

Seguridad de tu cuenta: verificación en dos pasos y claves de acceso

Para qué sirve

Tu cuenta es la llave de todo tu negocio: los datos de tus clientes, las reservas, los fichajes de tus empleados y tu facturación. Si alguien entra en ella, entra en todo. En este capítulo aprenderás a blindarla con cuatro herramientas: una contraseña fuerte, la verificación en dos pasos, las claves de acceso (tu huella o tu cara) y el control de los dispositivos que se conectan.

No hace falta que sepas nada de informática. Todo se hace desde una sola pantalla y en unos minutos.

Dónde se configura la seguridad de tu cuenta

Todos los ajustes de este capítulo viven en el mismo sitio.

1. Entra en tu panel de gestión.
2. Haz clic en tu **foto de perfil** (arriba, en la barra superior) y elige **Mi perfil**.
3. Verás una fila de pestañas: **Datos**, **Pedidos**, **Contraseña**, **2FA** y **Passkeys**.
4. Las tres últimas son las que nos interesan aquí.

Nota: si tu cuenta es de cliente y no gestionas ningún local, encontrarás exactamente las mismas pestañas en tu página **Mi cuenta**. Los pasos son idénticos.

Cambiar tu contraseña

1. En **Mi perfil**, haz clic en la pestaña **Contraseña**.
2. Rellena **Contraseña actual** con la que usas ahora mismo.
3. Escribe la nueva en **Nueva contraseña** y repítela en **Confirmar**.
4. Fíjate en la lista de requisitos que hay justo debajo: se van marcando con un tic verde según escribes.
5. Cuando estén todos en verde, pulsa **Cambiar contraseña**.

Estos son los requisitos que tiene que cumplir tu nueva contraseña:

Requisito	Qué significa
Minúscula	Al menos una letra minúscula (a-z)
Mayúscula	Al menos una letra mayúscula (A-Z)
Número	Al menos una cifra (0-9)

Requisito	Qué significa
Símbolo	Al menos un signo como !, @, #, -, _
6+ caracteres	Mínimo seis caracteres de largo
Coinciden	Las dos casillas tienen que ser iguales

Consejo: el mínimo son seis caracteres, pero eso es solo el mínimo legal del sistema, no una buena idea. Una frase larga que recuerdes fácil, del tipo **MiGimnasio2Puertas!**, es mucho más segura que un **Ab1!xz** corto y raro.

Aviso: si te equivocas en la **Contraseña actual**, el sistema no cambiará nada y te avisará. Es una protección para que nadie que se sienta en tu ordenador con la sesión abierta pueda cambiarte la contraseña sin saber la anterior.

Recibir un enlace por email para cambiar la contraseña

¿No recuerdas tu contraseña actual pero tienes la sesión abierta? No hace falta que cierres sesión.

1. Ve a la pestaña **Contraseña**.
2. Haz clic en el enlace **No recuerdo mi contraseña, enviar enlace para establecerla**.
3. Aparecerá una ventana de confirmación. Pulsa **Enviar email**.
4. Abre tu correo y haz clic en el enlace que te hemos enviado.
5. Escribe la contraseña nueva (sin pedirte la antigua) y guárdala.

Importante: ese enlace **caduca a los 10 minutos** por seguridad. Si tardas más, simplemente pide otro. Y solo puedes pedir un enlace cada 5 minutos: si lo intentas antes, te dirá que esperes.

Recuperar la contraseña si no puedes entrar

Si estás fuera y no consigues acceder:

1. En la pantalla de inicio de sesión, haz clic en **¿Olvidaste tu contraseña?**.
2. Escribe tu **correo electrónico** en la casilla.
3. Pulsa **Enviar enlace de recuperación**.
4. Revisa tu bandeja de entrada (y la carpeta de spam) y abre el enlace.
5. Establece tu nueva contraseña.

Nota: por seguridad, la pantalla siempre te dirá lo mismo, exista o no esa cuenta. Así, si alguien prueba con correos ajenos, no puede averiguar quién tiene cuenta con nosotros. El enlace también caduca a los 10 minutos y solo puedes pedir 3 en una hora.

