Alerta ID:	101
Fecha del reporte:	15/05/2026
Entidad:	Todas las entidades del ecosistema digital
Título:	Vulnerabilidades en Patch Tuesday de Microsoft – mayo 2026
Herramienta de detección	Análisis de fuentes oficiales (Microsoft, Tenable, etc)
Activo involucrado:	Sistemas operativos Microsoft Windows, plataformas en la nube y servicios de azure, SQL Server, Microsoft Office y herramientas de desarrollo.
Tipo de alerta:	Gestión de vulnerabilidades
Nivel de riesgo:	Alto

Objetivo:

Informar a las entidades del ecosistema digital sobre las vulnerabilidades abordadas en el Patch Tuesday de Microsoft de mayo de 2026, cubriendo un total de 118–137 **vulnerabilidades** en múltiples productos y componentes del ecosistema Windows, Microsoft Office, Azure y servicios en la nube. Este documento busca priorizar la mitigación de vulnerabilidades críticas y de alta severidad para garantizar la continuidad operativa de los servicios de salud y proteger la infraestructura tecnológica frente a vectores de ataque emergentes, enfocándose en resultados a nivel de servicio y resiliencia de la red.

Concientizando sobre los riesgos de explotación, facilitando la identificación de activos y versiones afectadas, promoviendo la aplicación oportuna de parches y medidas de mitigación, y fortaleciendo la capacidad de respuesta ante incidentes de seguridad.

Descripción:

El Martes de Parches (Patch Tuesday) es el ciclo mensual de actualizaciones de seguridad publicado por Microsoft el segundo martes de cada mes. Este mecanismo, establecido desde octubre de 2003, centraliza la distribución de correcciones de seguridad, actualizaciones críticas y mejoras funcionales para todo el ecosistema de productos Microsoft, incluyendo Windows, Microsoft Office, SharePoint, Active Directory, .NET, Azure y herramientas de desarrollo.

El ciclo de Patch Tuesday de mayo de 2026, publicado el 12 de mayo de 2026, incluye un conjunto importante de actualizaciones que abordan entre 118 y 137 vulnerabilidades, dependiendo de la fuente consultada. A continuación se presenta un resumen estadístico:

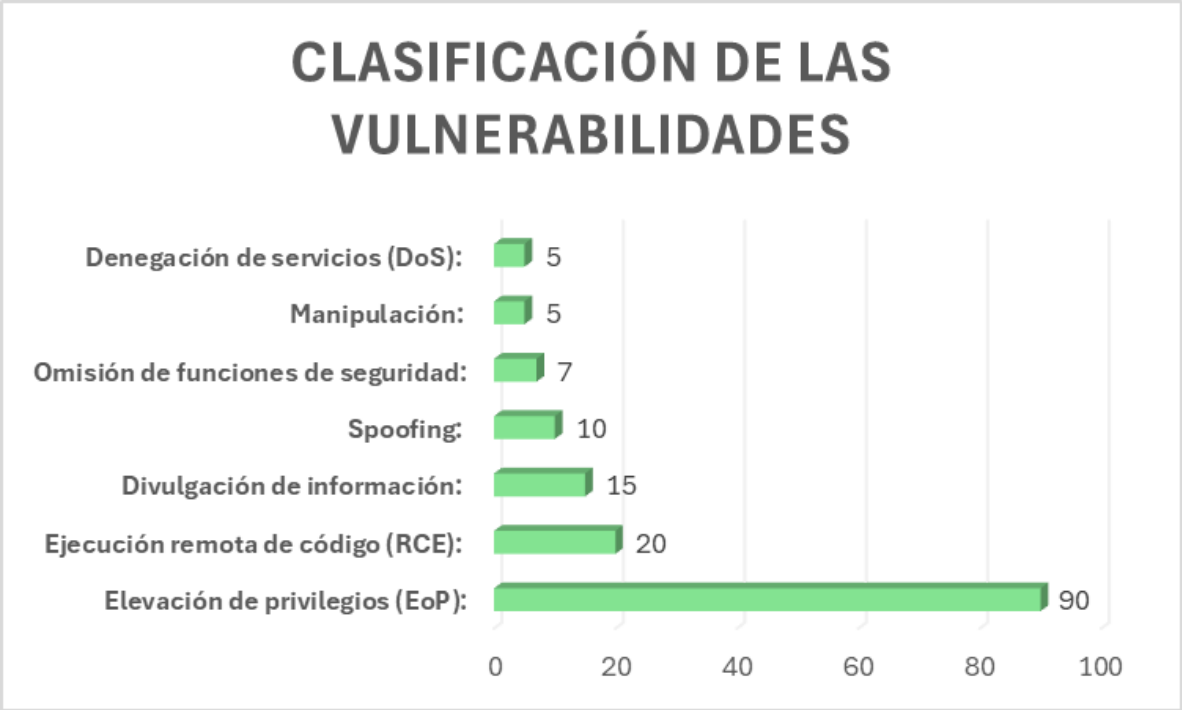
Categoría	Cantidad
Total de vulnerabilidades corregidas	137 CVEs
Vulnerabilidades Críticas	30
Vulnerabilidades Importantes	100
Moderadas / Bajas	15
Día cero explotado activamente	0
Día cero divulgado públicamente	0
RCE Críticas	20
DoS Críticas	5

