

Alerta ID:	055
Fecha del reporte:	16/07/2026
Entidad:	Todas las entidades del ecosistema digital
Título:	Explotación activa de la vulnerabilidad CVE-2026-56164 en Microsoft SharePoint Server
Herramienta de detección	N/A
Activo involucrado:	Microsoft SharePoint Server
Tipo de alerta:	Alerta
Nivel de riesgo:	Alto

Objetivo:

Informar a las organizaciones del sector salud en Colombia sobre la identificación y explotación activa de la vulnerabilidad CVE-2026-56164, que afecta a determinadas versiones locales de Microsoft SharePoint Server. La vulnerabilidad se origina por la ausencia de autenticación en una función crítica y podría permitir que un atacante no autenticado eleve sus privilegios a través de la red y obtenga acceso no autorizado a las instancias afectadas.

La explotación de esta vulnerabilidad podría permitir la modificación no autorizada de información, configuraciones, contenidos y recursos administrados mediante SharePoint Server. En organizaciones del sector salud, esto podría comprometer repositorios documentales, intranets institucionales, archivos administrativos, documentación contractual, procedimientos internos y otros recursos vinculados con la gestión de información clínica y administrativa. El nivel de afectación dependerá de la configuración del servidor, los privilegios



obtenidos, su exposición a internet y su integración con otros componentes de la infraestructura tecnológica.

El propósito de esta alerta es que las organizaciones del sector salud validen si utilizan versiones afectadas de Microsoft SharePoint Server en infraestructura propia, centros de datos, ambientes administrados por terceros o servicios integrados a sus procesos institucionales. Esta validación debe incluir la revisión de inventarios tecnológicos, versiones y compilaciones instaladas, servidores expuestos a internet, mecanismos de autenticación, integraciones con directorios corporativos, aplicaciones conectadas, cuentas privilegiadas, registros de actividad y medidas de segmentación de red.

Asimismo, se busca que las entidades prioricen la aplicación de las actualizaciones y medidas de mitigación publicadas por Microsoft, y desarrollen actividades de análisis que permitan identificar posibles indicadores de compromiso. Esta vulnerabilidad fue incorporada por CISA al Catálogo de Vulnerabilidades Conocidas Explotadas, KEV, el 14 de julio de 2026, debido a la existencia de evidencia de explotación activa.

Descripción:



La vulnerabilidad CVE-2026-56164 afecta a Microsoft SharePoint Server y se origina por la ausencia de un mecanismo de autenticación adecuado en una función crítica del producto. Esta debilidad, clasificada como CWE-306, puede permitir que un atacante no autenticado acceda al servidor a través de la red y eleve sus privilegios dentro de una instancia vulnerable de SharePoint. La explotación no requiere que el atacante posea previamente una cuenta válida ni que exista interacción por parte de un usuario.

La vulnerabilidad afecta a implementaciones locales, conocidas como *on-premises*, de Microsoft SharePoint Enterprise Server 2016, SharePoint Server 2019 y SharePoint Server



Subscription Edition que no cuenten con las actualizaciones de seguridad correspondientes. De acuerdo con la información registrada por Microsoft, se encuentran afectadas las versiones anteriores a las siguientes compilaciones:

- Microsoft SharePoint Enterprise Server 2016: 16.0.5561.1001.
- Microsoft SharePoint Server 2019: 16.0.10417.20175.
- Microsoft SharePoint Server Subscription Edition: 16.0.19725.20434.

Microsoft asignó a la vulnerabilidad una puntuación CVSS 3.1 de 5,3, correspondiente a severidad media, con afectación principalmente sobre la integridad de la información. Sin embargo, el análisis de NIST le asignó una puntuación CVSS 3.1 de 9,8, clasificada como crítica, al considerar un posible impacto alto sobre la confidencialidad, integridad y disponibilidad de los sistemas comprometidos. Debido a esta diferencia, la priorización no debe basarse únicamente en la puntuación asignada, sino también en la evidencia de explotación activa.

La Agencia de Seguridad de Infraestructura y Ciberseguridad de Estados Unidos, CISA, incorporó CVE-2026-56164 a su Catálogo de Vulnerabilidades Conocidas Explotadas, KEV, el 14 de julio de 2026. Esta incorporación confirma que existen evidencias de uso activo de la vulnerabilidad por parte de actores maliciosos. CISA también indicó que su explotación puede permitir el acceso no autorizado a servidores SharePoint instalados localmente.

En una organización del sector salud, el compromiso de un servidor SharePoint podría facilitar el acceso o la modificación no autorizada de documentos institucionales, procedimientos, archivos administrativos, información contractual, contenidos internos y otros recursos almacenados o gestionados mediante la plataforma. El impacto real dependerá de la información alojada, los permisos obtenidos, la exposición del servidor a internet, las integraciones con otros sistemas y el nivel de segmentación de la infraestructura tecnológica.



