**¿Qué pasaría si redujéramos las intersecciones donde se utilizan contraseñas?**

*La seguridad digital necesita menos memoria y más empatía.*

**Ciudad de México, abril de 2025.** En un entorno donde el trabajo híbrido y remoto es la norma, la seguridad empresarial se apoya, muchas veces sin cuestionarse, en un gesto cotidiano: ingresar una contraseña. Esta rutina representa la primera línea de defensa contra amenazas cibernéticas. Sin embargo, **ManageEngine**, la división de gestión de TI empresarial de Zoho Corporation, advierte que este sistema está fallando no por falta de herramientas, sino porque **no toma en cuenta cómo piensan y actúan las personas**.

## **Comportamiento huamno: el talón de Aquiles de la seguridad empresarial**

La mayoría de las organizaciones siguen confiando en políticas rígidas y entrenamientos repetitivos para fomentar el “buen uso” de contraseñas, sin comprender que el problema va más allá del conocimiento: se trata de **sesgos cognitivos profundamente arraigados**. Los trabajadores no eligen contraseñas inseguras por negligencia, sino porque buscan soluciones prácticas para mantenerse productivos.

Entre los principales sesgos identificados:

* **Racionalidad limitada**: Las personas toman decisiones “suficientemente buenas”, no necesariamente las más seguras.
* **Heurística de disponibilidad**: Se prefiere lo que es fácil de recordar, aunque no sea seguro.
* **Aversión a la pérdida**: El miedo a perder acceso inmediato supera el temor a una posible vulneración.

Estos patrones no se corrigen fácilmente con capacitación, porque responden a la naturaleza humana. Por eso, **ManageEngine propone un nuevo enfoque**.

**Eliminar la carga cognitiva: seguridad sin contraseñas**

La solución no está en exigir decisiones perfectas, sino en **diseñar sistemas que eliminen las decisiones vulnerables**. Esto se logra con tecnologías como:

* **Passkeys**: Credenciales cifradas y sincronizadas entre dispositivos.
* **Inicio de sesión único (SSO)**: Acceso unificado a múltiples plataformas.
* **Bóvedas seguras con passkeys**: Eliminan por completo la necesidad de recordar contraseñas.

Estas herramientas reducen errores y liberan a los empleados del desgaste que implica gestionar múltiples accesos.

## **Accesos privilegiados seguros con IA**

La protección también debe extenderse a quienes administran sistemas críticos. ManageEngine impulsa el uso de **gestión de accesos privilegiados (PAM)** con automatización e inteligencia artificial, para evitar accesos innecesarios o mal asignados.

La **IA analiza riesgos en tiempo real y sugiere políticas dinámicas**, corrigiendo errores humanos antes de que se conviertan en vulnerabilidades.

## **Una solución pensada para personas**

Como en el mito de Sísifo, muchas políticas de seguridad parecen castigar al usuario con tareas repetitivas y frustrantes. N**o se trata de añadir más complejidad, sino de repensar el sistema desde la empatía y el diseño centrado en las personas**.

La propuesta es clara: **pasar de la exigencia al entendimiento**, de la capacitación a la automatización, y del hábito al diseño inteligente.