

Protección de cuentas y contraseñas

GUÍA INTRODUCTORIA · MATERIAL EDUCATIVO



Protege tus cuentas con contraseñas únicas, un gestor de claves y autenticación multifactor.

Nivel: Principiante · Duración estimada del curso: 2-3 horas · Precio de catálogo: \$9 USD

Esta guía es una introducción escrita a los temas del catálogo. No equivale a un curso completo ni incluye videos. No otorga certificación oficial ni garantiza empleo.

Tus primeras herramientas

1. Creación de contraseñas seguras

Usa contraseñas largas y únicas para cada servicio. Un gestor puede generar claves aleatorias. Si necesitas recordarlas, una frase con varias palabras elegidas al azar puede ser útil. No uses nombres, fechas o patrones conocidos; no copies ejemplos publicados como contraseña real.

2. Uso de gestores de contraseñas

Un gestor de contraseñas almacena claves en una bóveda cifrada. Elige un proveedor confiable, protege su acceso con una contraseña maestra única y multifactor, y conserva de forma segura su mecanismo de recuperación. Nunca compartas la bóveda completa ni exportaciones sin cifrar.

3. Autenticación multifactor (MFA)

MFA añade un factor adicional a la contraseña. Prefiere claves de acceso (passkeys), llaves de seguridad o aplicaciones autenticadoras cuando estén disponibles. SMS suele ser mejor que no usar un segundo factor, aunque tiene limitaciones. Algunas formas de MFA también pueden ser víctimas de phishing.

De la teoría a tus hábitos

4. Protección del correo electrónico

El correo permite recuperar otras cuentas, por eso es prioritario. Revisa sesiones y dispositivos, reglas de reenvío y direcciones de recuperación. Si detectas una sesión desconocida, ciérrala, cambia la contraseña desde el sitio oficial y revisa servicios asociados.

5. Recuperación segura de cuentas

Guarda códigos de recuperación en un lugar seguro y separado del dispositivo. Mantén actualizados los datos de recuperación. Si pierdes acceso, usa únicamente la ayuda oficial del servicio; nunca pagues a perfiles que prometen recuperar cuentas ni entregues códigos a terceros.

Ejercicio seguro

Revisa tu correo principal: activa MFA, verifica las opciones de recuperación y guarda códigos de respaldo. No anotes contraseñas reales en esta guía. Comprueba que puedes entrar con el método configurado.

Antes de continuar

Realiza actividades únicamente en tus propias cuentas, equipos o entornos expresamente autorizados. No compartas contraseñas, códigos ni información privada. Los ajustes pueden variar según tu dispositivo o proveedor; consulta siempre su documentación oficial.