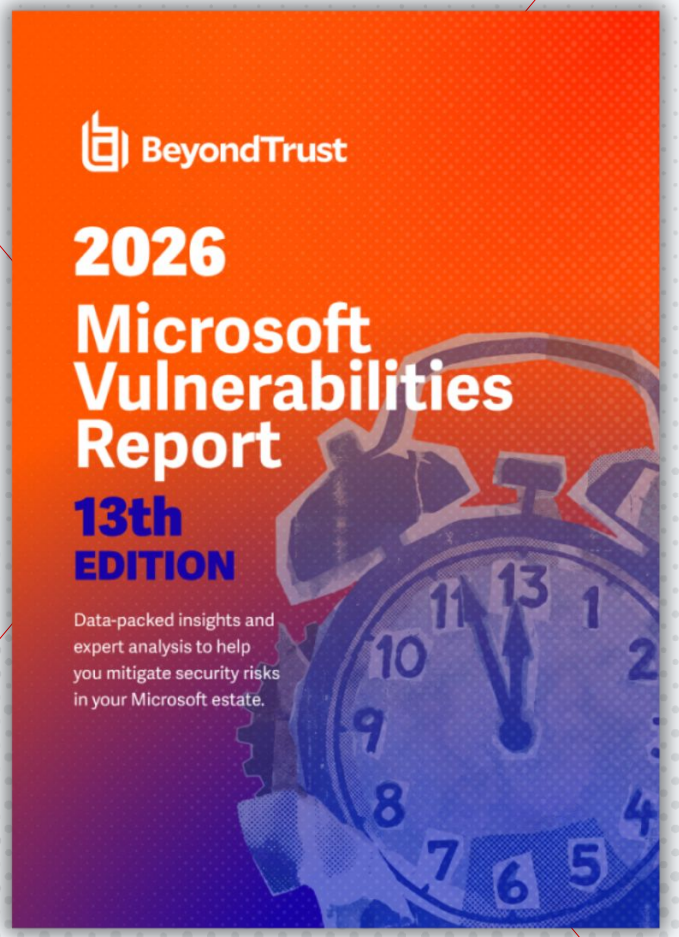
Tendencias de Vulnerabilidades Microsoft: Información Detallada y Análisis de Expertos

Informe BeyondTrust de la Vulnerabilidades Microsoft 2026



Agenda

1. Resumen del Informe Anual de Vulnerabilidades Microsoft
2. Datos destacados, tendencias y hallazgos clave: por categoría y producto
3. Cómo mitigar proactivamente los riesgos de Microsoft con controles de seguridad fundamentales
4. Opiniones de expertos en ciberseguridad
5. Seguridad de identidades centrada en privilegios de BeyondTrust

Informe de Vulnerabilidades Microsoft 2026

- **Analiza los datos de Patch Tuesday** de 2025 (las actualizaciones de seguridad mensuales oficiales de Microsoft para sus productos).
- **Examina qué vulnerabilidades afectan** a qué productos de Microsoft y cómo se pueden mitigar.
- **Ofrece información relevante** sobre el estado pasado, presente y futuro de las iniciativas de seguridad de Microsoft.

Aspectos Destacados y Principales Conclusiones

En 2025, el número de vulnerabilidades críticas de Microsoft se duplicó, pasando de 78 a 157.

40%

Del total de vulnerabilidades se encontraba **Elevación de Privilegio** (509).

9x
Increase in Critical Vulns

Microsoft Azure y Dynamics 365 experimentaron un aumento de nueve veces en las vulnerabilidades críticas.

