

Alerta ID:	109
Fecha del reporte:	10/06/2026
Entidad:	Todas las entidades del ecosistema digital
Título:	Vulnerabilidades en Patch Tuesday de Microsoft – junio, 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 junio de 2026**, el cual fue publicado el **9 de junio de 2026** y representa el ciclo de parches de seguridad más grande hasta la fecha, con más de **200 vulnerabilidades corregidas** en productos y servicios de Microsoft.

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, con un enfoque en resultados a nivel de servicio y resiliencia de la red. Se incluyen fallas que abarcan Windows, Microsoft Office, Azure, Exchange Server, componentes de red y otros servicios clave.

Se pretende concientizar sobre los riesgos de explotación —incluyendo varios fallos de remote code execution (RCE) y otras vulnerabilidades de alto impacto—, facilitar la



identificación de activos y versiones afectadas, promover la aplicación oportuna de parches y medidas de mitigación, y fortalecer 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 **cada segundo martes del 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 **Patch Tuesday de junio de 2026**, publicado el **9 de junio de 2026**, incluyó un conjunto significativo de actualizaciones que abordan más de **200 vulnerabilidades** en diversos productos y servicios, reforzando la seguridad de sistemas críticos frente a vectores de ataque emergentes:

Categoría	Cantidad
Total, de vulnerabilidades corregidas	200 CVEs
Vulnerabilidades Críticas	15–20
Vulnerabilidades Importantes	160–170
Moderadas / Bajas	10–15
Día cero explotado activamente	0
Día cero divulgado públicamente	0



Categoría	Cantidad
RCE Críticas	12-15
DoS Críticas	3-4

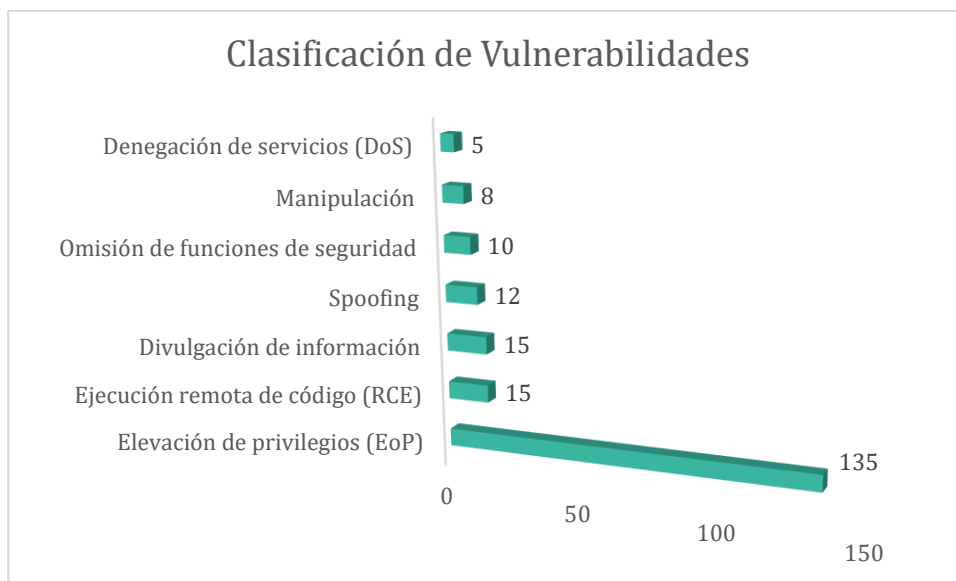
Las familias de productos afectados incluyen: Windows Boot Loader, Windows Kernel, Windows Active Directory, Windows IKE Extension, Windows TCP/IP, Microsoft Office (Word, Excel, PowerPoint), Microsoft SharePoint, Remote Desktop Client, .NET Framework, Microsoft Defender, Windows BitLocker, Hyper-V, 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: 8
- ❖ Omisión de funciones de seguridad: 10
- ❖ Spoofing: 12
- ❖ Denegación de servicios (DoS): 5
- ❖ Ejecución remota de código (RCE): 15
- ❖ Divulgación de información: 15
- ❖ Elevación de privilegios (EoP): 135





Vulnerabilidades de Día Cero y Más Importantes

Este ciclo de actualización incluye dos 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.

Vulnerabilidades de Día Cero y Más Importantes

El Patch Tuesday de junio de 2026 incluye vulnerabilidades críticas y clasificadas como Día Cero, que afectan a productos clave del ecosistema Microsoft. Estas vulnerabilidades requieren atención prioritaria para proteger la integridad, confidencialidad y disponibilidad de los sistemas de información.