Las familias de productos afectados incluyen: Windows Boot Loader, Windows Kernel, Windows Active Directory, Windows IKE Extension, Windows TCP/IP, Microsoft Office (Word, Excel, PowerPoint), Microsoft SharePoint, Remote Desktop Client, .NET Framework, Microsoft Defender, Windows BitLocker, Hyper-V, Azure Logic Apps, SQL Server, Windows Hello, Windows Kerberos, entre otros.

Distribución de Vulnerabilidades

Con respecto al total de las vulnerabilidades reportadas por Microsoft se encuentran categorizadas de la siguiente manera según el tipo:

Manipulación: 5
Omisión de funciones de seguridad: 7
Spoofing: 10
Denegación de servicios (DoS): 5
Ejecución remota de código (RCE): 20
Divulgación de información: 15
Elevación de privilegios (EoP): 90



Vulnerabilidades de Día Cero y Más Importantes

Este ciclo de actualización incluye cinco vulnerabilidades clasificadas como día cero: una explotada activamente en la naturaleza y otra divulgada públicamente antes de la disponibilidad del parche. Adicionalmente, se identificaron ocho vulnerabilidades Críticas de alta relevancia para el sector.

A continuación, se presentan las vulnerabilidades de día zero.

CVE-2026-41089 — Windows Netlogon: Ejecución Remota de Código (Crítica)

Esta vulnerabilidad en Windows Netlogon se produce por un desbordamiento de buffer en la función de autenticación de red, lo que permite a un atacante no autenticado ejecutar código

remoto con privilegios del sistema. Aunque Microsoft no ha reportado explotación activa, la falla es crítica debido a la exposición de servicios Netlogon a la red interna y a VPN.

El riesgo de explotación es elevado: un atacante con acceso a la red corporativa podría ejecutar código arbitrario, instalar malware persistente o comprometer controladores de dominio. La mitigación inmediata mediante la aplicación del parche de mayo 2026 es prioritaria.

CVE-2026-41096 — Windows DNS Client: Ejecución Remota de Código (Crítica)

Esta vulnerabilidad afecta al cliente DNS de Windows y permite la ejecución remota de código mediante respuestas DNS maliciosas. La falla se debe a un manejo incorrecto de la memoria en la resolución de paquetes IPv4/IPv6.

Si se explota, un atacante podría comprometer cualquier endpoint que realice consultas a un servidor DNS controlado por el atacante, ejecutar código arbitrario con permisos del usuario actual y potencialmente moverse lateralmente en la red corporativa. La mitigación requiere la actualización inmediata de los clientes afectados.

