LITORALPRESS

Fecha: 01-06-2026
Medio: Crónica de Chillán
Supl. : Crónica de Chillán
Tipo: Columnas de Opinión
Título: **Columnas de Opinión: El eslabón más débil de la seguridad digital**

Pág. : 4
Cm2: 195,6
VPE: $ 162.318

Tiraje: 2.400
Lectoría: 7.200
Favorabilidad: No Definida

Columna

El eslabón más débil de la seguridad digital

Por Edgardo Fuentes Cáceres.
Director Ingeniería en Ciberseguridad, UNAB

Hoy vivimos conectados de forma permanente. Revisamos el correo desde el teléfono, ingresamos a plataformas de trabajo desde el computador y realizamos trámites bancarios desde cualquier lugar. En todos esos espacios, la contraseña sigue siendo la llave principal de acceso a nuestra información. A pesar de su relevancia, su uso sigue estando marcado por malas prácticas: contraseñas cortas, repetidas o basadas en datos personales fáciles de adivinar. Esta fragilidad convierte a la contraseña en uno de los eslabones más débiles de la seguridad digital.

Frente a este escenario, los gestores de contraseñas se han transformado en una herramienta fundamental. Un gestor de contraseñas es un software diseñado para guardar de forma segura todas las claves del usuario dentro de una bóveda cifrada. Estos gestores pueden instalarse como aplicaciones en computadores, teléfonos móviles o tablets, y también funcionan como extensiones dentro de los navegadores web más comunes. En la práctica, el usuario interactúa con el gestor de n[illegible]tidiana, muchas veces sin notarlo, ya que este se integra de forma natural en los procesos de inicio de sesión.

Su funcionamiento es relativamente simple desde el punto de vista del usuario. Al crear una cuenta nueva en un sitio web, el gestor ofrece generar automáticamente una contraseña segura, larga y aleatoria. Esa clave se guarda en la bóveda cifrada y, a partir de ese momento, cada vez que el usuario visite el sitio, el gestor detectará el formulario de inicio de sesión y completará los datos de manera automática. Todo esto ocurre sin que la persona tenga que recordar la contraseña ni escribirla manualmente.

Uno de los aspectos más relevantes es que estos gestores funcionan tanto en aplicaciones móviles como en equipos de escritorio. En los teléfonos, suelen integrarse con el sistema operativo, permitiendo completar contraseñas en aplicaciones, navegadores e incluso redes Wi Fi. En los computadores, se complementan con extensiones de navegador que reconocen los sitios web y facilitan el acceso con solo uno o dos clics. Además, muchos gestores sincronizan la información entre dispositivos, lo que permite acceder a las contraseñas desde cualquier lugar manteniendo el mismo nivel de seguridad.

Desde el punto de vista técnico, los gestores utilizan cifrado fuerte para proteger la información almacenada. Esto significa que ni siquiera el proveedor del servicio puede ver las contraseñas del usuario. La seguridad se concentra en una contraseña maestra, que es la única que debe memorizarse y que nunca debería compartirse. En algunos casos, esta protección se refuerza con autenticación de dos factores, añadiendo una capa adicional frente a accesos no autorizados.

El principal valor de los gestores no es solo la comodidad, sino el cambio de hábito que promueven. Permiten que cada servicio tenga una contraseña distinta, eliminando el riesgo de que una filtración comprometa múltiples cuentas. También ayudan a detectar contraseñas débiles o repetidas y, en algunos casos, alertan cuando una clave ha aparecido en filtraciones conocidas. Así, el gestor no solo guarda contraseñas, sino que educa indirectamente al usuario en buenas prácticas de seguridad.