Contraseñas seguras

Cómo crearlas y cuidarlas para proteger tu identidad digital y tus datos.

La importancia de las contraseñas

Las contraseñas son las llaves de tus cuentas, dispositivos e información personal. Si alguien las obtiene, puede acceder a tus datos, hacerse pasar por vos, vaciar tus cuentas o afectar tu privacidad.

Elegir una buena contraseña es una de las medidas más simples y efectivas para cuidar tu información.

¿Qué es una contraseña segura?

Robusta	Difícil de adivinar. Cuanto más predecible, más fácil de vulnerar.
Única	Distinta para cada servicio. Si una cuenta se ve comprometida, las demás siguen protegidas.
Secreta	No se comparte con nadie.
Bien guardada	Nada de cuadernos, post-it ni archivos sin protección. Lo ideal es un gestor de contraseñas, como Bitwarden o KeePass.

Qué no hacer

- Usar datos personales: nombre, fecha de nacimiento, dirección, nombre de tu mascota o tu equipo favorito.
- Elegir contraseñas comunes, como “1234”, “qwerty” o “7777”.
- Repetir patrones obvios, como cambiar letras por números o usar el nombre de la plataforma.
- Mantener la misma estructura en todas tus claves.
- Dejar las contraseñas que vienen por defecto en dispositivos o servicios.

Qué sí hacer

- **Usá frases de contraseña.** Por ejemplo: “yo tomo café en el sillón rojo” → “ytceesr” → “ytc44,ees,R!?”.
- **Combiná palabras al azar con símbolos.** Por ejemplo: “casa$torre%perro&hijo=calle”.
- **Usá el generador** que incluyen los gestores de contraseñas.
- **Respetá el mínimo recomendado:** al menos **15 caracteres**, con **mayúsculas y minúsculas**, **números** y **caracteres especiales**.

Una contraseña distinta para cada cuenta

Si usás la misma clave en varios servicios y una plataforma sufre una filtración, alguien podría usarla para entrar al resto de tus cuentas. Por eso, cada servicio tiene que tener su propia contraseña. Un **gestor de contraseñas** te ayuda a generarlas, guardarlas y administrarlas de forma simple.

Activá el segundo factor de autenticación (MFA)

Hoy no alcanza con una buena contraseña. El MFA agrega un paso extra al iniciar sesión y protege tu cuenta aunque tu clave haya quedado expuesta. Activalo siempre que puedas.

Código por SMS o correo	Fácil de usar y compatible con la mayoría de los servicios. Es menos seguro que otras opciones, pero siempre es mejor que no tener segundo factor.
App de autenticación	Por ejemplo, Google Authenticator o Microsoft Authenticator. Es la opción más segura y recomendable.

> **Nunca compartas tus códigos de verificación con nadie, bajo ninguna circunstancia.**
>
> BA-CSIRT

Buenas prácticas adicionales

- No compartas tus contraseñas.
- No las anotes en papeles, cuadernos o archivos sin protección.
- No las guardes en el navegador.
- Mantené actualizados tus dispositivos y aplicaciones.
- Desconfiá de correos, mensajes o sitios que te pidan tus datos de acceso.