Activar la verificación en dos pasos (2FA)

La verificación en dos pasos añade una segunda barrera: aunque alguien robe tu contraseña, no podrá entrar sin el móvil que tienes en el bolsillo. Es la mejor mejora de seguridad que puedes hacer hoy en cinco minutos.

Antes de empezar instala en tu móvil una app de autenticación gratuita. Las más habituales son **Google Authenticator** o **Authy**, y las tienes en la tienda de aplicaciones de tu móvil.

1. Ve a **Mi perfil** y haz clic en la pestaña **2FA**.
2. Verás una etiqueta naranja que pone **2FA inactivo**. Pulsa el botón verde **Activar 2FA**.
3. Aparecerá un **código QR** en pantalla. No cierres esta ventana.
4. Abre la app de autenticación en el móvil y pulsa su botón de añadir cuenta (normalmente un +), eligiendo la opción de **escanear código QR**.
5. Enfoca el QR de la pantalla con la cámara del móvil. La app añadirá una entrada llamada **Newaccess** con tu correo.
6. La app te mostrará un número de **6 dígitos** que cambia cada 30 segundos. Escríbelo en la casilla **Código de verificación**.
7. Pulsa **Verificar y activar**.
8. Verás el mensaje **2FA Activado** y la etiqueta pasará a verde.

Consejo: si tu móvil no lee el QR (mala luz, cámara con problemas), usa el campo **O introduce este código manualmente** que hay debajo. Copia esa cadena de letras y pégala a mano en tu app de autenticación. Funciona exactamente igual.

Aviso muy importante: guarda ese código manual en un lugar seguro (una nota en tu gestor de contraseñas, por ejemplo) **antes** de terminar. Si algún día pierdes el móvil, ese código es lo que te permitirá volver a configurar la app en un teléfono nuevo sin depender de nadie.

Entrar con la verificación en dos pasos activada

Una vez activada, tu forma de entrar cambia ligeramente.

1. Escribe tu correo y tu contraseña como siempre y pulsa **Iniciar Sesión**.
2. En lugar de entrar directamente, verás la pantalla **Verificación 2FA**.
3. Abre tu app de autenticación y mira el código de 6 dígitos del momento.
4. Escríbelo en la casilla y pulsa el botón de verificar.

Nota: el sistema acepta también el código de los 30 segundos anteriores, así que si el número cambia justo mientras lo tecleas, no pasa nada. Si te sale **Código incorrecto**, comprueba que la hora de tu móvil esté puesta en automático: es la causa número uno

de este fallo.

Este segundo paso se te pedirá tanto si entras con tu contraseña, como si entras con el botón de **Google**, como si entras con tu clave de acceso. La protección va contigo por cualquier puerta.

Desactivar la verificación en dos pasos

1. Ve a **Mi perfil** y a la pestaña **2FA**.
2. Pulsa el botón rojo **Desactivar 2FA**.
3. Se abrirá una casilla. Escribe el código de 6 dígitos actual de tu app.
4. Pulsa **Confirmar desactivación**.

Aviso: para desactivarla **necesitas un código válido**. No se puede quitar sin el móvil. Si has perdido el teléfono y no guardaste el código manual, tendrás que escribir a soporte para que verifiquen tu identidad y la retiren a mano.

Ten en cuenta: al desactivarla se borra el vínculo con tu app. Si más adelante quieres volver a activarla, tendrás que escanear un **código QR nuevo**; el antiguo ya no sirve y puedes borrar esa entrada de tu app.

Crear una clave de acceso (passkey)

Una clave de acceso te deja entrar con tu **huella dactilar**, tu **cara (Face ID)** o tu **PIN de Windows Hello**, sin escribir ninguna contraseña. Es más rápido y, además, más seguro: no hay ninguna contraseña que robar o que te puedan sacar con un engaño.

1. Ve a **Mi perfil** y haz clic en la pestaña **Passkeys**.
2. Pulsa el botón **Añadir clave de acceso**.
3. Te pedirá un **nombre** para reconocerla. Pon algo descriptivo: **Mi PC de la oficina**, **iPhone de Ana**, **Portátil de casa**.
4. Pulsa **Continuar**.
5. Tu propio dispositivo tomará el mando: te pedirá tu huella, tu cara o tu PIN. Confírmalo.
6. Verás el mensaje **Registrada** y la clave aparecerá en la lista.