CVE-2026-40361 — Microsoft Word: Ejecución Remota de Código (Crítica)

Esta vulnerabilidad permite la ejecución remota de código al procesar documentos maliciosos en Microsoft Word. La falla se produce debido a errores en la gestión de memoria al abrir documentos con objetos especialmente construidos, incluyendo .docx y .rtf.

El exploit podría ser distribuido mediante correo electrónico de phishing o descarga desde sitios comprometidos, permitiendo que un actor de amenaza ejecute código arbitrario en el equipo del usuario, robe información o instale malware persistente. La actualización del parche de mayo 2026 es obligatoria para todas las estaciones de trabajo que utilicen Microsoft Word.

CVE-2026-41090 — Windows Kernel: Elevación de Privilegios (Crítica)

Esta vulnerabilidad en el kernel de Windows permite a un usuario con privilegios limitados escalar sus permisos hasta nivel SYSTEM mediante la manipulación de handles de proceso y objetos del kernel mal gestionados.

Aunque no se reporta explotación activa, cualquier usuario local autenticado podría aprovechar esta falla para obtener control total del sistema, desactivar controles de seguridad y ejecutar cargas maliciosas. La aplicación del parche de mayo 2026 es crucial para entornos con múltiples usuarios y servidores compartidos.

CVE-2026-41103 — Windows Server: Divulgación de Información (Crítica)

Esta vulnerabilidad permite la divulgación de información sensible a través de servicios de red en Windows Server. La falla se debe a la exposición de memoria interna en respuestas de red, lo que puede permitir que un atacante obtenga datos confidenciales de configuración, usuarios y credenciales.

Si se explota, un actor de amenaza podría recolectar información que facilite ataques posteriores, incluyendo escalada de privilegios y movimientos laterales en la red. La mitigación requiere la aplicación inmediata de los parches correspondientes.

Consecuencias de la Explotación

La explotación exitosa de las vulnerabilidades descritas en este boletín puede generar consecuencias de alto impacto para las entidades del sector salud, incluyendo:

Ejecución Remota de Código en Windows Netlogon (CVE-2026-41089)

- Compromiso total de controladores de dominio y servidores expuestos a la red interna.
- Movimiento lateral dentro de la infraestructura corporativa, incluyendo servidores críticos y endpoints de usuarios.
- Posible despliegue de malware, backdoors o ransomware sobre sistemas vulnerables.

- Interrupción de servicios esenciales, incluyendo autenticación de usuarios y gestión de políticas de seguridad en Active Directory.

Ejecución Remota de Código en Windows DNS Client (CVE-2026-41096)

- Compromiso de endpoints que realizan consultas a servidores DNS controlados por el atacante.
- Exfiltración de información sensible a través de ataques de red.
- Posibilidad de ejecutar código arbitrario en estaciones de trabajo o servidores, afectando disponibilidad e integridad de sistemas.
- Vector para ataques de movimiento lateral hacia sistemas críticos internos.

Ejecución Remota de Código en Microsoft Word (CVE-2026-40361)

- Ejecución de código malicioso al abrir documentos Word manipulados.
- Vector para campañas de spear-phishing dirigidas a personal corporativo o de salud.
- Descarga y ejecución de cargas maliciosas (stealers, loaders, ransomware) en los endpoints afectados.
- Posible compromiso de información confidencial contenida en documentos y archivos corporativos.

Escalada de Privilegios en Windows Kernel (CVE-2026-41090)

- Un atacante con acceso inicial limitado puede obtener control total del sistema operativo.
- Desactivación de controles de seguridad locales, incluyendo antivirus y soluciones EDR.
- Instalación de malware persistente, backdoors, ransomware o herramientas de acceso remoto (RAT).
- Exfiltración de datos sensibles y corporativos de los endpoints comprometidos.

Divulgación de Información en Windows Server (CVE-2026-41103)

- Acceso no autorizado a datos internos de configuración, credenciales y secretos corporativos.
- Posibilidad de facilitar ataques posteriores mediante recopilación de información (reconocimiento interno).
- Riesgo de exposición de información crítica en servidores que soportan aplicaciones de negocio o sistemas de salud.
- Vector para ataques de escalada de privilegios y movimiento lateral en la red.

