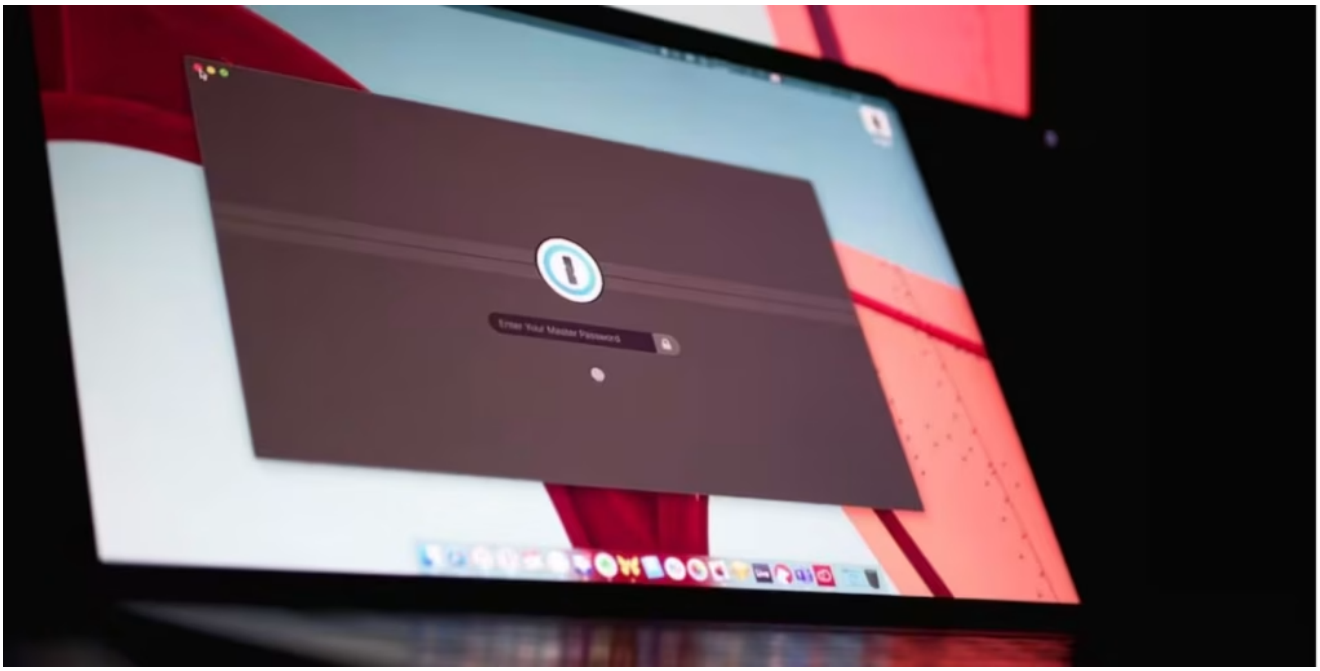
El motivo por el que jamás hay que usar contraseñas generadas por ChatGPT

05/03/2026



Usar una IA para crear claves parece cómodo y moderno, pero especialistas en ciberseguridad alertan que **no es una solución segura**. Muchos usuarios en **Argentina** y el mundo piden a herramientas conversacionales que inventen sus contraseñas creyendo que están protegidos; sin embargo, las claves generadas por modelos como **ChatGPT** presentan fallas estructurales que facilitan los ataques automatizados.

El motivo por el que jamás hay que usar contraseñas generadas por IA

El problema central es que los modelos de lenguaje **no generan aleatoriedad verdadera**. A diferencia de los sistemas diseñados específicamente para la seguridad, las IA responden según patrones estadísticos aprendidos durante su entrenamiento.

Esto significa que tienden a repetir estructuras predecibles, combinando palabras familiares, números y signos de una manera que el ojo humano ve como “compleja”, pero que para un algoritmo de ataque es totalmente descifrable.

Empresas de seguridad como **Kaspersky** han advertido que estos modelos suelen recurrir a fórmulas simples, como la clásica secuencia de **“Palabra + Número + Símbolo”**. Esta es una pauta que ya está integrada en herramientas ofensivas de cracking como *Hashcat* o *John the Ripper*, las cuales pueden adaptar sus diccionarios para explotar estos esquemas y reducir drásticamente el tiempo necesario para adivinar la clave.

Además, existe un riesgo de **concentración**: si dos personas piden criterios idénticos (misma longitud y tipo de caracteres), es muy probable que la IA entregue resultados similares, facilitando enormemente el trabajo de un atacante.

Qué herramientas usar para una seguridad real

Para proteger tus cuentas de forma robusta, lo ideal es alejarse de los “atajos” conversacionales y optar por herramientas diseñadas con fines criptográficos:

- **Gestores de contraseñas:** Aplicaciones como **Bitwarden** o **1Password** emplean generadores basados en sistemas de números aleatorios criptográficamente seguros (**CSPRNG**). Estos garantizan una entropía real, entregando claves que no siguen patrones lingüísticos ni lógicos.
- **Verificación en dos pasos (2FA):** No dependas solo de la contraseña. Activar la autenticación mediante aplicaciones (como Google Authenticator) o llaves de hardware multiplica la dificultad para cualquier intruso.

- **Claves de hardware:** Si manejás información muy sensible, las llaves físicas (estilo YubiKey) son hoy el estándar de oro en protección digital.

Fuente: La 100