Resumen de vulnerabilidades destacadas



- Se identificaron vulnerabilidades de suplantación y elevación de privilegios en productos como Microsoft SharePoint Server y Microsoft Defender.
- Estas fallas podrían permitir que un atacante con acceso inicial limitado intente escalar privilegios o comprometer información sensible si no se aplican los parches correspondientes.
- La inclusión en catálogos de vulnerabilidades conocidas y explotadas (CISA KEV) indica que estas vulnerabilidades son relevantes y que su mitigación inmediata es prioritaria para reducir riesgos de seguridad en entornos críticos.

Recomendaciones generales de mitigación

1. Aplicar de inmediato los parches de seguridad publicados por Microsoft en todos los sistemas afectados.
2. Priorizar la actualización de productos críticos, incluyendo Windows, SharePoint, Defender, Azure y Microsoft Office.
3. Revisar y reforzar controles de acceso y autenticación para limitar la explotación de posibles vulnerabilidades.
4. Monitorear actividad sospechosa y mantener alertas sobre intentos de escalamiento de privilegios o acceso no autorizado.
5. Actualizar inventario de activos y versiones afectadas para asegurar que todos los sistemas vulnerables sean mitigados.

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:



La explotación exitosa de vulnerabilidades críticas identificadas en el Patch Tuesday de junio de 2026 puede generar impactos significativos en entidades del sector salud y otros entornos críticos. Los posibles efectos incluyen:

Compromiso de Confidencialidad e Integridad

- Acceso no autorizado a documentos corporativos, datos confidenciales y comunicaciones internas.
- Modificación de información crítica, incluyendo registros administrativos o regulatorios.
- Posible uso de sistemas comprometidos como puntos de pivote para ataques internos y campañas de phishing dirigidas.

Escalada de Privilegios

- Un atacante con acceso limitado podría obtener control elevado del sistema operativo.
- Desactivación de controles de seguridad locales y soluciones EDR, incluyendo herramientas como Microsoft Defender.
- Instalación de malware persistente, backdoors o herramientas de acceso remoto (RAT).
- Exfiltración de datos corporativos sensibles y activos críticos.

Ejecución Remota de Código

- Compromiso total de sistemas expuestos a la red.
- Movimiento lateral dentro de la infraestructura corporativa hacia servidores críticos y endpoints estratégicos.
- Posible despliegue de ransomware o malware dirigido a infraestructura estratégica.
- Interrupción de servicios esenciales para la operación de la organización.

Compromiso de Directorios y Controladores

- Posible ejecución de código con privilegios de servicios críticos.
- Riesgo de toma de control de controladores de dominio (Domain Controller takeover).
- Persistencia avanzada mediante creación de cuentas privilegiadas o modificación de políticas de seguridad.
- Acceso a todos los sistemas autenticados por el dominio, incluyendo aplicaciones críticas y servicios internos.



Explotación a través de Documentos Corporativos

- Ejecución de código malicioso al abrir archivos Office manipulados (Word, Excel, PowerPoint).
- Vector común para campañas de spear-phishing dirigidas a personal corporativo o administrativo.
- Descarga y ejecución de cargas maliciosas en los endpoints del usuario.

Recomendación general:

Se enfatiza la aplicación inmediata de parches, la revisión de controles de acceso y la monitorización de actividad anómala para reducir riesgos de explotación y proteger la integridad de la información y continuidad de los servicios.

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

El Patch Tuesday de junio de 2026 incluye vulnerabilidades críticas y de Día Cero que pueden ser explotadas de diversas formas, afectando servicios de SharePoint, Microsoft Defender, Windows IKE/TCP-IP, Active Directory y Microsoft Office. A continuación se describe de forma generalizada cómo podrían ocurrir los ataques y las medidas de mitigación recomendadas:

Microsoft SharePoint Server — Suplantación (Spoofing)

- Riesgo: Un atacante podría intentar explotar fallas de validación de entradas para acceder o modificar información sensible y realizar suplantación de usuarios.
- Impacto potencial: Acceso no autorizado a documentos corporativos, modificaciones en permisos y exposición de información confidencial.
- Medidas de mitigación:



- Aplicar parches de seguridad inmediatamente.
- Revisar configuraciones de acceso y permisos en SharePoint.
- Monitorear actividad sospechosa y registros de auditoría.

Microsoft Defender — Elevación de Privilegios (EoP)

- Riesgo: Explotación de fallas de control de acceso insuficiente podría permitir a un atacante con privilegios bajos obtener permisos elevados.
- Impacto potencial: Control total del sistema, desactivación de soluciones de seguridad, instalación de malware o persistencia maliciosa.
- Medidas de mitigación:
 - Actualizar Microsoft Defender y componentes del sistema operativo.
 - Revisar y reforzar políticas de acceso y autenticación.
 - Monitorear actividad de privilegios y procesos sospechosos.

