

GUÍA PRÁCTICA

Tu plan de seguridad personal en 30 días

Una lista corta que sí puedas mantener: qué proteger primero, qué revisar cada mes, qué hacer cuando salta una alerta y cómo recuperar el acceso si algo sale mal.



No hace falta saber de tecnología ni comprar nada para estar mejor protegido. Hace falta un plan corto que de verdad cumplas. Un plan pequeño que usas protege más que uno perfecto que se queda en un cajón.

Las cuatro partes de tu plan

Cabe en una hoja:

- **Lo que proteges primero:** tus cuentas clave. Casi siempre son el correo principal, el banco y la mensajería. El correo va el primero porque con él se recuperan todas las demás.
- **Lo que mejoras hoy:** una contraseña distinta y larga en cada una, y la verificación en dos pasos activada.
- **Cómo vuelves a entrar:** un correo y un teléfono de recuperación que sigan siendo tuyos, y los códigos de respaldo guardados fuera del teléfono.
- **A quién avisas:** el teléfono de tu banco, la persona de confianza que te ayuda con la tecnología y dónde se reporta un problema en cada servicio.

Hoy, cada mes y cuando salta una alerta

Hoy, una sola vez:

1. Elige tus tres cuentas clave.
2. Dales una contraseña única y la verificación en dos pasos.
3. Guarda los códigos de respaldo en un lugar privado y fuera del teléfono.

Cada mes, diez minutos:

1. Instala las actualizaciones pendientes.
2. Revisa en tus cuentas clave si hay inicios de sesión que no reconoces.
3. Comprueba que tus fotos y documentos tienen una copia reciente.

Cuando salta una alerta, no pulses el enlace del aviso: entra tú por la app oficial y mira desde dentro.

No hace falta cambiar contraseñas por calendario si son únicas y fuertes. Se cambian cuando se repitieron en otro sitio, cuando se filtraron o cuando hubo una alerta real.

El orden cuando algo no cuadra

Te llega un aviso de un inicio de sesión que no reconoces. El susto empuja a hacer todo a la vez; un orden fijo baja la presión:

1. **Comprueba** desde la app o la web oficial que la alerta aparece dentro de tu cuenta.
2. **Cierra las sesiones** y los dispositivos que no reconozcas.
3. **Cambia la contraseña** por una nueva que no uses en ningún otro sitio.
4. **Activa o renueva** la verificación en dos pasos.
5. **Revisa** que el correo y el teléfono de recuperación sigan siendo tuyos.

Si esa contraseña la usabas en otra cuenta, cámbiala también allí, empezando por el correo y por lo que mueve dinero.

Tu reto de 30 días

Un plan que no se vuelve a mirar se oxida. Este reto lo convierte en costumbre:

- **Semana 1:** tu correo principal con contraseña única, verificación en dos pasos y códigos de respaldo guardados.
- **Semana 2:** lo mismo para tu banco y tu mensajería.
- **Semana 3:** permisos de las apps revisados y redes sociales con la audiencia ajustada.
- **Semana 4:** tu primera copia de seguridad, comprobada abriendo dos archivos.
- **Día 30:** vuelve a mirar tu plan y apunta en el calendario la próxima revisión.

Tu lista para hoy

1. Escribí mis tres cuentas clave en una hoja.
2. Anoté a dónde llega mi enlace de «olvidé mi contraseña» y comprobé que es mío.
3. Guardé los teléfonos de mi banco y de mi persona de confianza.
4. Puse en mi calendario un recordatorio mensual de diez minutos.
5. Apunté el día 30 para revisar mi plan.

Prácticalo · Módulo 8 de Tu primer escudo: Tu plan personal

En el módulo completas el plan a medias de otra persona, escribes el tuyo y terminas con un caso final que no conoces: una tienda de barrio cuyos clientes dicen haber pagado pedidos que nadie cobró. 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/tu-plan-personal

Esta guía en la web: pro.whoami-labs.com/guias/plan-de-seguridad-personal