NAVI
CIBERSEGURIDAD PARA TODOS

// ALERTA DE SEGURIDAD · MÉXICO 2026

PATCH TUESDAY · JULIO 2026

El parche más grande de la historia de Microsoft.

El 14 de julio de 2026, Microsoft lanzó su actualización de seguridad mensual más grande registrada: 570 vulnerabilidades corregidas de un solo golpe, casi el triple del récord anterior (alrededor de 300).

01 — LOS NÚMEROS EXACTOS

TOTAL

570 vulnerabilidades

Cifra récord histórica, muy por encima de las 206 de junio 2026 y las 164 de abril 2026.

CRÍTICAS

59 vulnerabilidades

48 permiten ejecución remota de código, 9 son de escalada de privilegios.

ZERO-DAY

3 vulnerabilidades

Fallos conocidos públicamente antes de que existiera el parche oficial.

EXPLOTADAS

2 de esas 3 zero-day

Ya estaban siendo explotadas activamente en ataques reales al momento del parche.

02 — LAS DOS FALLAS QUE YA ESTABAN BAJO ATAQUE

CVE-2026-56155 — Windows Server / Active Directory

Permite a un usuario con privilegios bajos escalar hasta convertirse en administrador del sistema. Afecta directamente la infraestructura de identidad corporativa (AD FS).

Falla en SharePoint Online

Incluida en el catálogo de vulnerabilidades explotadas conocidas de CISA. Compromete sistemas de colaboración corporativa expuestos a internet.

CVE-2026-50661 — BitLocker (zero-day adicional, sin confirmación de explotación activa)

Con acceso físico a una laptop robada o perdida, permite eludir el cifrado principal mediante el Entorno de Recuperación de Windows y acceder a los datos del disco.

03 — POR QUÉ HAY TANTAS DE GOLPE (NO ES QUE WINDOWS EMPEORÓ)

✓ **Microsoft usa ahora IA para auditar código antiguo** — un sistema interno llamado MDASH, con más de un centenar de agentes de IA, encontró en meses lo que ingenieros humanos no habían detectado en años.

✓ **Es un backlog que se destapó de golpe**, no una caída repentina en la calidad del software — la propia Microsoft lo explicó así públicamente.

✓ **Esperen más volumen en los próximos meses**, según Pavan Davuluri (jefe de Windows): a medida que la IA ayuda a encontrar más fallos, habrá más actualizaciones de seguridad por versión.

04 — QUÉ HACER HOY MISMO

✓ **Actualiza Windows ahora**, no esperes al reinicio automático — ve a Configuración → Windows Update → Buscar actualizaciones.

✓ **Reinicia tu equipo** en cuanto termine la descarga — el parche no protege nada hasta que se aplica por completo.

✓ **Si administras un servidor con AD FS o SharePoint**, prioriza esos parches sobre cualquier otro — son los que ya están bajo ataque confirmado.

✓ **Revisa si usas BitLocker en equipos que salen de la oficina** — el fallo de recuperación aplica directamente a laptops perdidas o robadas.

// REGLA DE ORO

570 parches no significa que Windows sea 500 veces menos seguro.
Significa que ahora se encuentran más fallos — y hay que instalarlos ya.

Ignorar este parche por su tamaño es exactamente lo contrario de lo que deberías hacer.