

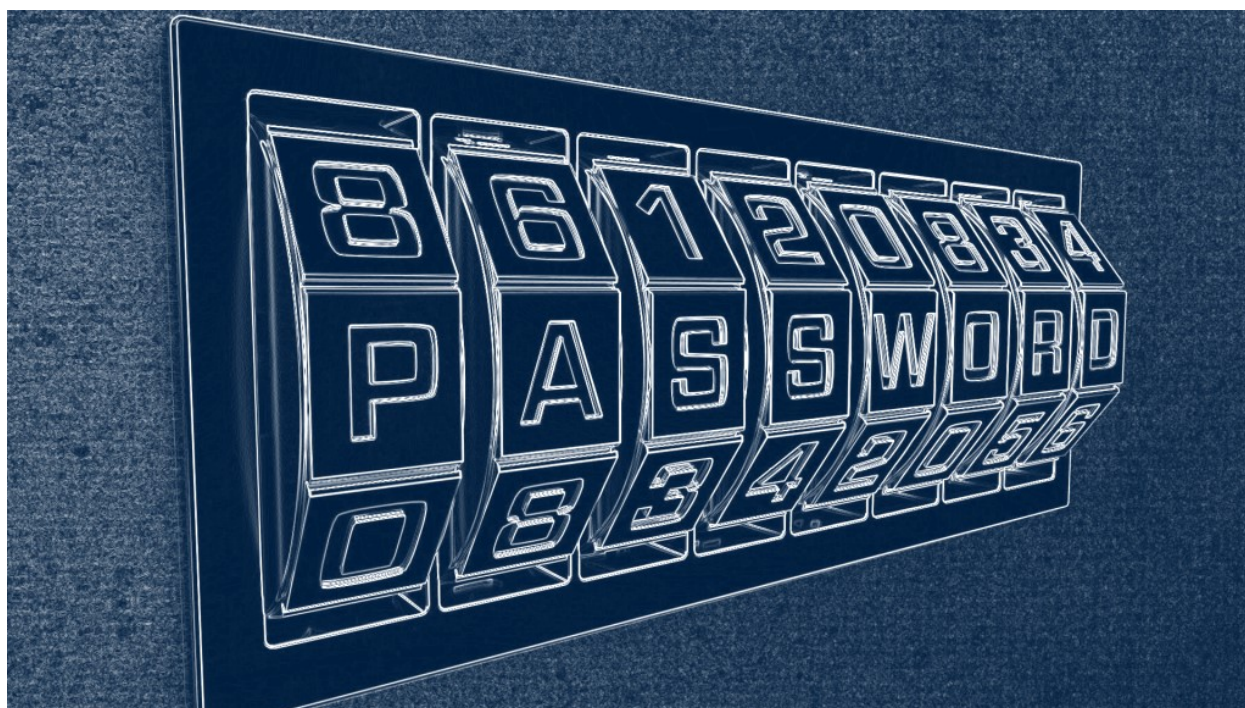


Departamento de TIC

Capsula informativa

Las contraseñas más utilizadas de 2022 Por: Juan José Ruiz.

En el *ranking* de las contraseñas más comunes de 2022, se observa que los usuarios continúan utilizando las ya clásicas ‘password’ y ‘123456’.



NordPass ha presentado un informe que recoge las contraseñas más comúnmente utilizadas por los usuarios a lo largo del año. En colaboración con investigadores independientes, se han **evaluado millones de credenciales procedentes de incidentes de ciberseguridad** para elaborar un *ranking* de las contraseñas más utilizadas y más inseguras. En total **se han analizado más de 3TB de datos procedentes de más de 30 países**, principalmente de los continentes europeo y americano.

En los 2 primeros puestos se encuentran las clásicas ‘password’ y ‘123456’, utilizadas por casi 5 millones de usuarios y más de 1.5 millones de usuarios respectivamente. Ambas son contraseñas extremadamente débiles y para nada recomendables; tanto es así que **el tiempo estimado para adivinarlas es inferior a 1 segundo** mediante un ataque de diccionario.

En el top 25 del *ranking* global se pueden encontrar principalmente **códigos numéricos** (hasta en el 76% de los casos), **palabras simples de diccionario** como ‘guest’, y **combinaciones de teclas que siguen el orden determinado por su ubicación en el teclado** como ‘qwerty’. El tiempo para obtener todas estas contraseñas es de apenas unos segundos. Únicamente una de ellas tomaría un tiempo superior al estar formada por mayúsculas, minúsculas y números: ‘D1lakiss’; sin embargo al disponer de una longitud de tan solo 8 caracteres, el tiempo es para romperla mediante un ataque de fuerza bruta es de unas 3 horas.

