En serio, ¿no somos capaces de crear mejores contraseñas?

NordPass, una de las principales soluciones comerciales de administración de contraseñas, ha publicado la séptima edición de su estudio anual sobre las 200 contraseñas más usadas, y **los resultados son, cuanto menos, vergonzantes**. Este listado lo confeccionan investigadores independientes especializados en el análisis de incidentes de ciberseguridad que producen violaciones de datos, sumando la información pública de las expuestas entre septiembre de 2024 y septiembre de 2025 y los repositorios de la Dark Web donde se venden por paquetes que incluyen miles de ellas.

El listado, que incluye datos pormenorizados de 44 países y a nivel mundial, confirma que la tecnología mundial tiene un gran problema y que **conviene acelerar el despliegue de métodos alternativos**, más seguros e intuitivos, que tienen que llegar de los sistemas biométricos como las claves de acceso.

Contraseñas más usadas en 2025

La historia se repite año a año para mal. A nivel mundial, «123456» es la contraseña más común, seguida de «admin» en segundo lugar y «12345678» en el tercero, otra secuencia de números básica. Estos patrones débiles, que van desde «12345» hasta «1234567890», junto a otras claves simples que se usan bastante, como «qwerty123», dominan el top 20 en muchos países.

La investigación muestra que la exposición a la tecnología de los nativos digitales, aquellos que crecieron en el mundo en línea, no se traduce automáticamente en un mejor entendimiento de las prácticas básicas de seguridad de las contraseñas, ni de los riesgos asociados. Curiosamente, los malos hábitos de creación de contraseñas se extienden por igual entre generaciones, mayores o las generaciones X y Z.

En general, a pesar de todos los esfuerzos educativos en ciberseguridad y conciencia digital a través de los años, el incremento del uso de los caracteres especiales es la única nota positiva del listado.

Las más usadas en España

En 2025, «admin» fue la contraseña más utilizada en España, sustituyendo en el primer puesto a «123456», que ahora ocupa el segundo lugar. Sin embargo, distintas variaciones de la palabra

«password» ocupan tres puestos en el top 20 de las claves más usadas en el país. Las combinaciones numéricas están ocho veces en el listado.

1. admin
2. 123456
3. 12345678
4. 123456789
5. 12345
6. password
7. 1234567890
8. 111111
9. Nacho2006
10. Talocha1
11. 13090123
12. 1234ivan
13. 1234567
14. vivela10
15. Contraseña
16. iphone77
17. Password
18. vodafone
19. 12345678aA
20. javier55

El resumen es claro: **somos un chollo para los ciberdelincuentes** que ni siquiera tienen que emplear métodos avanzados de pirateo, ya que la mayoría de las contraseñas usadas son tan débiles que -mediante un solo comando- cualquiera puede descifrarla en un tiempo mínimo. Más del 70% de las filtradas puede descifrarse en menos de un segundo y la mayoría de las restantes tampoco suponen un reto, ya que los ataques automatizados de fuerza bruta o de relleno de credenciales logran infiltrarse y acceder a la información confidencial de los usuarios.

Cómo crear contraseñas fuertes

Es urgente la implementación de funciones más avanzadas (seguras y amigables) que nos libren de las contraseñas y todo apunta a que las claves de acceso (códigos únicos vinculados a dispositivos específicos, como computadoras, tabletas o teléfonos inteligentes) son el método de elección. Y en general, todo lo que llegue de la biometría.

Hasta que eso suceda y teniendo en cuenta que las contraseñas siguen siendo el método de autenticación preferente para

loguearse ante sistemas operativos, aplicaciones, juegos o acceder a los servicios de Internet en todo tipo de máquinas, debemos hacer un esfuerzo en su creación y mantenimiento. Una vez más, te dejamos las **recomendaciones generales para crearlas**:

- Combina mayúsculas con minúsculas y también números con letras.
- Añade caracteres especiales.
- Alarga la contraseña con el mayor número de dígitos.
- Nunca uses palabras típicas o números comunes.
- Nunca uses nombres personales, de mascotas o fechas de nacimiento.
- No utilices la misma contraseña en todos los sitios.
- Usa contraseñas específicas y lo más fuertes posibles para banca y sitios de compra on-line donde exponemos tarjetas de crédito u otro tipo de información financiera.
- Mantén la contraseña a salvo de cualquier tercero.
- No reveles nunca la contraseña a nadie. Tampoco en supuestas peticiones oficiales que suelen ser ataques de phishing.
- Refuerza el uso de las contraseñas siempre que estén disponibles funciones como la doble autenticación (2FA) o sistemas biométricos, sensores de huellas o reconocimiento facial.
- Limpia las cuentas en línea que no uses como tarea regular de mantenimiento.
- Comprueba si tus contraseñas están hackeadas. Have I Been Pwned es un buen lugar donde mirar y también en los gestores de navegadores.

Gestores de contraseñas, muy útiles

Es casi imposible para un humano internauta manejar con seguridad las credenciales para acceder a las centenares de cuentas que seguramente estemos suscritos. Hay un grupo de aplicaciones que son de gran ayuda. Básicamente, este tipo de software **reduce los errores humanos en el manejo de las contraseñas**, ya que automatiza el proceso de generación y de acceso a los sitios web y servicios.

Por supuesto, las contraseñas creadas por estos gestores son altamente seguras cumpliendo las normas estándar en tamaño y complejidad. También ayudan contra los ataques de phishing al identificar de forma inmediata los caracteres procedentes de

otros alfabetos y añaden una enorme ventaja: **solo necesitamos recordar una contraseña maestra y el gestor hará el resto**.

Seguro que te suenan aplicaciones como NordPass, LastPass y otras comerciales y/o de pago, pero desde nuestra sección de prácticos te propusimos en su día estas cinco soluciones de código abierto y **totalmente gratuitas** que gustó mucho a nuestros usuarios. La gran ventaja de los administradores de código abierto es la posibilidad de auditar el software y mantener las credenciales bajo tu control, instalando y auto hospedándolas en nuestra propia máquina. Te recordamos las tres que más nos gustan:

– KeePass. Es el 'abuelo' entre los gestores de contraseñas de código abierto y existe desde los días de Windows XP. KeePass almacena las contraseñas en una base de datos cifrada a la que puedes acceder mediante una contraseña o clave digital. Puede importar y exportar contraseñas en una amplia variedad de formatos.

– Bitwarden. Especialmente destinada a usuarios de LastPass que buscan una alternativa más transparente, funciona como un servicio web al que puedes acceder desde cualquier navegador de escritorio, mientras que para Android e iOS cuenta con sus respectivas apps móviles. Bitwarden puede compartir contraseñas y tiene acceso seguro con autenticación multifactor y registros de auditoría.

– Passbolt. Un administrador de contraseñas autohospedado diseñado específicamente para equipos de trabajo. Se integra con herramientas de colaboración en línea como navegadores, correo electrónico o clientes de chat. Puedes autohospedar el programa en tus propios servidores para mantener un control completo de los datos, aunque equipos sin experiencia o infraestructura pueden usar una versión en nube que los aloja en los servidores de la compañía.

Navegadores web. Si no quieres usar gestores de terceros, otra opción es usar los administradores de contraseñas de los propios navegadores. Chrome, Edge, Firefox… Todos los navegadores han ido mejorando sus gestores para incluir las funciones que ofrecen los especializados de arriba, como la detección de contraseñas vulneradas, el aviso cuando crees alguna débil o una edición de la misma muy sencilla en el propio gestor. No hay excusa. Ponte a la tarea. Solo tardarás unos minutos en mejorar la seguridad de tu vida digital.

Muy Computer