Modo de Explotación de las vulnerabilidades de day-zero y críticas.

Explotación de CVE-2026-41089 (Windows Netlogon — RCE — Crítica)

- **Reconocimiento:** El atacante identifica controladores de dominio y servidores Netlogon accesibles en la red mediante escaneo activo (nmap, Nessus) o pasivo (Shodan, Censys). Se verifica la versión del servicio y las configuraciones mediante análisis de respuesta de red y logs.
- **Construcción del payload:** Se preparan paquetes de autenticación especialmente diseñados para desbordar buffers en la función de Netlogon, manipulando la memoria del servicio de autenticación.
- **Explotación:** Al enviar los paquetes maliciosos, el servicio Netlogon procesa incorrectamente los datos, permitiendo ejecución remota de código con privilegios de sistema.
- **Post-explotación:** El atacante puede instalar malware, crear cuentas privilegiadas, realizar movimientos laterales dentro de la red y comprometer controladores de dominio.

Explotación de CVE-2026-41096 (Windows DNS Client — RCE — Crítica)

- **Identificación de objetivos:** Hosts Windows que realicen consultas DNS a servidores controlados por el atacante.

- **Construcción del payload:** Se preparan respuestas DNS maliciosas que desencadenan corrupción de memoria en el cliente DNS vulnerable.
- **Ejecución de código:** El cliente procesa la respuesta y ejecuta código arbitrario con los privilegios del usuario actual.
- **Post-explotación:** Permite movimiento lateral, exfiltración de datos y despliegue de cargas maliciosas en endpoints corporativos.

Explotación de CVE-2026-40361 (Microsoft Word — RCE — Crítica)

- **Preparación del documento:** El atacante crea archivos .docx o .rtf con estructuras de memoria diseñadas para causar ejecución de código (heap corruption o punteros no confiables).
- **Entrega:** Se distribuye el documento vía correo electrónico de phishing, mensajería interna o descarga desde sitios web comprometidos.
- **Ejecución:** Al abrir el archivo en una versión vulnerable de Word, WINWORD.EXE procesa la memoria manipulada, ejecutando shellcode del atacante.
- **Post-explotación:** Se instalan cargas maliciosas (dropper/loader, ransomware, stealer), se compromete información confidencial y se posibilita movimiento lateral en la red.

Explotación de CVE-2026-41090 (Windows Kernel — EoP — Crítica)

- **Acceso inicial:** Usuario estándar con acceso local.
- **Explotación:** Se manipulan handles de procesos y objetos del kernel mal gestionados para obtener un token SYSTEM.
- **Post-explotación:** Escalada de privilegios completa, desactivación de controles de seguridad y persistencia de malware con permisos máximos del sistema.

Explotación de CVE-2026-41103 (Windows Server — Divulgación de Información — Crítica)

- **Identificación de objetivos:** Servidores Windows expuestos a la red interna o pública con servicios de red activos.
- **Explotación:** Se envían paquetes maliciosos que permiten al atacante acceder a memoria interna y obtener información sensible.
- **Post-explotación:** Recopilación de datos críticos que pueden facilitar ataques posteriores, escalada de privilegios y movimiento lateral dentro de la red corporativa.

Recursos y versiones afectadas:

- **Sistemas Operativos Windows**

Sistema Operativo	Versiones / Builds Afectadas
Windows 11	Versiones 23H2, 24H2, 25H2 — Builds anteriores al parche de mayo 2026
Windows 10	Versión 22H2 — Builds anteriores al parche de mayo 2026
Windows Server 2025	Todas las versiones RTM y cumulative updates anteriores a mayo 2026
Windows Server 2022	Todas las versiones anteriores al parche de mayo 2026
Windows Server 2019	Todas las versiones anteriores al parche de mayo 2026
Windows Server 2016	Todas las versiones anteriores al parche de mayo 2026

