



ControlMed

Guía del médico

Verificación en dos pasos — Guía del médico

Cómo activar la verificación en dos pasos, guardar tus códigos de respaldo y recuperar el acceso si pierdes tu teléfono.

ControlMed · controlmed.com.mx · Guía para el médico · 11 de julio de 2026



Índice

1. Qué es la verificación en dos pasos y por qué activarla	2
2. Cómo activarla, paso a paso	2
3. Tus códigos de respaldo (¡guárdalos!)	2
4. Perdiste tu teléfono: qué hacer	3
5. Regenerar tus códigos	3
6. Preguntas frecuentes	3
7. Recomendaciones de seguridad	3



Esta guía es para ti, el médico que usa ControlMed. Está escrita en lenguaje sencillo, sin tecnicismos. Te explica qué es la verificación en dos pasos, cómo activarla, y —lo más importante— cómo recuperar el acceso a tu cuenta si pierdes tu teléfono.

1. Qué es la verificación en dos pasos y por qué activarla

La verificación en dos pasos (también llamada "2FA") es una capa extra de seguridad para tu cuenta. Con ella, además de tu contraseña, al iniciar sesión te pedimos un código temporal que genera una app en tu teléfono.

¿Por qué importa tanto en tu caso? Porque tu expediente contiene **datos de salud de tus pacientes**. Si alguien te roba o adivina tu contraseña, con la verificación en dos pasos activada **no le basta para entrar**: necesitaría también tu teléfono. Es la diferencia entre una puerta con una cerradura y una puerta con dos.

Te recomendamos activarla. Es rápido y solo lo haces una vez.

2. Cómo activarla, paso a paso

1. **Descarga una app de autenticación** en tu teléfono. Las más comunes son **Google Authenticator**, **Microsoft Authenticator** o **Authy**. Cualquiera funciona; son gratuitas. 2. En ControlMed, entra a **Seguridad** y pulsa **"Activar 2FA"**. 3. Verás un **código QR**. Abre tu app de autenticación, elige "escanear código" y apunta la cámara al QR. (Si no puedes escanear, la app te deja escribir la clave a mano; ControlMed también te la muestra.) 4. Tu app empezará a mostrar un **código de 6 dígitos** que cambia cada 30 segundos. Escríbelo en ControlMed y pulsa **"Activar"**.

Listo: la próxima vez que inicies sesión, después de tu contraseña te pediremos el código de 6 dígitos de tu app.

3. Tus códigos de respaldo (¡guárdalos!)

Esta es la sección más importante de toda la guía. Léela con calma.

En el momento en que activas la verificación en dos pasos, ControlMed te muestra 10 códigos de respaldo.

- **Son tu única forma de entrar si pierdes tu teléfono.** Si tu teléfono se pierde, se rompe o borras la app de autenticación, estos códigos son lo que te permite volver a entrar a tu cuenta.
- **Guárdalos FUERA de tu teléfono.** Imprímelos y guárdalos en un lugar seguro (un cajón con llave, tu consultorio), anótalos en papel, o guárdalos en un gestor de contraseñas. Lo importante es que **no dependan del mismo teléfono** que tiene la app de autenticación: si pierdes ese teléfono, no querrás perder también los códigos.
- **Solo se muestran UNA VEZ.** Al activarlos, ControlMed te ofrece **copiarlos o descargarlos como archivo**. Hazlo en ese momento. Después no se vuelven a mostrar (por seguridad, nadie —ni tú desde otra pantalla— puede volver a verlos).
- **Cada código sirve UNA SOLA VEZ.** Cuando usas uno para entrar, ese código deja de funcionar. Por eso son 10: te alcanzan para varias emergencias.

Si no guardaste tus códigos al activar el 2FA, no te preocupes: puedes generar unos nuevos en cualquier momento (ver la sección "Regenerar tus códigos").



4. Perdiste tu teléfono: qué hacer

No entres en pánico. Tienes tres niveles de recuperación, del más simple al último recurso.

Paso 1 — Usa un código de respaldo. En la pantalla donde te pedimos el código de 6 dígitos, pulsa el enlace "**¿Perdiste tu teléfono? Usa uno de tus códigos de respaldo.**". Escribe uno de tus códigos de respaldo (el formato es tipo XXXX-XXXX) y entra con normalidad.

Paso 2 — Reconfigura el 2FA en tu teléfono nuevo. Una vez dentro, ve a **Seguridad**. Ahí puedes desactivar y volver a activar la verificación en dos pasos con la app de tu teléfono nuevo. Aprovecha para **regenerar tus códigos de respaldo** y guárdalos otra vez en un lugar seguro.

Paso 3 — Último recurso: contacta a soporte. Si también perdiste tus códigos de respaldo, escríbenos a **info@controlmed.com.mx** o llámanos al **33 1098 5044**. Antes de restablecer tu acceso, **te pediremos verificar tu identidad** (por ejemplo, una llamada al teléfono registrado en tu cuenta y el cotejo de una identificación oficial). Puede parecer estricto, pero es exactamente lo que protege tu cuenta: así nos aseguramos de que solo tú puedas pedir ese restablecimiento, y no alguien haciéndose pasar por ti.

5. Regenerar tus códigos

Puedes generar un juego nuevo de 10 códigos cuando quieras, desde **Seguridad -> Regenerar**. Te pediremos un código actual de tu app (o uno de respaldo que aún tengas) para confirmar que eres tú.

Importante: al regenerar, **los códigos anteriores dejan de funcionar**. Los nuevos son los únicos válidos, así que guárdalos y descarta la lista vieja.

¿Cuándo conviene regenerar?

- Cuando ya usaste varios y te quedan pocos (ControlMed te muestra cuántos te quedan y te avisa si llegas a cero).
- Si crees que tu lista de códigos pudo quedar expuesta (la perdiste, la dejaste a la vista).
- Después de recuperar tu cuenta con un código de respaldo.

6. Preguntas frecuentes

¿Qué app de autenticación uso? Cualquiera estándar sirve: Google Authenticator, Microsoft Authenticator o Authy son las más usadas y gratuitas.

¿Qué pasa si cambio de teléfono? Lo ideal es configurar la verificación en dos pasos en tu teléfono nuevo **antes** de deshacerte del viejo (desde Seguridad). Si ya no tienes el viejo, entra con un código de respaldo y vuelve a configurarla en el nuevo.

¿Es obligatorio el 2FA? No es obligatorio, pero sí muy recomendable por el tipo de información que manejas. Puedes activarlo y desactivarlo cuando quieras desde Seguridad.

¿Qué pasa si alguien usa uno de mis códigos? Cada vez que se usa un código de respaldo para entrar a tu cuenta, **te enviamos un correo de aviso** que dice cuántos códigos te quedan. Si recibes ese correo y **no fuiste tú**, cambia tu contraseña de inmediato y regenera tus códigos de respaldo (los que tenías dejarán de servir). Si tienes dudas, contáctanos.

7. Recomendaciones de seguridad

- **No compartas tus códigos con nadie.** Ni siquiera con el soporte de ControlMed: **nunca te los pediremos**. Si alguien dice ser de ControlMed y te pide tus códigos o tu contraseña, no es de ControlMed.
- **No guardes los códigos en el mismo teléfono** que tiene la app de autenticación. Si pierdes ese teléfono, perderías ambas cosas a la vez.



- Guarda una copia impresa o en un gestor de contraseñas, en un lugar al que solo tú tengas acceso.
- Trata tus códigos de respaldo con el mismo cuidado que las llaves de tu consultorio.