1,273
Total Vulnerabilities

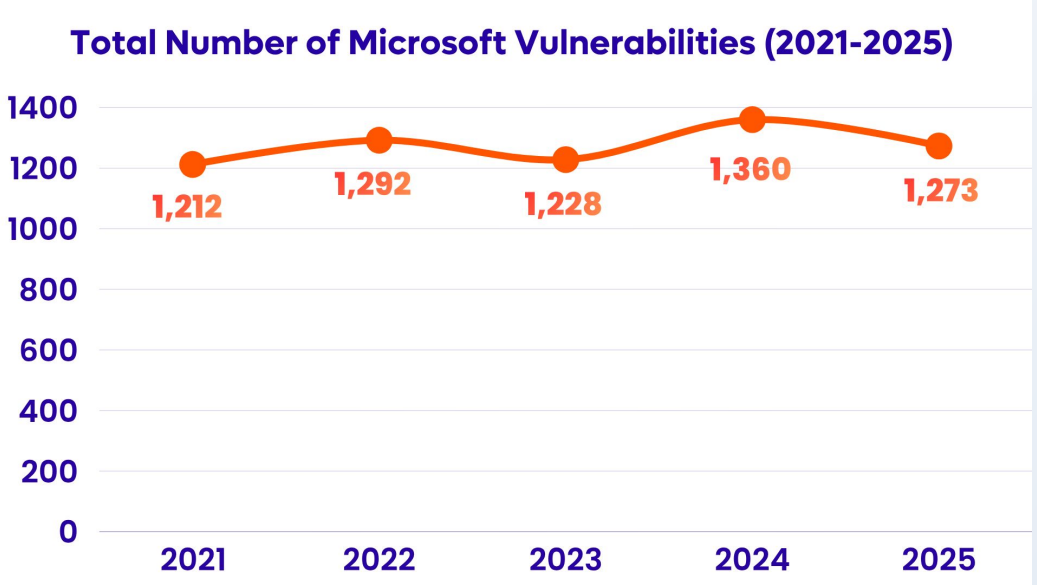
El número total de vulnerabilidades Microsoft **disminuyó un 6 %** (desde 1360).

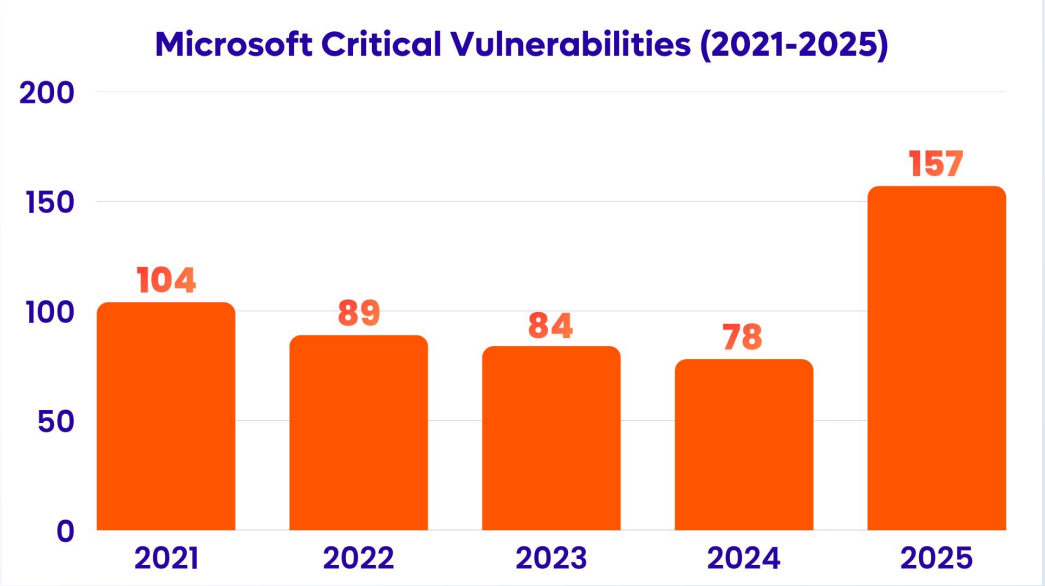
3x
Increase in Total Vulns

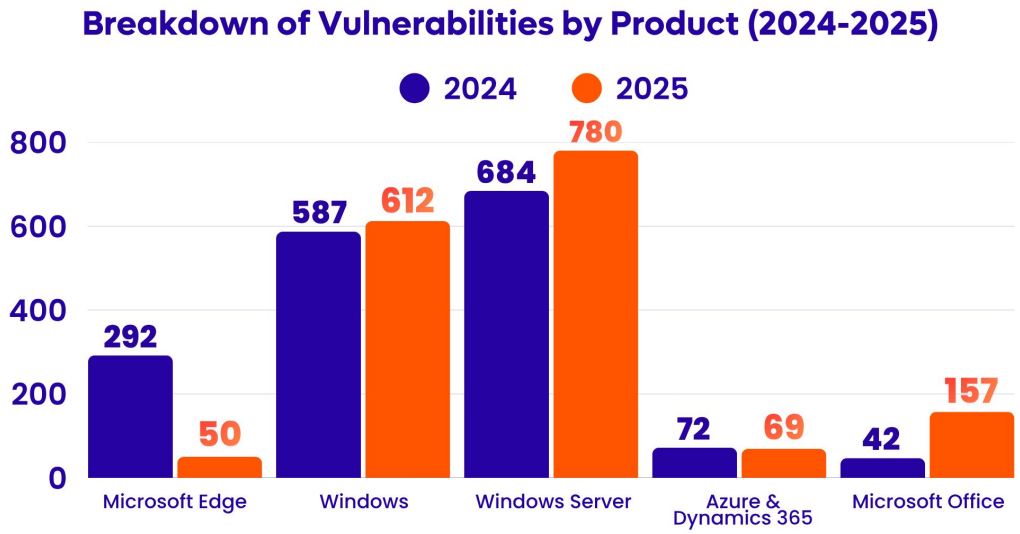
Microsoft Office experimentó un aumento de 3x en las vulnerabilidades totales.

