# 

[1.](#_heading=h.30j0zll) Métodos de autenticación 1

[1.1.](#_heading=h.1fob9te) ¿Qué es la autenticación? 1

[1.2.](#_heading=h.3znysh7) Políticas de contraseñas 2

[1.2.1.](#_heading=h.2et92p0) Práctica: Política de contraseña 3

[1.3.](#_heading=h.tyjcwt) Plataformas para la gestión de contraseñas 4

# 

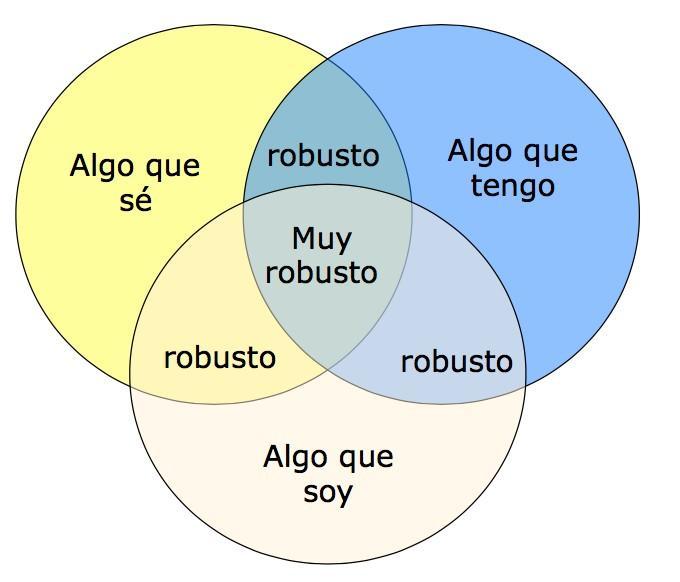
# Métodos de autenticación

## ¿Qué es la autenticación?

La autenticación es el proceso de confirmar que alguien es quien dice ser mediante la introducción de un identificador y de una contraseña que solo él sabe.

Existen varios métodos de autenticación:

* + - * Algo que sabemos, el PIN o la contraseña.
      * Algo que tenemos, tarjetas, token, fichero de llave, …
      * Algo que somos, huella biométrica digital, rostro, …



La combinación de diferentes métodos de autenticación mejora la seguridad en la cuanto a ella. Es por eso por lo que plataformas como Google ofrecen ya hoy en día la autenticación mediante doble factor: la contraseña (algo que sé) y la activación mediante el móvil (algo que se tiene).

La autenticación por contraseña es el método más utilizado para el acceso a un sistema o servicio. Es necesario identificarse con el identificador del usuario y una contraseña. Se trata de “algo que sabemos”; a menudo se utilizan un identificativo y una contraseña muy fáciles de averiguar. Contraseñas como *12345678*, fechas de cumpleaños, nombres de mascotas… son las primeras contraseñas que un atacante utilizará para poder acceder al sistema o servicio. Como curiosidad, mira el [listado de las contraseñas más utilizadas](https://www.ncsc.gov.uk/static-assets/documents/PwnedPasswordsTop100k.txt) según el NCSC (Centro Nacional de Ciberseguridad del Reino Unido).

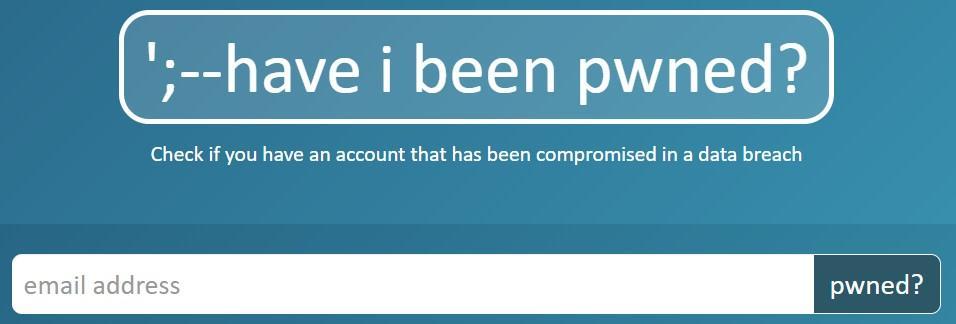
Para tener una contraseña robusta será necesario que al menos cumpla con las siguientes características:

* + **Complejidad**. Debe formarse por letras minúsculas y mayúsculas, números decimales y caracteres especiales.
  + **Longitud**. Debe tener al menos una longitud 8 caracteres.
  + **Estructura**. No debe formar parte de una palabra de ningún diccionario.
  + **Caducidad**. No debe haberse usado con anterioridad.

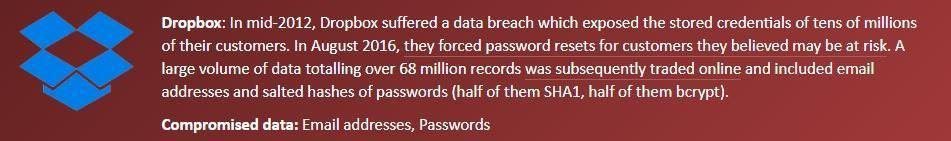


Actividad: 

Accede a <https://haveibeenpwned.com/> y comprueba si tu correo ha sido visto en algún diccionario.



