



Un **gestor de contraseñas** es una solución que ayuda a los usuarios a **almacenar, gestionar y compartir de forma segura sus credenciales de acceso**. Algunos gestores de contraseñas también ayudan a almacenar de forma segura datos adicionales como **claves de acceso, documentos, archivos e imágenes**.

Protege tu gestor de contraseñas



Contraseña maestra segura

Es recomendable que la clave de acceso a tu gestor sea lo suficientemente robusta como para no ser vulnerada fácilmente.

Recuerda que, en él, pueden residir los accesos a portales o aplicaciones que contengan tus datos personales.



Habilita el doble factor de autenticación

Si es posible, habilita en tu gestor el doble factor de autenticación. Añadirá seguridad adicional en su acceso



Revisa frecuentemente el gestor

Es recomendable que accedas al gestor con frecuencia. Puede ser que nuevas contraseñas hayan sido comprometidas.



Activa el bloqueo automático

Si es posible activa el cierre de la sesión tras un cierto periodo de inactividad. Esto te protegerá ante posibles descuidos.



Cambia las contraseñas sugeridas

Normalmente los gestores analizan tus contraseñas usadas. Intenta cambiar aquellas que estén repetidas, que no sean seguras o bien hayan sido vulneradas.

Gestores de contraseñas reconocidos



No utilices cualquier gestor de contraseñas, pueden ser que sean fraudulentos.

A continuación puedes consultar una lista de los más reconocidos:

- Llaverito de iCloud (Apple)
- Google password manager
- Microsoft Authenticator
- 1Password (compatible con todos los SO)
- Bitwarden (compatible con todos los SO)



¿No usas un gestor de contraseñas? ¡Tranquilo! Puedes comprobar si tus credenciales han sido comprometidas:



Click para comprobarlo