regularmente (cada 3-6 meses).

Gestores de Contraseñas: Utilizar un gestor de contraseñas confiable para almacenar las contraseñas de forma segura y generar contraseñas fuertes automáticamente.

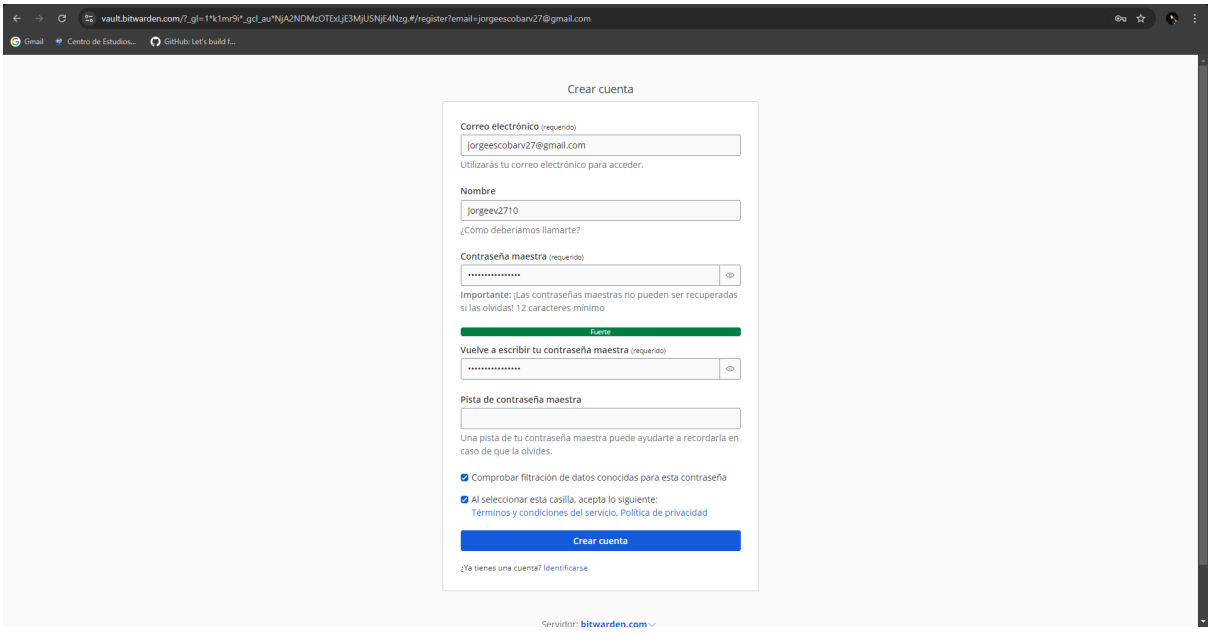
Autenticación en Dos Factores: Activar la autenticación de dos factores siempre que esté disponible. Esto añade una capa adicional de seguridad a tus cuentas.
Sensibilización: Mantenerse informado sobre las últimas amenazas a la seguridad y las mejores prácticas para proteger las contraseñas.

Es importante seguir la política de generación de contraseñas porque:

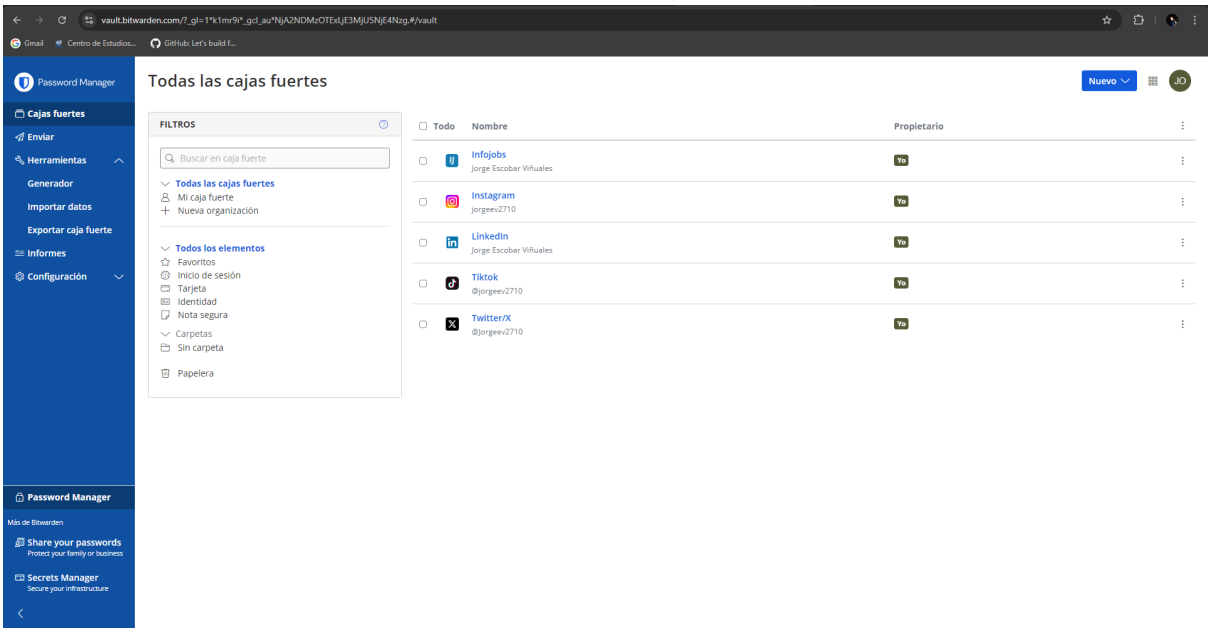
1. ***PROTECCIÓN DE DATOS***: Al utilizar contraseñas seguras, protegemos la información personal y financiera ante posibles robos o fraudes.
2. ***PREVENCIÓN A ATAQUES CIBERNÉTICOS***: Las contraseñas débiles son una puerta de entrada para los hackers. Al seguir esta política, se reduce significativamente el riesgo de sufrir un ataque cibernético.
3. ***CUMPLIMIENTO NORMATIVO***: Muchas empresas y organizaciones tienen requisitos de seguridad que incluyen políticas de contraseñas sólidas.

2. *Utiliza y muestra un gestor de contraseñas*

Me he creado una cuenta en Bitwarden para tener mis contraseñas seguras:



Una vez creado, pongo mis cuentas para tener las contraseñas seguras:



Y muestro una de las aplicaciones con la contraseña, en este caso, Instagram: