Contraseñas y accesos: la primera línea de defensa

El problema con "123456" o el nombre de tu negocio

Imagina que tienes una caja fuerte en tu oficina con toda la documentación de tus clientes, tus facturas y tus datos bancarios. Ahora imagina que la combinación de esa caja fuerte es "1234". Absurdo, ¿verdad? Pues eso es exactamente lo que ocurre cuando usas una contraseña débil.

Los ciberdelincuentes no se sientan delante de una pantalla a adivinar tu contraseña letra por letra. Utilizan programas automatizados que pueden probar **millones de combinaciones por segundo**. Estas herramientas empiezan siempre por las contraseñas más usadas del mundo, y año tras año, las estadísticas son demoledoras: "123456", "password", "qwerty" o el nombre de la empresa siguen siendo las más utilizadas — y, por tanto, las primeras que prueban.

Además, hay otro problema igual de grave: **reutilizar la misma contraseña en varios sitios**. Si usas la misma clave para tu correo, tu banco y tu perfil de una tienda online, y esa tienda sufre una brecha de seguridad, el atacante probará esa contraseña en el resto de tus servicios. Este ataque se llama *credential stuffing* y es mucho más común de lo que parece.

Cómo crear una contraseña segura

Una contraseña segura debe cumplir tres condiciones: ser **larga**, ser **única** para cada servicio, y ser **difícil de adivinar** (pero no necesariamente imposible de recordar).

El truco más sencillo es usar una **frase de contraseña**: en lugar de una palabra con símbolos raros, piensa en tres o cuatro palabras aleatorias encadenadas.

Por ejemplo: **caballo-bateria-grapa-21**

Esta contraseña es mucho más segura que **P@ssw0rd!** y además es más fácil de recordar. Tiene longitud, variedad y no aparece en ningún diccionario de ataques.

Algunas reglas básicas:

- **Mínimo 12 caracteres.** Cuanto más larga, mejor.
- **Nunca uses datos personales:** tu fecha de nacimiento, el nombre de tu empresa, tu ciudad o el nombre de tu perro son los primeros que alguien con malas intenciones probará.
- **Una contraseña diferente para cada servicio importante.** Sí, es un lío. Por eso existe la siguiente sección.

Gestores de contraseñas

Si tienes una contraseña diferente y segura para cada servicio, es humanamente imposible recordarlas todas. La solución no es apuntarlas en un papel ni en un documento de Word — la solución es usar un **gestor de contraseñas**.

Un gestor de contraseñas es una aplicación que guarda todas tus contraseñas en una especie de caja fuerte digital, cifrada y protegida. Tú solo necesitas recordar **una única contraseña maestra** para acceder a todas las demás.

El programa incluso puede generar contraseñas aleatorias y seguras para ti, y auto rellenarlas cuando entras a una web.

Opciones recomendadas (gratuitas o muy económicas):

Gestor	Precio	Plataformas	Ideal para
Bitwarden	Gratuito	Windows, Mac, móvil, navegador	La mejor opción gratuita
KeePass	Gratuito	Windows, portable	Si prefieres guardar todo en local
1Password	~3€/mes	Todas	Si quieres algo muy pulido y de pago
Gestor del navegador	Gratuito	Chrome, Firefox, Safari	Aceptable, pero menos seguro

⚠️ ***Nota sobre los gestores del navegador:*** *Chrome o Firefox pueden guardar contraseñas, y es mejor que nada, pero tienen limitaciones de seguridad. Si puedes, da el paso a un gestor dedicado como Bitwarden.*

¿Es seguro guardar todas las contraseñas en una sola aplicación?

Es una pregunta lógica. La respuesta es sí, siempre que elijas un gestor reconocido y uses una contraseña maestra robusta. El riesgo de usar contraseñas débiles o repetidas es mucho mayor que el de usar un gestor de contraseñas consolidado.

Autenticación en dos pasos (2FA)

Imagina que, aunque alguien consiga tu contraseña, necesite también tu teléfono físico para poder entrar. Eso es exactamente lo que hace la **autenticación en dos pasos**, también llamada 2FA (*Two-Factor Authentication*) o verificación en dos pasos.

El funcionamiento es simple: al iniciar sesión, además de tu contraseña, el sistema te pide un **segundo código** que llega a tu móvil o se genera en una aplicación. Sin ese código, la contraseña sola no sirve de nada.

Los tres tipos más comunes, de menor a mayor seguridad:

1. **SMS al móvil** — El código te llega por mensaje de texto. Es el método más básico y tiene vulnerabilidades conocidas, pero sigue siendo mucho mejor que no tener 2FA.
2. **App de autenticación** *(recomendado)* — Aplicaciones como **Google Authenticator**, **Authy** o **Microsoft Authenticator** generan códigos temporales en tu teléfono. Son más seguros que el SMS y funcionan incluso sin cobertura.
3. **Llave de seguridad física** — Un pequeño dispositivo USB que conectas al ordenador. El más seguro de todos, pero menos habitual en pequeñas empresas.

¿Dónde activar el 2FA cuanto antes?

Prioriza estos servicios por encima de todo:

- **Correo electrónico** (Gmail, Outlook) — Es la llave maestra: quien controla tu email puede resetear el acceso al resto de cuentas.