- **Aplicaciones y Servicios Microsoft**

Producto / Componente	Versiones Afectadas
Microsoft Word	Office 2016, 2019, 2021, Microsoft 365 Apps
Microsoft Excel	Office 2016, 2019, 2021, Microsoft 365 Apps

Producto / Componente	Versiones Afectadas
Microsoft SharePoint Server	SharePoint Server Subscription Edition, 2019, 2016
Microsoft Defender (Antivirus)	Versiones de definición y motor anteriores a mayo 2026
Remote Desktop Client	Clientes RDP integrados en Windows 10/11 y Server
Windows Active Directory	AD DS en Windows Server 2016/2019/2022/2025
Windows IKE Extension	Servicio IKEv2 en Windows 10/11 y todas las versiones Server
Windows TCP/IP Stack	. Servicio IKEv2 en Windows 10/11 y todas las versiones Server
.NET Framework	Stack de red con IPv6 habilitado en Windows 10/11 y Server
Hyper-V	3.5, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8, 4.8.1
Azure Monitor Agent / Logic Apps	Todas las versiones anteriores al parche de mayo 2026
SQL Server	Versiones anteriores a las actualizaciones de mayo 2026
SQL Server	SQL Server 2019, 2022 en todas las ediciones
Microsoft Edge (Chromium)	Versiones anteriores al parche de mayo 2026

Vector de impacto:

- **Elevación de Privilegios (EoP)**

Este fue uno de los vectores de impacto más predominantes en el ciclo de mayo 2026, con aproximadamente 70–90 vulnerabilidades. Una vulnerabilidad de elevación de privilegios permite a un atacante con acceso limitado a un sistema obtener permisos mayores, como los de administrador. Este tipo de vulnerabilidad suele utilizarse como un segundo paso tras obtener acceso inicial, permitiendo al atacante tomar control total del sistema afectado y desplegar cargas maliciosas persistentes.

● **Ejecución Remota de Código (RCE)**

Se corrigieron aproximadamente 15–20 vulnerabilidades de este tipo. Las vulnerabilidades de RCE son críticas porque permiten a un atacante ejecutar código arbitrario en un sistema vulnerable a través de la red, sin necesidad de acceso físico. Esto puede llevar al compromiso total del sistema, instalación de malware y movimientos laterales dentro de la red corporativa.

● **Divulgación de Información**

Se abordaron cerca de 10–15 vulnerabilidades de divulgación de información. Estas fallas de seguridad podrían permitir a un atacante acceder a datos sensibles que normalmente estarían protegidos, incluyendo credenciales, configuración de servicios y datos corporativos críticos.

● **Denegación de Servicio (DoS)**

Se solucionaron aproximadamente 3–5 vulnerabilidades de DoS. Un ataque de denegación de servicio tiene como objetivo interrumpir la disponibilidad de sistemas o servicios para los usuarios legítimos, afectando la continuidad operativa de la infraestructura crítica.

● **Omisión de Funciones de Seguridad**

Se corrigieron alrededor de 5–7 vulnerabilidades de este tipo. Estas fallas permiten a un atacante evadir mecanismos de seguridad implementados en el sistema, sin necesidad de romperlos directamente, incrementando la superficie de ataque.

● **Suplantación de Identidad (Spoofing)**

Se corrigieron 8–10 vulnerabilidades de spoofing, que podrían permitir a un atacante hacerse pasar por otra persona o sistema para ganar la confianza de un usuario y realizar acciones maliciosas, como acceso no autorizado o modificación de datos.

● **Manipulación**

Se corrigieron 3–5 vulnerabilidades de manipulación (tampering). El objetivo principal es alterar la integridad de sistemas, logs o datos en tránsito, generalmente para beneficiarse, evadir controles o causar daños en la infraestructura tecnológica.