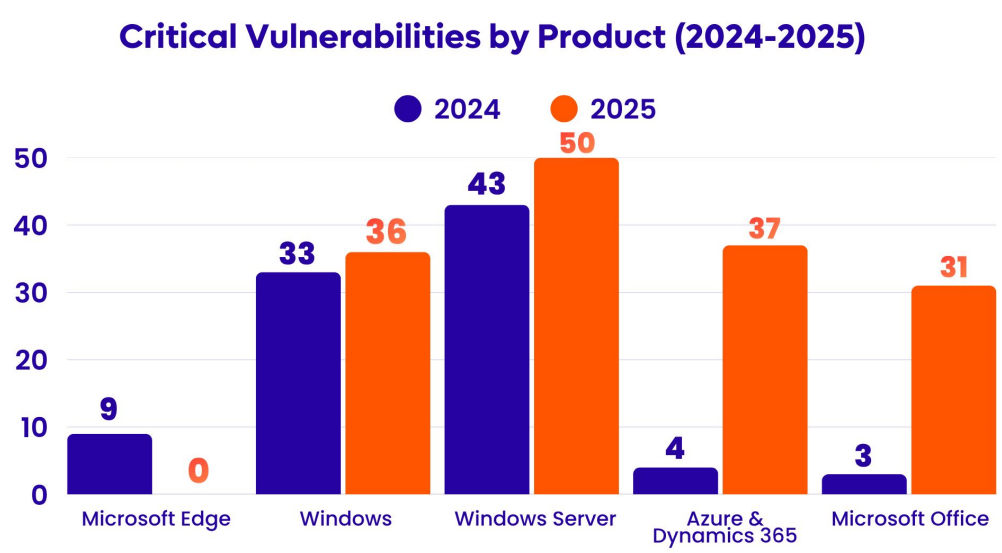
En 2025 se observó un fuerte aumento de las vulnerabilidades críticas.

- **Las vulnerabilidades críticas se** duplicaron con respecto al año anterior, pasando de 78 a 157.
- El total de vulnerabilidades **disminuyó un 6%,** de 1360 a 1273.





