AUTENTICACIÓN DE DOS PASOS

Autenticación de dos factores es conocida por varios nombres, como 2FA, autenticación multifactorial, verificación de dos factores, MFA, y demás. Se suele definir como:

1) **Algo que conoces**
   Es el primer factor: tu usuario y tu contraseña

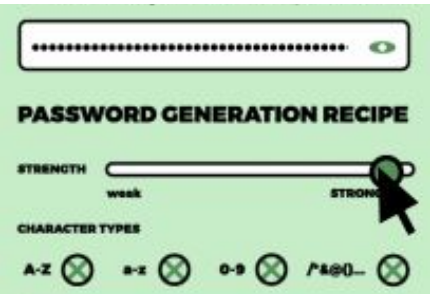
2) **Algo que tienes**
   Es el segundo factor: el dispositivo que llevas (celular, computadora, etc.)

Siga las pautas sugeridas para mejorar la seguridad de tus cuentas.

1 USAR CONTRASEÑAS FUERTES

CADA CONTRASEÑA PARA CADA CUENTA DEBE SER:

- Aleatoria
- Larga
- Unica



Consulta la guía del EFF sobre cómo generar contraseñas seguras:
https://ssd.eff.org/es/module/creando-contrase%C3%B1as-seguras

PERO ¿CÓMO PUEDO RECORDAR TODAS ESTAS CONTRASEÑAS ALEATORIAS, LARGAS Y ÚNICAS?

Dependiendo de tu estrategia, es posible que desees utilizar un gestor de contraseñas.

Mira el video del EFF sobre el uso de un gestor de contraseñas aquí:
https://ssd.eff.org/es/module/vision-animada-uso-de-gestores-de-contrasenas-para-estar-seguro-en-linea

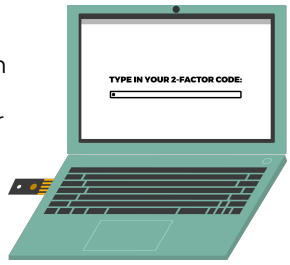
¿BUSCAS UN GESTOR DE CONTRASEÑAS?
Mira una de las opciones aquí:
https://ssd.eff.org/es/module/como-usar-keepassxc

2 ALGO QUE TIENES: ELIGE TU METODO

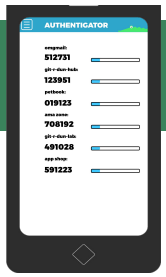
Hardware token ★

Conecta el token de hardware en el puerto USB y presiona el botón cuando el servicio de 2FA lo solicita.

Lo bueno: los códigos se almacenan en el token. Es la opción más recomendada para la seguridad de sus cuentas. Dado que no está almacenado en tu teléfono, queda protegido de los malware.
Lo malo: tienes que comprar uno de estos aparatos (Yubikey es una opción popular) y llevarlo contigo. Hacer un seguimiento del token puede resultar complicado. Si lo pierdes, se te bloqueará el acceso a tus cuentas (a menos que hayas escrito códigos de respaldo).

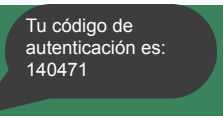


Aplicación de Autenticación



Escriba el código de seis dígitos cuando el servicio de 2fa lo solicite. Para las aplicaciones de autenticación basadas en el tiempo (TOTP), debe escribir el código antes de que se actualice.

Lo bueno: los códigos se almacenan en tu celular o tablet. No son visibles para ningún proveedor de servicios. La información de la aplicación está protegida por cifrado.
Lo malo: si tu celular tiene malware, un atacante puede leer los códigos. Si pierdes tu teléfono, no podrá acceder a tus cuentas (a menos que hayas anotado los códigos de seguridad).



2FA por SMS

Ciertos servicios te envían un mensaje de texto de seis dígitos al celular. Escriba este código cuando para iniciar sesión. Algunos servicios solo ofrecen esta forma de 2FA.

Lo bueno: es conveniente. si cambias de dispositivo ni de números de celular, obtendrá tus códigos.
Lo malo: los SMS no son seguros. Si vas a otro país y no tiene servicio, no recibirá el código. Si cambias de número de celular, no tendrás tus códigos. Si tu teléfono tiene malware, un atacante puede leer los códigos.