Recomendaciones de mitigación:

Las siguientes acciones deben ejecutarse de forma transversal a todos los sistemas afectados:

1. Aplicar las actualizaciones de seguridad de mayo 2026 de Microsoft vía Windows Update, WSUS o SCCM/Intune para todos los sistemas Windows del inventario.
2. Priorizar el parcheo de los sistemas y CVEs críticos, incluyendo:
    - Windows Netlogon (CVE-2026-41089)
    - Windows DNS Client (CVE-2026-41096)
    - Microsoft Word (CVE-2026-40361)
    - Windows Kernel (CVE-2026-41090)
    - Windows Server (CVE-2026-41103)
3. Si el parcheo inmediato de las vulnerabilidades críticas de red no es posible, implementar reglas de firewall para restringir tráfico desde fuentes externas no confiables, especialmente en servicios Netlogon y DNS.
4. Actualizar Microsoft Defender y otras soluciones EDR a la versión más reciente para mitigar riesgos de escalada de privilegios locales.

5. Aplicar las actualizaciones de Microsoft Office en todas las estaciones de trabajo de usuarios que manipulen documentos Word o Excel para mitigar riesgos de RCE a través de documentos maliciosos.

6. Revisar configuraciones de IPv6 y servicios de red expuestos, deshabilitando protocolos no requeridos para reducir la superficie de ataque.

Mitigaciones Adicionales y Hardening

- Implementar el Principio de Mínimo Privilegio: asegurar que los usuarios operen con cuentas estándar, sin privilegios de administrador local, limitando el impacto de la explotación de vulnerabilidades críticas.
- Habilitar Protected Users Security Group en Active Directory para reducir riesgo de técnicas de movimiento lateral (Pass-the-Hash, Pass-the-Ticket).
- Configurar filtrado de adjuntos en soluciones de correo electrónico para bloquear archivos .docx, .docm, .rtf y .xlsx de remitentes externos no verificados.
- Activar Protected View y Application Guard en Microsoft Office para aislar la apertura de documentos externos.
- Bloqueo de macros VBA por defecto mediante GPO, siguiendo las directrices de endurecimiento de Microsoft.
- Implementar Network Access Control (NAC) o segmentación de red para limitar acceso al Controlador de Dominio únicamente a hosts autorizados.

- Verificar que las actualizaciones automáticas de Windows Defender estén habilitadas en todos los endpoints.
- Revisar y aplicar el diálogo de advertencia de RDP introducido en la actualización de mayo 2026 para proteger a usuarios de servidores RDP maliciosos.

Fuentes:

- Microsoft Security Response Center (MSRC) — Guía de actualizaciones de mayo 2026: https://msrc.microsoft.com/update-guide
- CISA Known Exploited Vulnerabilities Catalog — CVEs de Microsoft: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- Qualys — Microsoft and Adobe Patch Tuesday, May 2026 Security Update Review https://blog.qualys.com/vulnerabilities-threat-research/2026/05/12/microsoft-patch-tuesday-may-2026-security-update-review
- Tenable — Microsoft's May 2026 Patch Tuesday Addresses 118 CVEs (ejemplo CVE-2026-41103) https://www.tenable.com/blog/microsofts-may-2026-patch-tuesday-addresses-118-cves-cve-2026-41103
- Cisco Talos Intelligence — Microsoft Patch Tuesday for May 2026: Snort Rules and Prominent Vulnerabilities https://blog.talosintelligence.com/microsoft-patch-tuesday-may-2026

- BleepingComputer — Microsoft May 2026 Patch Tuesday fixes 118–137 flaws https://www.bleepingcomputer.com/news/security/microsoft-may-2026-patch-tuesday/
- MITRE ATT&CK Framework v15 — mapeo de técnicas y tácticas asociadas a CVEs de mayo 2026: https://attack.mitre.org
- Windows 11 KB5087591 May 2026 Patch Tuesday Update — Microsoft https://support.microsoft.com/en-us/topic/windows-11-kb5087591-update

En caso de dudas, inquietudes o requerir asistencia adicional relacionada con esta alerta de seguridad, puede comunicarse directamente con el **CSIRT Salud** a través de las líneas telefónicas **(+57) 316 893 1490 - 318 155 3570** o mediante el correo electrónico **csirtsalud@minsalud.gov.co**. Nuestro equipo está disponible para brindar el acompañamiento necesario.