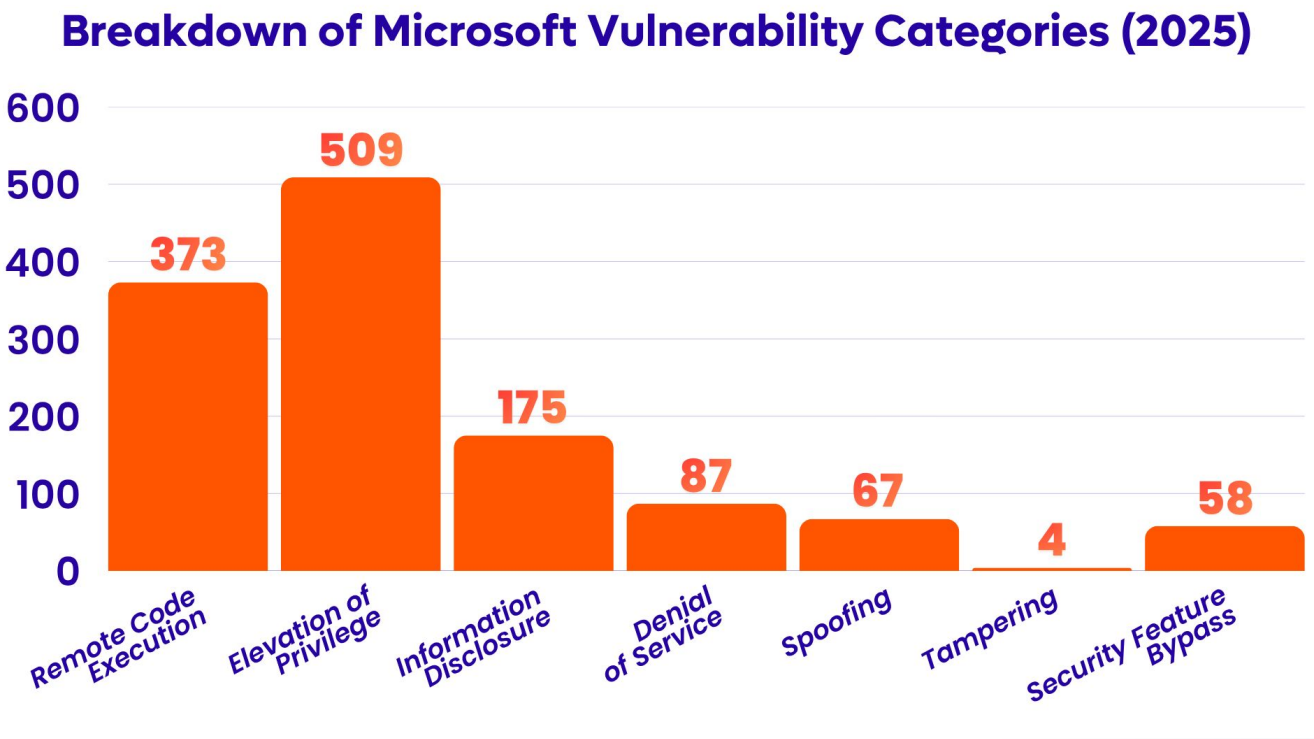




Vulnerabilidades por Producto

- **Microsoft Azure y Dynamics 365** experimentaron un aumento de 9x en las vulnerabilidades críticas, pasando de 4 a 37. El total de vulnerabilidades se estabilizó en 69.
- **Microsoft Office** experimentó 157 vulnerabilidades en 2025, más del triple que en 2024. Las vulnerabilidades críticas aumentaron 10 veces.
- **Microsoft Edge** experimentó 50 vulnerabilidades en total el año pasado, un 83 % menos que el año anterior, sin ninguna vulnerabilidad crítica.
- Se publicaron 612 vulnerabilidades de **Windows** en 2025, 36 de ellas críticas.
- **Windows Server** tuvo 780 vulnerabilidades en 2025, 50 de ellas críticas.

Vulnerabilidades por Categoría



- **La elevación de privilegios** sigue siendo la categoría de vulnerabilidad número uno.
- **La ejecución remota** de código se mantiene en el segundo lugar, pero volvió a los niveles de años anteriores tras un repunte en 2024.
- Además, **la divulgación de información** experimentó un aumento notable, pasando de 101 a 175 casos.

3 Verdades Sobre los Riesgos delas Vulnerabilidades

1. Las vulnerabilidades no existen de forma aislada; se explotan mediante identidades. No todos los riesgos basados en las identidades se identifican con un CVE.

2. Cada vez más, las aplicaciones vulnerables son operadas por identidades no humanas con privilegios (incluidos agentes de IA): el «fantasma en la máquina».

3. Las organizaciones deben combinar los parches con controles que reduzcan el impacto.

“El recuento de CVE siempre ha ofrecido una imagen incompleta. Las configuraciones erróneas de identidades, las cuentas de máquina con privilegios excesivos y los agentes de IA con acceso ilimitado no generan CVE, pero tienen las mismas consecuencias críticas. En cambio, necesitamos conectar los datos con la forma en que realmente ocurren los ataques.”

—Marc Maiffret, CTO de BeyondTrust

Controles Fundamentales para Proteger su Entorno de Microsoft.

1. **Adapte la gestión de vulnerabilidades a su propio entorno.** Aborde los riesgos más acuciantes de su organización, al tiempo que evalúa el impacto en el negocio.
2. **Implemente el principio de mínimo privilegio y el control de confianza cero en toda su infraestructura.** Priorice un enfoque coherente en cada capa de su sistema de identidades y accesos, incluyendo la red, las identidades humanas y no humanas, las cuentas, los endpoints, las aplicaciones, las sesiones, la nube, los entornos locales, etc.
3. **Garantize el acceso remoto seguro.** Asegúrese de que el protocolo RDP no esté expuesto a internet y evite la combinación de VPN y dispositivos personales en el trabajo (BYOD). Además, implemente una autenticación sólida y la monitorización de sesiones para detectar usos indebidos.
4. **Implemente ITDR.** Utilice un enfoque multidisciplinario que integre la visibilidad integral de la seguridad de identidades, la detección de amenazas, la investigación y las capacidades de respuesta.
5. **Prepárese para el futuro.** Reduzca las vulnerabilidades de software e identidad para limitar el riesgo de movimiento lateral y escalada de privilegios, ya que el panorama de amenazas evoluciona rápidamente en la era de la IA.