Avanzando en la clasificación aparecen también **nombres propios, de series y marcas** como ‘daniel’, ‘Gizli’, o ‘samsung’, e incluso **contraseñas cuya longitud es de tan solo 3 caracteres** como ‘123’, ‘vip’ o ‘usr’. El listado de las 50 peores y más utilizadas contraseñas de 2022 es el siguiente:

1. password	18. 654321	35. 222222
2. 123456	19. 7777777	36. qwertyuiop
3. 123456789	20. 123	37. qwerty123
4. guest	21. D1lakiss	38. qazwsx
5. qwerty	22. 777777	39. vip
6. 12345678	23. 110110jp	40. asdasd
7. 111111	24. 1111	41. 123qwe
8. 12345	25. 987654321	42. 123654
9. col123456	26. 121212	43. iloveyou
10. 123123	27. Gizli	44. a1b2c3
11. 1234567	28. abc123	45. 999999
12. 1234	29. 112233	46. Groupd2013
13. 1234567890	30. azerty	47. 1q2w3e
14. 000000	31. 159753	48. usr
15. 555555	32. 1q2w3e4r	49. Liman1000
16. 666666	33. 54321	50. 1111111
17. 123321	34. pass@123	

Top50 global de contraseñas más comunes en 2022

También se encuentra disponible un *ranking* para cada país. En el caso de usuarios españoles, la contraseña más utilizada en 2022 ha sido el código numérico ‘123456’. También se pueden encontrar **palabras simples, nombres propios, ciudades y equipos de fútbol** como ‘hola’, ‘andrea’, ‘barcelona’, y ‘realmadrid’ entre las primeras 25 posiciones.

1. 123456	18. 666666	35. carlos
2. 123456789	19. 12345678910	36. gemeliers
3. swing	20. alejandro	37. gratis
4. 12345	21. cristina	38. qwertyuiop
5. 12345678	22. realmadrid	39. daniel
6. 1234	23. holahola	40. 987654321
7. 1234567890	24. tuputamadre	41. princesa
8. 000000	25. patata	42. 654321
9. password	26. estrella	43. maria
10. 1234567	27. thiscrush	44. mariposa
11. 111111	28. carmen	45. alejandra
12. hola	29. AlLom!	46. daniela
13. barcelona	30. pampling	47. marina
14. qwerty	31. natalia	48. chocolate
15. tequiero	32. 123	49. carolina
16. 123123	33. claudia	50. mierda
17. andrea	34. temporal1	

Top50 de contraseñas más comunes en 2022 en España

Se recomienda evitar el uso de este tipo de contraseñas y seguir una serie de directrices a la hora de **establecer credenciales seguras** para los servicios *online* utilizados. Algunas de estas recomendaciones son:

- **Combinar caracteres de distinto tipo: mayúsculas, minúsculas, números y símbolos.**
- Usar **una longitud adecuada** para evitar que pueda obtenerse a través de ataques de fuerza bruta (al menos 12 caracteres).
- **Evitar palabras que aparezcan en el diccionario** (de cualquier idioma), **nombres propios, de mascotas, fechas, lugares, o datos de carácter personal**, etc. y combinaciones de ellas, como por ejemplo nombre + fecha de nacimiento.
- **Evitar patrones de caracteres sucesivos en el teclado**, como por ejemplo 'qwertyuiop' o '1qaz2wsx'.

Existen otras técnicas de generación de contraseñas robustas, como por ejemplo combinar varias palabras sin relación entre ellas y usar una regla nemotécnica para recordar la cadena obtenida. Por ejemplo con las palabras 'mochuelo', 'abrigo', 'violeta', 'pradera' y 'noche' se generaría la contraseña 'mochueloabrigovioletapraderanoche' con una longitud adecuada para evitar los

ataques por fuerza bruta y tan fácil de recordar como imaginar a un mochuelo con un abrigo violeta en una pradera por la noche.

Por supuesto también es importante **evitar la reutilización de la misma contraseña en diferentes servicios** y, sobre todo, **no apuntarlas en notas o *post-its* y pegarlos al escritorio o debajo del teclado**. Esto hace que una contraseña, por muy segura que sea, pierda todo su sentido.

También se recomienda el uso de **gestores de contraseñas** con los que se puede generar contraseñas seguras de forma sencilla y almacenarlas en local en un dispositivo independiente (por ejemplo un *pendrive* o memoria USB).

Más información:

- <https://nordpass.com/es/most-common-passwords-list/>