Nota: si no ves el botón **Añadir clave de acceso**, es que el navegador o el equipo desde el que estás no admite esta tecnología. Prueba desde un móvil moderno o desde un navegador actualizado (Chrome, Edge, Safari o Firefox).

Consejo: registra una clave en **cada dispositivo** que uses habitualmente: el ordenador del mostrador y tu móvil, por ejemplo. Cada uno tendrá la suya, con su nombre, y podrás

quitarlas por separado.

Entrar con tu clave de acceso

1. En la pantalla de inicio de sesión, mira los botones redondos que hay debajo del formulario.
2. Haz clic en el botón de la **llave**.
3. Tu dispositivo te pedirá la huella, la cara o el PIN.
4. Entrarás directamente, sin escribir correo ni contraseña.

Eliminar una clave de acceso

Si vendes un ordenador, cambias de móvil o pierdes un dispositivo, retira su clave cuanto antes.

1. Ve a **Mi perfil** y a la pestaña **Passkeys**.
2. Localiza la clave en la lista. Cada una muestra su **nombre** y la **fecha en que se registró**.
3. Pulsa el botón rojo de la **papelera** que hay a su derecha.
4. Confirma pulsando **Eliminar**.

Entrar con Google o con Apple

Además del correo y la contraseña, en la pantalla de inicio de sesión tienes botones redondos para entrar con tu cuenta de **Google** o de **Apple**. Es cómodo porque no tienes que recordar nada.

1. Pulsa el botón de **Google** o el de **Apple**.
2. Elige tu cuenta en la ventana que aparece y autoriza el acceso.
3. Si es la primera vez, te crearemos la cuenta automáticamente y te enviaremos un correo de bienvenida.
4. Si tienes la verificación en dos pasos activa, te pediremos además tu código de 6 dígitos.

Consejo: en la pantalla de inicio de sesión hay una casilla **Recuérdame**. Márcala solo en tus dispositivos personales: mantiene tu sesión abierta durante 30 días. Nunca la marques en un ordenador compartido o en el del mostrador de cara al público.

Qué método de acceso te conviene

Método	Rapidez	Seguridad	Ideal para
Correo y contraseña	Normal	Media	Tenerlo siempre como respaldo
Correo + verificación en dos pasos	Un poco más lento	Muy alta	La opción recomendada para el día a día
Clave de acceso (huella / Face ID)	Muy rápida	Muy alta	Tu móvil y tu ordenador de confianza

Método	Rapidez	Seguridad	Ideal para
Google o Apple	Rápida	Alta	Quien ya vive dentro de esas cuentas

Nuestra recomendación: activa la verificación en dos pasos **y** registra una clave de acceso en tus dispositivos habituales. Entrarás con la huella en un segundo y, el día que falle algo, seguirás teniendo la contraseña con el código como red de seguridad.

Autorizar o rechazar un dispositivo nuevo

Tu cuenta vigila desde qué móvil se usa la app. Si detectamos que **un dispositivo distinto** intenta entrar con tus credenciales, te avisamos por correo antes que nada.

1. Recibirás un email con el asunto **Dispositivo no reconocido**, indicando el nombre del aparato y desde qué conexión se intentó.
2. Haz clic en el enlace del correo. Se abrirá la página **¿Reconoces este dispositivo?**.
3. Verás el nombre del dispositivo detectado en un recuadro.
4. **Si eres tú** (te has comprado un móvil nuevo, por ejemplo), pulsa el botón verde **Autorizar**.
5. **Si no eres tú**, pulsa el botón rojo **Rechazar** y confirma pulsando **Bloquear**. Ese aparato no podrá entrar con tu cuenta.

Aviso: si recibes este correo y **no** has cambiado de móvil, rechaza el dispositivo y cambia tu contraseña inmediatamente. Es la señal de que alguien tiene tus credenciales.