Que Dicen Los Expertos?

"El verdadero riesgo en los entornos modernos no reside en la presencia de vulnerabilidades, sino en la presencia de privilegios innecesarios... Quienes adoptan el principio del mínimo privilegio como principio fundamental de diseño no eliminarán las vulnerabilidades, pero reducirán drásticamente su capacidad p causar daño."

—Sami Laiho
Senior Technical Fellow at Adminize & Microsoft MVP

"El factor fundamental aquí es la confianza... El modelo Zero Trust es importante porque la defensa moderna ya no se basa en asumir la confianza y luego reaccionar. Se trata de validar continuamente la confianza, limitar los privilegios y gobernar cada identidad (humana y no humana)... Esa es la lección que este informe debería dejar en cada líder de seguridad."

—David (DJ) Morimanno
Field CTO at Xalient

"Los agentes de IA heredan identidad, acceso y privilegios... El aumento repentino de vulnerabilidades críticas en Azure es relevante aquí, ya que esta es la capa de infraestructura donde los servicios de IA residen, se autentican e interactúan con sus datos. Un aumento de casi diez veces en las vulnerabilidades críticas en ese entorno, combinado con identidades de máquinas no controladas que operan de forma autónoma dentro de él, es un riesgo convergente, teórico."

—Jane Frankland, MBE
Founder of the IN Security Movement,
CEO of KnewStart & Best-Selling Author

"La mayoría de las organizaciones no fracasan por técnicas innovadoras, sino porque sus entornos permiten que los ataques tengan éxito. Este es un patrón que se observa sistemáticamente en incidentes reales y que se ve reforzado por el último Informe de Vulnerabilidades Microsoft."

—Paula Januszkiewicz
CEO of CQURE Inc. and CQURE Academy,
Security Expert, Penetration Tester and Trainer,
Microsoft MVP on Security and Microsoft Regional Director

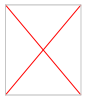
BeyondTrust

Seguridad de Identidades Centrada en Privilegios

- Permite a las organizaciones visualizar, gestionar y proteger los privilegios para reducir los riesgos en todos sus entornos.
- Nuestra plataforma Pathfinder integra todas nuestras soluciones, unificando la visibilidad, la inteligencia y la protección en una única consola.
- Reconocida por los principales analistas del sector como líder en Gestión de Accesos Privilegiados (PAM), Gestión de Derechos de Infraestructura en la Nube (CIEM), Detección y Respuesta ante Amenazas de Identidad (ITDR), Gestión de Secretos y mucho más.

Los clientes confían en BeyondTrust para:

- Obtener visibilidad y comprensión integral de su postura de seguridad de identidades, incluyendo el True Privilege™ de cada identidad: humana, máquina e IA.
- Visualizar los derechos y las Rutas hacia los Privilegios™, incluyendo aquellos que otras soluciones no contemplan.
- Implementar un modelo de privilegio mínimo que elimine los derechos de administrador y el acceso permanente, en consonancia con los principios de Zero Trust.
- Proteger las vías de acceso remoto y la infraestructura garantizando que todo acceso, ya sea humano, máquina, empleado o tercero/proveedor, esté controlado y auditado de forma granular.
- Evitar el secuestro de cuentas y la escalada de privilegios gestionando de forma segura todas las credenciales privilegiadas humanas y de NHI, secretos de DevOps, claves SSH y contraseñas de empleados.
- Gestionar, supervisar y auditar cada sesión privilegiada, por efímera que sea.
- Gestionar y reducir eficazmente toda la superficie de ataque de identidades, abarcando Microsoft, Okta, Ping, Salesforce, GitHub y otros dominios.
- Detectar y neutralizar de forma inteligente los ataques de identidad con rapidez y precisión.
- Cumplir con los rigurosos requisitos de cumplimiento normativo y análisis forense proporcionando informes de fácil acceso sobre toda la actividad privilegiada.
- Acceder a un seguro cibernético cumpliendo con los controles de seguridad clave exigidos por las aseguradoras



Descargue el informe de 2026.