Windows IKE / TCP-IP — Ejecución Remota de Código (RCE)

- Riesgo: Exposición de sistemas con servicios de red vulnerables que podrían permitir ejecución de código remoto.
- Impacto potencial: Compromiso de sistemas críticos expuestos a la red, movimiento lateral, interrupción de servicios.
- Medidas de mitigación:
 - Aplicar parches de seguridad publicados por Microsoft.



- Implementar reglas de firewall para bloquear tráfico sospechoso.
- Revisar logs de red y sistemas para detectar actividad anómala.

Active Directory — Ejecución Remota de Código

- Riesgo: Vulnerabilidades podrían permitir ejecución de código con permisos de servicios críticos.
- Impacto potencial: Creación de cuentas privilegiadas, modificación de políticas de seguridad y compromiso de sistemas autenticados por el dominio.
- Medidas de mitigación:
 - Aplicar actualizaciones de seguridad a controladores de dominio y servidores AD.
 - Revisar políticas de GPO y cuentas privilegiadas.
 - Monitorear autenticaciones y cambios de privilegios.

Microsoft Office — RCE a través de documentos maliciosos

- Riesgo: Archivos manipulados de Word, Excel o PowerPoint podrían comprometer endpoints al abrirse.
- Impacto potencial: Instalación de malware, robo de información y movimiento lateral dentro de la infraestructura corporativa.
- Medidas de mitigación:
 - Mantener Office y componentes actualizados con los últimos parches.
 - Implementar protección contra macros y contenido activo no confiable.
 - Capacitar usuarios para identificar correos y documentos sospechosos



Recursos y versiones afectadas:

A continuación, se presentan los sistemas operativos, aplicaciones y servicios de Microsoft afectados por las vulnerabilidades identificadas en el Patch Tuesday de junio de 2026. Esta información permite a las entidades priorizar la aplicación de parches y medidas de mitigación de forma efectiva

- **Sistemas Operativos Windows**

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



Producto / Componente	Versiones Afectadas
Microsoft Defender (Antivirus)	Versiones de definición y motor anteriores a junio 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	Stack de red con IPv6 habilitado en Windows 10/11 y Server
.NET Framework	3.5, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8, 4.8.1
Hyper-V	Todas las versiones anteriores al parche de junio 2026
Azure Monitor Agent / Logic Apps	Versiones anteriores a las actualizaciones de junio 2026
SQL Server	2019, 2022
Microsoft Edge (Chromium)	Versiones anteriores al parche de junio 2026

Vector de Impacto

El ciclo de **Patch Tuesday de junio de 2026** incluye vulnerabilidades clasificadas según el tipo de impacto, permitiendo a las entidades priorizar acciones de mitigación y aplicación de parches. Los vectores de impacto más relevantes son los siguientes:

1. Elevación de Privilegios (EoP)

- Representa uno de los vectores más críticos, con aproximadamente **75–90 vulnerabilidades** de este tipo.
- Permite a un atacante con acceso limitado a un sistema obtener **permisos elevados**, como los de administrador, facilitando la **toma de control completo del sistema afectado**.



- **Mitigación:** Aplicar inmediatamente parches críticos, reforzar políticas de acceso y monitorear cuentas privilegiadas.

2. Ejecución Remota de Código (RCE)

- Se corrigieron aproximadamente **15–20 vulnerabilidades de RCE**.
- Estas vulnerabilidades permiten a un atacante ejecutar **código malicioso de forma remota**, comprometiendo sistemas completos y posibilitando la propagación de malware dentro de la red corporativa.
- **Mitigación:** Actualizar todos los sistemas expuestos y configurar reglas de firewall para tráfico sospechoso.

3. Divulgación de Información

- Cerca de **8–10 vulnerabilidades** permitían el acceso no autorizado a datos sensibles, incluyendo credenciales y configuraciones críticas.
- **Mitigación:** Aplicar los parches, auditar permisos de acceso y reforzar la protección de datos.

4. Denegación de Servicio (DoS)

- Se solucionaron **2–3 vulnerabilidades** que podrían permitir interrumpir la disponibilidad de sistemas o servicios, afectando la continuidad operativa.
- **Mitigación:** Aplicar actualizaciones y revisar medidas de redundancia y tolerancia a fallos.