- **Banca online** — La mayoría de bancos ya lo tienen activado por ley, pero verifica que esté funcionando.
- **Almacenamiento en la nube** (Google Drive, Dropbox, OneDrive)
- **Redes sociales de empresa** (Instagram, Facebook, LinkedIn)
- **Plataformas de venta o gestión** (Amazon Seller, Shopify, tu software de facturación)

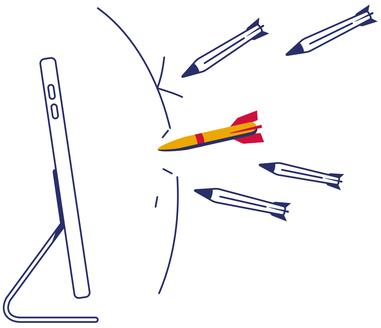
Activarlo suele ser tan sencillo como ir a *Configuración → Seguridad → Verificación en dos pasos* en cada servicio.

✅ Lista de comprobación — Contraseñas y accesos

- He revisado mis contraseñas más importantes: ninguna es obvia ni repetida
- He comprobado en haveibeenpwned.com si algún correo mío ha sido filtrado
- He instalado o tengo previsto instalar un gestor de contraseñas
- Tengo el 2FA activado en mi correo electrónico principal
- Tengo el 2FA activado en mi banca online
- Los accesos de empleados o colaboradores que ya no trabajan conmigo están revocados

CONTRASEÑAS Y ACCESOS

Tu primera línea de defensa



¿Tu contraseña es realmente segura?

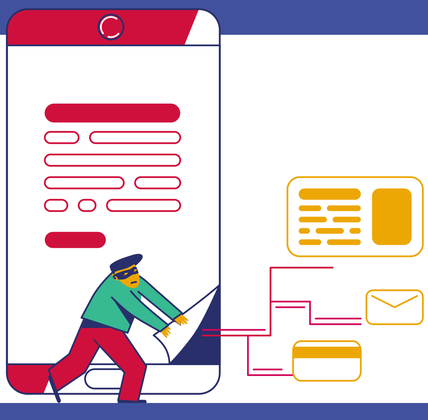
Una contraseña segura es la primera barrera frente a ciberataques.

Los ciberdelincuentes prueban millones de combinaciones por segundo, empezando por las claves más comunes. **Evita contraseñas débiles y nunca reutilices la misma en varios servicios.**

Cómo crear una contraseña segura

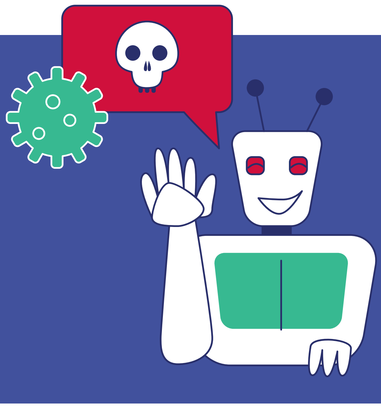
Una contraseña segura debe cumplir tres condiciones:

- **Mínimo 12 caracteres**: cuanto más larga sea mejor.
- **Nunca uses datos personales**: evita fechas de cumpleaños, tu ciudad, el nombre de tu perro, el nombre de tu empresa...
- **Una contraseña diferente para cada servicio importante.**



Gestores de contraseñas

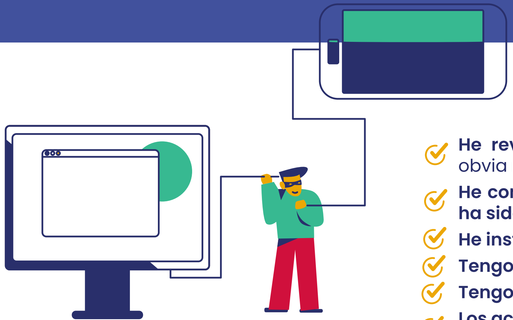
Un gestor de contraseñas **almacena tus claves de forma segura y cifrada**, para que solo tengas que recordar una contraseña maestra.
Además, **puede generar contraseñas seguras** y autorellenarlas al acceder a tus servicios.
Algunas opciones recomendadas son **Bitwarden**, **KeePass**, **1Password** o el **gestor de contraseñas de tu navegador.**



Autenticación en dos pasos

La autenticación en dos pasos (2FA) añade una **segunda barrera de seguridad:** además de tu contraseña, **necesitas un código o dispositivo adicional para acceder.**

Actívala especialmente en el correo electrónico, banca online, almacenamiento en la nube, redes sociales y plataformas de gestión de tu empresa.



Lista de comprobación

- **He revisado mis contraseñas más importantes**: ninguna es obvia ni repetida
- **He comprobado en haveibeenpwned.com si algún correo mío ha sido filtrado**
- **He instalado** o tengo previsto instalar **un gestor de contraseñas**
- **Tengo el 2FA activado en mi correo electrónico** principal
- **Tengo el 2FA activado en mi banca online**
- **Los accesos de empleados o colaboradores que ya no trabajan conmigo están revocados**

Cofinanciado por la Unión Europea

MINISTERIO DE HACIENDA

Fondos Europeos

GOBIERNO DE ESPAÑA · MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA · SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

red.es