



# GESTOR DE CONTRASEÑAS

Un gestor de contraseñas es una herramienta que se ocupa de crear, recordar y rellenar las contraseñas.

# TIPOS DE GESTOR DE CONTRASEÑAS

## SIMPLE

No crea contraseñas, las guarda. Por lo que podremos poner contraseñas seguras y complejas sin la necesidad de recordarlas. Además, va asociado a nuestra cuenta de correo, por lo que si cambiamos de dispositivo solo tendremos que poner la contraseña del correo. Suelen ser gratuitos.

Ejemplo: Gestor de contraseñas de Google

## COMPLEJO

Son programas especializados, los cuales crean una contraseña segura y la recuerdan en nuestro navegador o en nuestro dispositivo. Suelen ser de pago.

Por ejemplo: LastPass es un gestor conocido, pero todos tienen en base el mismo funcionamiento.

VS



### Seguridad de conocimiento cero

La información guardada en la bóveda es secreta, incluso para LastPass. Su bóveda se cifra y descifra a nivel de dispositivo. La contraseña maestra es la única forma de acceder a ella.

[Más información sobre seguridad >](#)



### Amenazas digitales en el radar

Los robos de datos son cada vez más habituales. El Control de Dark Web le avisa de inmediato en caso de exposición de sus datos online.

[Control de Dark Web >](#)



### Cambio de hábitos

LastPass le ayuda a encontrar y cambiar contraseñas poco seguras y reutilizadas por contraseñas únicas creadas por nuestro generador de contraseñas.

[Panel de seguridad >](#)



### Autenticación multifactor

Defina un mecanismo de autenticación adicional, como un código de acceso de un solo uso o el escaneo de huellas dactilares, para que acceder a sus cuentas sea prácticamente imposible para los hackers.

[Opciones multifactor >](#)