Verás si tu cuenta ha sido hackeada y en qué servicios.



## Políticas de contraseñas

Si dejamos la gestión de las contraseñas en manos de los usuarios de una organización, la seguridad de ésta se verá claramente amenazada, ya que si las contraseñas son poco robustas el acceso a los equipos por parte de un intruso será muy fácil. Es por ello por lo que se hace necesario configurar e implantar una política de contraseñas que obligue a que la contraseña de cada usuario cumpla unos mínimos de seguridad.

### Práctica: Política de contraseña

Para tener una política de contraseñas robusta, realiza los siguientes pasos.

1. Preparación e instalación de paquetes:

sudo dpkg --configure –a  
sudo apt-get update

sudo apt-get -y install libpam-pwquality cracklib-runtime

1. Cambia la fecha de renovación de contraseña editando el siguiente fichero: */etc/login.defs*

sudo nano /etc/login.defs

* + Cambia el parámetro PASS\_MAX\_DAYS a 30.

PASS\_MAX\_DAYS 30

1. Edita el siguiente fichero

sudo nano /etc/pam.d/common-password

Sustituye

password requisite pam\_pwquality.so retry=3

por lo siguiente:

password requisite pam\_pwquality.so retry=3 minlen=10 maxrepeat=3 ucredit=-1 lcredit=-1 dcredit=-1 ocredit=-1 difok=3 gecoscheck=1 reject\_username enforce\_for\_root

Los parámetros introducidos significan lo siguiente:

* + **retry=3**: Preguntar al usuario 3 veces por una contraseña válida.
  + **minlen=8** : Mínimo de caracteres en la contraseña.
  + **maxrepeat=3**: Los caracteres sólo pueden aparecer 3 veces de manera consecutiva.
  + **ucredit=-1** : Debe haber al menos un carácter en mayúscula.
  + **lcredit=-1** : Debe haber al menos un carácter en minúscula.
  + **dcredit=-1** : Debe haber al menos un digito.
  + **difok=3** : como mínimo tiene 3 caracteres diferentes a la contraseña anterior.
  + **gecoscheck=1**: No debe haber palabras que aparezcan en el nombre completo de la cuenta del usuario.
  + **reject\_username**: El nombre de usuario no puede estar en la contraseña ni tampoco a la inversa.
  + **enforce\_for\_root**: Aplica la política de contraseña también para el usuario root.

1. Guarda los cambios y reinicia la máquina.

sudo reboot

Una vez reiniciado el sistema, realiza la prueba con un nuevo usuario. Para ello

1. Crea un nuevo usuario

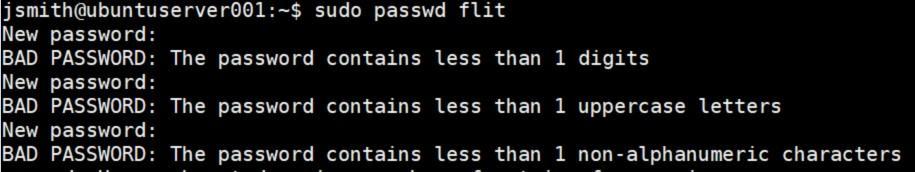
sudo useradd flit

1. Configura una contraseña para la nueva cuenta.

sudo passwd flit

1. Introduce diferentes passwords para comprobar los parámetros de complejidad configurados anteriormente: *contraseña*, *abc003*, *tilf944AS*

…



1. Finalmente, introduce una password válida; por ejemplo: Password123!



## Plataformas para la gestión de contraseñas

Hoy en día manejamos muchas cuentas online con respecto a las que no recordamos si estábamos registrados o no y mucho menos de las contraseñas que hemos utilizado para acceder.



Existen varios programas para la gestión de contraseñas que permiten almacenar usuarios, contraseñas, URLs y algunas propiedades más. El objetivo es que nuestras contraseñas, al no tener que ser recordadas por nosotros, sean muy complejas. Ni siquiera es obligatorio que nosotros las pensemos, el propio software puede hacerlo. La única que sí tendremos que recordar es la maestra, y ésa tendrá que ser muy robusta. Hay dos tipos de gestores de contraseñas: locales y online. 

**Keepass**: es un programa de gestión de contraseñas local; es gratuito y uno de los más usados.

Si usas Keepass, tendrás que mover el archivo con las contraseñas en caso de querer usarlo en más de un dispositivo; poniéndolo en el Drive, por ejemplo. Ése es el lado malo de los gestores locales.

**1Password:** es un software online. [Vídeo promocional](https://www.youtube.com/watch?time_continue=112&amp;v=mcly2-b1W20)

**Drivepassword**: software que ofrece Google para la gestión de las contraseñas. Se puede utilizar mediante una extensión.

El lado malo de los gestores online -1password, por ejemplo- es que te tienes que fiar de la empresa que te ofrece el servicio; ¿por qué no pueden ser atacados y ser tus contraseñas robadas?