Windows 11: de bloquear actualizaciones a bloquear PCs

Windows 11 prometía convertir las actualizaciones en un proceso casi invisible: más seguridad, más estabilidad y menos complicaciones para el usuario. La realidad, sin embargo, lleva bastante tiempo siguiendo un camino muy distinto. Hace apenas unos días Microsoft reconocía que la actualización acumulativa de junio de 2026 podía fallar al instalarse en algunos equipos, bloqueando incluso la recepción de futuros parches. Ya parecía un problema bastante serio. Pero ahora empieza a dibujarse un escenario todavía más incómodo: algunos usuarios que sí consiguieron instalarla están descubriendo que **quizá el verdadero problema no era no poder actualizar… sino haber actualizado**.

La actualización en cuestión es KB5094126, publicada el pasado 9 de junio como parte del Patch Tuesday de junio para Windows 11 24H2 y 25H2. Sobre el papel, se trataba de un parche importante: correcciones de seguridad, mejoras para Windows Hello, soporte para Bluetooth LE Audio y arreglos relacionados con errores de virtualización que venían afectando tanto a juegos como a máquinas virtuales. El problema es que, apenas unos días después de su despliegue, empiezan a acumularse informes bastante preocupantes sobre **sistemas congelados, bucles de recuperación de BitLocker, errores con OneDrive, problemas de red local e incluso pantallazos azules** en determinados equipos HP.

Entre todos los fallos reportados, probablemente el más preocupante sea el relacionado con BitLocker. Diversos usuarios aseguran que, tras instalar KB5094126, **sus equipos entran automáticamente en modo de recuperación BitLocker al reiniciar, incluso en máquinas donde el cifrado del disco y Device Encryption estaban explícitamente desactivados**. En algunos entornos empresariales el problema resulta especialmente delicado: muchos equipos utilizan cuentas locales sin vinculación a cuenta Microsoft, lo que significa que no existe una copia automática de la clave de recuperación. El resultado puede ser demoledor: si no se dispone de esa clave, **la única solución termina siendo borrar completamente el sistema y reinstalar Windows desde cero**. Dicho de otra forma: una actualización de seguridad puede convertir un PC perfectamente funcional en un equipo completamente inaccesible.

A esto se suman los casos de sistemas que directamente dejan de

funcionar con normalidad tras instalar el parche. Usuarios en los foros de Microsoft reportan **congelaciones completas apenas minutos después del arranque, algunas tan rápidas que ni siquiera dejan margen suficiente para desinstalar la actualización** desde Windows. En ciertos casos ha sido necesario recurrir al entorno de recuperación de Windows (WinRE) para revertir el parche, mientras que otros usuarios aseguran haber terminado reinstalando completamente el sistema operativo **después de que incluso el propio modo recuperación generara nuevos problemas**. Resulta difícil no ver cierta ironía incómoda en todo esto: hace unos días el problema parecía ser no poder instalar la actualización; ahora empieza a parecer que instalarla tampoco garantiza precisamente tranquilidad.

La lista de incidencias no termina ahí. Algunos usuarios empresariales reportan que **OneDrive deja de integrarse correctamente con el Explorador de archivos**, mostrando carpetas vacías al acceder desde el panel lateral. También han aparecido informes sobre **fallos completos de conectividad en red local** —aunque Internet siga funcionando aparentemente con normalidad—, algo especialmente problemático en oficinas y entornos compartidos. Y, para rematar, algunos usuarios aseguran que incluso después de intentar bloquear el parche o pausarlo manualmente, Windows termina reinstalándolo automáticamente durante la noche. En determinados modelos de HP también se han detectado pantallazos azules relacionados con limitaciones de espacio en la partición EFI del sistema.

El problema de fondo, una vez más, es el patrón. Porque cuesta muchísimo seguir viendo este tipo de incidentes como excepciones aisladas. Marzo, abril, mayo y ahora junio: el calendario reciente de Windows 11 parece más **una sucesión de problemas acumulativos** que un ciclo de mantenimiento estable. Errores de instalación, fallos con BitLocker, impresoras rotas, drivers conflictivos, problemas de rendimiento, incidencias de red o sistemas que terminan exigiendo reparaciones manuales forman parte ya de una secuencia demasiado larga como para seguir despacharla como simples accidentes inevitables.

Y aquí aparece probablemente el problema más serio de todos: la confianza. Porque cuando una actualización de seguridad empieza a generar más miedo que tranquilidad, **algo falla profundamente en el proceso**. Actualizar Windows debería ser una tarea aburrida, automática e invisible. Cuando cada Patch Tuesday obliga a revisar foros, buscar errores concretos o incluso

plantearse retrasar la instalación por miedo a romper el PC, Microsoft ya no tiene únicamente un problema técnico. Tiene también un problema de credibilidad. Y lo más preocupante es que muchos usuarios empiezan a asumir estas situaciones como algo normal.

Si me dieran una cana por cada contenido que he escrito relacionado con la tecnología… pues sí, tendría las canas que tengo. Por lo demás, música, fotografía, café, un eReader a reventar y una isla desierta. ¿Te vienes?

Muy Computer