

Verificación en dos pasos: cuál usar y por qué el SMS no basta

Qué hace fuerte a una contraseña, por qué no se repite y qué segundo paso conviene para tu correo y tu banco: SMS, app de códigos o llave de acceso.



Una contraseña sola es una cerradura con una única llave. Si esa llave se copia, la puerta se abre. Esta guía explica cómo hacer una buena llave y, sobre todo, cómo ponerle a tus cuentas importantes una segunda cerradura.

Una buena contraseña es larga, no rara

Los programas que adivinan contraseñas ya conocen los trucos de siempre: cambiar la «a» por «@», la «o» por «0», añadir un «!» al final. Lo que de verdad les cuesta es el **largo**: cada carácter que sumas multiplica el trabajo.

- Prefiere una frase de cuatro o cinco palabras que no tengan relación entre sí a una palabra corta llena de símbolos.
- Que no salga de nada que se sepa de ti: ni tu fecha de nacimiento, ni el nombre de tu mascota, ni tu equipo de fútbol. Todo eso aparece en tus redes.

Una contraseña distinta para cada cuenta

Si repites la misma contraseña, basta con que se filtre la del sitio más pequeño para que alguien la pruebe en tu correo y en tu banco. Y «distinta» significa sin parecido: cambiar solo el número del final no sirve, porque es lo primero que se prueba.

Nadie puede recordar decenas de contraseñas distintas. Para eso existen los **gestores de contraseñas**: aplicaciones que crean y guardan una clave diferente para cada sitio. Tú solo recuerdas una, la clave maestra, que debe ser larga y no usarse en ningún otro sitio.

El segundo paso: una cerradura más

La verificación en dos pasos pide algo más que la contraseña al entrar. Así, aunque alguien tenga tu contraseña, se queda fuera. Pero no todos los segundos pasos protegen igual.

Por qué el código por SMS es el más débil

El código por mensaje de texto es mucho mejor que nada, pero depende de tu línea telefónica. Existe un engaño llamado **duplicado de SIM**: alguien convence a tu operadora de pasar tu número a un chip suyo y, desde ese momento, los códigos le llegan a él.

Se reconoce por dos señales que aparecen juntas:

- Tu teléfono se queda **sin servicio** de golpe, aunque el Wi-Fi siga funcionando.
- Te llegan avisos de códigos o de cambios de contraseña que **tú no pediste**.

Si las ves, llama a tu operadora desde otro teléfono y pregunta si hubo un cambio de SIM. Después entra a tus cuentas importantes desde un aparato de confianza.

Mejor: una app de códigos

Una app de códigos no recibe nada por la red: **calcula** un número nuevo cada pocos segundos a partir de un secreto que solo conocen la app y el servicio. Como nada viaja por la línea telefónica, un duplicado de SIM no le sirve a nadie y funciona aunque no tengas cobertura.

Al activarla, el servicio muestra un código QR para vincularla. No le hagas foto a ese QR ni lo compartas: con él, otra persona podría generar tus mismos códigos.

Todavía mejor: las llaves de acceso

Las **llaves de acceso** (en inglés, passkeys) sustituyen a la contraseña. Tu teléfono guarda una llave y la usa cuando la apruebas con tu huella, tu cara o tu PIN. No hay nada que teclear ni que te puedan robar con una página falsa, porque la llave solo funciona en la dirección real del sitio. Si tu correo o tu banco la ofrecen, actívala.

No te quedes fuera de tu propia cuenta

Cuando actives el segundo paso, el servicio te dará unos **códigos de respaldo**. Sirven para entrar si pierdes el teléfono, y cada uno vale una sola vez.

- Guárdalos fuera del teléfono: en papel o en tu gestor de contraseñas.
- No los guardes como foto en el mismo teléfono: si lo pierdes, los pierdes con él.
- Si cambias de teléfono, pasa la app de códigos al nuevo **antes** de borrar el viejo.

Tu lista para hoy

1. Instalé una app de códigos desde la tienda oficial de mi teléfono.
2. Activé la verificación en dos pasos en mi correo principal, con la app y no con SMS.
3. Guardé los códigos de respaldo fuera del teléfono.
4. Cerré la sesión y volví a entrar para comprobar que funciona.
5. Hice lo mismo con mi banco, o activé su llave de acceso si la ofrece.

Práctico · Módulo 2 de Tu primer escudo: Claves y el segundo paso

En el módulo generas una clave y ves cuánto tardaría en romperse, y sigues a alguien cuyo teléfono se queda sin señal mientras le llegan códigos que no pidió. Puedes leer las salas sin cuenta; responder los casos y guardar tu avance pide iniciar sesión.

Empieza aquí: pro.whoami-labs.com/rutas/tu-primer-escudo/claves-y-el-segundo-paso

Esta guía en la web: pro.whoami-labs.com/guias/verificacion-en-dos-pasos