5. Omisión de Funciones de Seguridad

- Alrededor de **5–7 vulnerabilidades** permitían evadir mecanismos de seguridad sin romperlos directamente, aumentando la superficie de ataque.
- **Mitigación:** Actualizar sistemas y reforzar controles de seguridad internos.

6. Suplantación de Identidad (Spoofing)



- Se corrigieron **6–8 vulnerabilidades** que podrían permitir a un atacante hacerse pasar por otro usuario o sistema, accediendo a información o ejecutando acciones maliciosas.
- **Mitigación:** Actualizar productos afectados, habilitar autenticación multifactor y monitorear actividad inusual.

7. Manipulación (Tampering)

- Se corrigieron 3–5 vulnerabilidades que permiten alterar la integridad de sistemas, registros o datos en tránsito, con potencial impacto en la infraestructura tecnológica.
- Mitigación: Aplicar parches, validar integridad de sistemas críticos y auditar logs regularmente

Recomendaciones de mitigación:

- Las siguientes acciones deben ejecutarse de manera **transversal** en todos los sistemas afectados por el **Patch Tuesday de junio de 2026**:
- **Aplicación de Parches**
- Aplicar las actualizaciones de seguridad de **junio 2026** de Microsoft utilizando **Windows Update, WSUS, SCCM o Intune** en todos los sistemas Windows del inventario.
- Priorizar el parcheo de sistemas y vulnerabilidades críticas (Elevación de Privilegios, RCE, DoS), incluyendo:
- Sistemas **Windows Netlogon y DNS Client**
- **Microsoft Word, Excel y Office** en todas las estaciones de trabajo
- **Windows Kernel y Windows Server / Active Directory**
- Si el parcheo inmediato no es posible, **implementar reglas de firewall** para bloquear tráfico entrante desde fuentes externas no confiables, especialmente en servicios **IKEv2, TCP/IP y Netlogon**.



- Actualizar **Microsoft Defender** y soluciones EDR a la versión más reciente para mitigar riesgos de escalada de privilegios locales.
- **Reducción de Superficie de Ataque**
- Revisar y deshabilitar servicios o protocolos no requeridos (**IPv6, IKEv2**) en segmentos de red expuestos.
- Aplicar actualizaciones de **Microsoft Office** en todas las estaciones de trabajo para mitigar vulnerabilidades de ejecución remota de código mediante documentos manipulados.
- **Medidas Adicionales y Hardening**
- Implementar el **Principio de Mínimo Privilegio**: los usuarios deben operar con cuentas estándar, limitando el impacto de vulnerabilidades críticas.
- Habilitar **Protected Users Security Group** en Active Directory para reducir riesgos de movimiento lateral (Pass-the-Hash, Pass-the-Ticket).
- Configurar **filtrado de adjuntos en correo electrónico** para bloquear archivos Office (.docx, .docm, .rtf, .xlsx) de remitentes externos no verificados.
- Activar **Protected View y Application Guard** en Microsoft Office para aislar documentos externos.
- Bloquear macros VBA por defecto mediante **GPO**, siguiendo directrices de endurecimiento de Microsoft.
- Implementar **Network Access Control (NAC)** o segmentación de red, limitando el acceso al Controlador de Dominio solo a hosts autorizados.
- Verificar que las **actualizaciones automáticas de Windows Defender** estén habilitadas en todos los endpoints.
- Aplicar las recomendaciones de **seguridad en RDP** introducidas en las actualizaciones de junio 2026 para proteger a los usuarios de posibles amenazas remotas.



Fuentes:



Microsoft Security Response Center (MSRC) — Guía de actualizaciones de junio 2026

<https://msrc.microsoft.com/update-guide>

CISA — Known Exploited Vulnerabilities Catalog (CVE de Microsoft)

<https://www.cisa.gov/known-exploited-vulnerabilities-catalog>

Qualys — Microsoft and Adobe Patch Tuesday, June 2026 Security Update Review

<https://blog.qualys.com/vulnerabilities-threat-research/2026/05/19/microsoft-patch-tuesday-may-2026-security-update-review>

Tenable — Microsoft's June 2026 Patch Tuesday Addresses 125–140 CVEs

<https://www.tenable.com/blog/microsofts-may-2026-patch-tuesday-addresses-125-cves>

Cisco Talos Intelligence — Microsoft Patch Tuesday June 2026: Snort Rules and Prominent Vulnerabilities

<https://blog.talosintelligence.com/microsoft-patch-tuesday-may-2026>

BleepingComputer — Microsoft June 2026 Patch Tuesday fixes 125–140 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 junio 2026

<https://attack.mitre.org>

Windows 11 KB5087591 — June 2026 Patch Tuesday Update

<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.