Ten muy presentes estas dos reglas del sistema:

- Solo se permite **cambiar de dispositivo una vez cada 24 horas**.
- Autorizar dispositivos nuevos una y otra vez se interpreta como que estás **compartiendo tu cuenta**. La primera vez recibirás un simple aviso; si se repite, la cuenta acumula advertencias y puede quedar suspendida temporalmente. A partir de cuatro advertencias sin apelar, el bloqueo es permanente.

Importante: no compartas tu cuenta con nadie, ni siquiera con tu socio o tus empleados. Si necesitan acceso, dales su propio usuario desde la gestión de empleados de tu local. Es gratis, es más seguro y así sabrás quién hace cada cosa.

Preguntas frecuentes

¿He perdido el móvil con la app de autenticación y no puedo entrar. Qué hago?

Si guardaste el código manual que te mostramos al activarla, instala la app en tu móvil nuevo,

introduce ese código a mano y volverás a tener tus 6 dígitos. Si no lo guardaste, escribe a soporte: verificaremos tu identidad y desactivaremos la verificación a mano para que puedas entrar y volver a configurarla.

¿Puedo tener a la vez verificación en dos pasos y clave de acceso?

Sí, y es lo que recomendamos. Son cosas distintas y compatibles: la clave de acceso es tu puerta rápida del día a día, y la verificación en dos pasos protege la puerta clásica del correo y la contraseña. Si entras con la clave de acceso y tienes la verificación activa, también te pediremos el código.

¿Las claves de acceso guardan mi huella en vuestros servidores?

No, en ningún momento. Tu huella o tu cara nunca salen de tu dispositivo: se quedan dentro de tu móvil o de tu ordenador. Nosotros solo guardamos el nombre que le pusiste a la clave y la fecha en que la registraste.

¿Por qué me dice "Código incorrecto" si estoy copiando bien los 6 dígitos?

Casi siempre es la hora del móvil. Estos códigos se calculan con la hora exacta, así que si tu teléfono va adelantado o atrasado unos minutos, los números no cuadran. Entra en los ajustes de fecha y hora de tu móvil y activa la opción automática. También comprueba que no estés leyendo el código de otra cuenta distinta dentro de la app.

¿Puedo cambiar el correo de mi cuenta desde Mi perfil?

No. El campo del correo aparece en gris porque no se puede editar: es el identificador de tu cuenta y de él cuelgan tus accesos, tus pedidos y tus avisos de seguridad. Si necesitas cambiarlo, contacta con soporte.

¿Cada cuánto debería cambiar mi contraseña?

No hay que cambiarla por rutina. Cámbiala si sospechas que alguien la conoce, si la has reutilizado en otra web que ha sufrido un robo de datos, o si recibes un aviso de dispositivo no reconocido que no eras tú. Es mucho más eficaz tener una contraseña larga y única con verificación en dos pasos que cambiar cada mes una contraseña corta.

Glosario

- **Verificación en dos pasos (2FA):** segunda comprobación al entrar. Además de tu contraseña, pedimos un código temporal de tu móvil. Aunque te roben la contraseña, sin tu teléfono no entran.
- **App de autenticación:** aplicación gratuita de móvil (Google Authenticator, Authy) que genera los códigos de 6 dígitos que cambian cada 30 segundos.
- **Código QR:** el cuadro de puntos blanco y negro que escaneas con la cámara para vincular tu app de autenticación con tu cuenta, sin teclear nada.
- **Clave de acceso (passkey):** forma de entrar sin contraseña usando la huella, la cara o el PIN

de tu propio dispositivo. Es más rápida y no se puede robar por correo falso.

- **Face ID:** sistema de reconocimiento facial de los iPhone y iPad.
- **Windows Hello:** sistema de Windows que te identifica por huella, cara o un PIN del propio ordenador.
- **Recuérdame:** casilla del inicio de sesión que mantiene tu sesión abierta 30 días en ese dispositivo.
- **Dispositivo no reconocido:** aviso que te enviamos por correo cuando alguien intenta usar tu cuenta desde un móvil distinto al habitual.
- **Advertencia:** marca que el sistema pone en tu cuenta cuando detecta señales de que se está compartiendo. Acumular varias puede suspenderla.
- **Enlace de recuperación:** enlace temporal que te enviamos por correo para poner una contraseña nueva. Caduca a los 10 minutos.