Uso Seguro
De Contraseñas

Cómo proteger tu información en el día a día

La mayoría de nuestras actividades dependen de contraseñas

- Dinero
- Datos
- Identidad ¿a que se refiere?

DATO IMPORTANTE
Te suena 123456?...

1 seg

Errores Comunes

❌ Usar claves cortas o simples (“1234”, “admin”).

❌ Reutilizar la misma clave en varios sitios.

❌ Guardarlas en papel, notas o post-it.

❌ Compartirlas con terceros.

Riesgo Real

Cómo Crear una Contraseña Segura

Ejemplo:
Si tu correo y tu banco tienen la misma contraseña, y se filtra la del correo → el atacante también accede al banco.

- Mínimo 12 caracteres.
- Mezcla de mayúsculas, minúsculas, números y símbolos.
- Evita nombres, fechas o datos personales.
- Usa frases fáciles de recordar

Gestión de contraseñas

1. Ejemplo

- En vez de Juan1990, usar: C@fe!En_LaTarde2024.
- Difícil de adivinar, pero fácil de recordar.

2. No memorizar todas ¿Como?

- ej: Bitwarden, 1Password, LastPass, KeePass

3. Autenticación de dos factores

- El 2FA es como tener una segunda cerradura

Señales de alerta

1. Recibes correos

- Correo con solicitud de cambio de contraseña

2. Actividad sospechosa

- Modificaciones en tus archivos que desconoces

3. Mensajes de inicio de sesión

- Mensaje a tu celular de inicio de sesión en dispositivos desconocidos

4. Qué hacer?

- Primera Medida.

Qué tan seguro es Bitwarden?

1. Cifrado de extremo a extremo (E2EE):

- Todas tus contraseñas se cifran en tu dispositivo antes de enviarse a los servidores de Bitwarden.
- Bitwarden solo almacena datos cifrados, no tiene la clave maestra para descifrarlos.
- Eso significa que aunque alguien hackeara los servidores, lo que vería sería un montón de datos ilegibles.

2. Código abierto:

- Bitwarden es open source, lo que permite a expertos en seguridad auditar el código y confirmar que no hay “puertas traseras”.

3. Clave maestra bajo tu control:

- El único punto débil es tu contraseña maestra (Master Password).
- Si usas una clave débil, todo tu “baúl de contraseñas” queda en riesgo.
- La fortaleza de Bitwarden depende directamente de qué tan fuerte sea tu contraseña maestra y si activas el 2FA.

4. Auditorías externas:

- Bitwarden ha sido auditado por empresas de ciberseguridad independientes y cumple normas de seguridad internacionales (como SOC 2).

Recordemos

Resumen

❌ Contraseñas fuertes y únicas.

❌ Gestores de contraseñas para organizar.

❌ Activar siempre el 2FA.

El Cepillo de Dientes

“Las contraseñas son como el cepillo de dientes: no se comparten, se cambian regularmente y deben mantenerse limpias y fuertes.”

EnorChile