Módulo 2

Protege tus cuentas

Objetivo del módulo

Aprender a blindar nuestras cuentas online mediante **contraseñas seguras**, **gestores de contraseñas** y **verificación en dos pasos (2FA)**, para evitar accesos no autorizados.

Contraseñas seguras: la primera barrera

Las contraseñas son como las **llaves de tu casa digital**.
Si alguien las roba o adivina, podrá entrar en tu correo, redes sociales, banco, fotos, y más.

Errores comunes:

- Usar contraseñas cortas como `123456`, `qwerty` o `contraseña`.
- Repetir la misma clave en todas las cuentas.
- Usar datos personales fáciles de adivinar: fecha de nacimiento, nombre de tu mascota, etc.

Cómo crear una contraseña fuerte:

- Mínimo **12 caracteres**.
- Mezclar mayúsculas, minúsculas, números y símbolos.
- No debe estar en un diccionario ni ser una palabra común.

Ejemplo inseguro: `maria1990`
Ejemplo seguro: `M4riA!Azul#2025`

Consejo práctico:
Usa una **frase fácil de recordar** y agrega símbolos.
Ejemplo: `"Me gustan los gatos en 2025"` → `MeGust4n!LosGat0s2025`

Gestores de contraseñas: tus “cajas fuertes”

Recordar decenas de contraseñas seguras es imposible. Para eso existen los **gestores de contraseñas**: aplicaciones que guardan todas tus claves cifradas.

Ventajas:

- Solo necesitas recordar una **contraseña maestra**.
- Generan claves largas y seguras automáticamente.
- Se sincronizan entre tus dispositivos.

Ejemplos recomendados:

- **Bitwarden** (gratuito y de código abierto).
- **KeePass** (gratuito, versión local).
- **1Password** o **LastPass** (opciones de pago, fáciles de usar).

Consejo práctico: instala Bitwarden en tu móvil y navegador. Guarda ahí todas tus contraseñas.

Verificación en dos pasos (2FA): doble candado

La **verificación en dos pasos** añade un nivel extra de seguridad. Incluso si un hacker obtiene tu contraseña, necesitará un **código adicional** para entrar.

Formas de 2FA:

1. **SMS**: recibes un código en tu móvil.
2. **App de autenticación** (más segura): Google Authenticator, Authy, Microsoft Authenticator.
3. **Llaves físicas de seguridad** (YubiKey, Titan Key).

Cómo activarla en tus cuentas principales:

En Gmail:

1. Ve a tu cuenta de Google → Seguridad.
2. Activa “Verificación en dos pasos”.
3. Elige SMS o aplicación.

En WhatsApp:

1. Ajustes → Cuenta → Verificación en dos pasos.
2. Activa un PIN de 6 dígitos.

Caso real

Ana usaba la misma contraseña en Facebook y en su correo. Esa clave se filtró en una página web hackeada. Un ciberdelincuente probó la misma contraseña en su Facebook... y entró.
Si Ana hubiera usado un **gestor de contraseñas** y activado el **2FA**, habría evitado el robo.

Resumen del módulo

- Usa contraseñas largas y únicas para cada cuenta.
- Apóyate en gestores de contraseñas para no olvidarlas.
- Activa siempre la verificación en dos pasos en tus cuentas más importantes.