Hasta el momento, las fuentes oficiales consultadas no publican detalles técnicos completos sobre el procedimiento utilizado para explotar la vulnerabilidad. Por esta razón, no se debe asumir que la aplicación de la actualización elimina por sí sola cualquier compromiso previo. Las organizaciones que hayan mantenido servidores vulnerables expuestos a internet deben complementar la actualización con revisión de registros, cuentas, configuraciones, archivos modificados y posibles indicadores de actividad maliciosa.

Consecuencias de la explotación



La explotación exitosa de CVE-2026-56164 puede generar impactos técnicos, operativos y legales significativos para las entidades afectadas. Las principales consecuencias incluyen:

- **Acceso no autorizado al servidor SharePoint:** un atacante remoto sin credenciales válidas podría aprovechar la vulnerabilidad para obtener privilegios indebidos dentro de una instancia vulnerable de Microsoft SharePoint Server.
- **Modificación no autorizada de información:** el atacante podría alterar documentos, configuraciones, contenidos, bibliotecas, listas y otros recursos administrados mediante SharePoint, afectando la integridad de la información institucional.
- **Exposición de información sensible:** dependiendo de los permisos obtenidos y de la configuración del entorno, podrían quedar expuestos documentos administrativos, contratos, procedimientos internos, reportes, credenciales almacenadas, datos personales y otra información relacionada con los procesos del sector salud.
- **Compromiso de cuentas y privilegios:** la explotación podría facilitar el acceso a cuentas con mayores permisos o permitir el uso indebido de identidades vinculadas con SharePoint, el directorio corporativo u otros servicios integrados.



- **Movimiento lateral dentro de la red:** un servidor SharePoint comprometido podría utilizarse como punto de apoyo para intentar acceder a otros sistemas internos, especialmente cuando el servidor comparte credenciales, servicios, integraciones o conectividad con componentes críticos de la infraestructura.
- **Alteración de procesos institucionales:** la modificación o eliminación de documentos y flujos de trabajo podría afectar procesos administrativos, jurídicos, contractuales, financieros, asistenciales o de gestión documental.
- **Interrupción de servicios:** la explotación podría causar indisponibilidad parcial o total de SharePoint, afectar el acceso a intranets, repositorios documentales y aplicaciones internas, y generar retrasos en actividades operativas.
- **Compromiso de integraciones:** cuando SharePoint está conectado con servicios de autenticación, correo, directorios corporativos, aplicaciones administrativas o plataformas de colaboración, el incidente podría ampliar su impacto hacia otros componentes tecnológicos.
- **Persistencia del acceso malicioso:** si el atacante logra modificar configuraciones, cuentas, archivos o componentes del servidor, podría mantener acceso incluso después de aplicar la actualización de seguridad. Por esta razón, la instalación del parche debe complementarse con una revisión de posibles indicadores de compromiso.
- **Pérdida de trazabilidad y confianza en la información:** la alteración de registros, documentos o configuraciones puede dificultar la reconstrucción del incidente y afectar la confiabilidad de la información almacenada en la plataforma.
- **Impacto regulatorio y reputacional:** la exposición, alteración o pérdida de datos personales y sensibles podría generar incumplimientos frente a la Ley 1581 de 2012, la normativa sobre protección de datos personales y las obligaciones aplicables a las entidades del sector salud, además de afectar la reputación y la confianza de pacientes, usuarios, proveedores y entidades de control.



- **Afectación de la continuidad operativa:** la necesidad de aislar servidores, restaurar información, cambiar credenciales, realizar análisis forense y validar integraciones podría producir interrupciones prolongadas y aumentar los costos de recuperación.

Modo de explotación del ataque



La explotación de CVE-2026-56164 se produce de forma remota contra servidores Microsoft SharePoint instalados localmente. De acuerdo con la información disponible, el ataque puede ejecutarse a través de la red, presenta baja complejidad, no requiere credenciales previas ni interacción de un usuario. La vulnerabilidad se origina en la ausencia de autenticación para una función crítica del producto, lo que permite que un actor no autorizado eleve sus privilegios dentro de una instancia vulnerable.

Aunque Microsoft, CISA y NIST no han divulgado públicamente todos los detalles técnicos del procedimiento de explotación, el flujo general puede representarse mediante las siguientes fases:

Fase 1. Identificación de servidores SharePoint vulnerables

El atacante identifica servidores Microsoft SharePoint Server accesibles desde internet o desde una red previamente comprometida. La búsqueda puede centrarse en instancias locales de SharePoint Enterprise Server 2016, SharePoint Server 2019 o SharePoint Server Subscription Edition que no cuenten con las compilaciones corregidas.

La exposición directa a internet incrementa la posibilidad de explotación. Sin embargo, un servidor no expuesto públicamente también podría ser atacado desde la red interna si el actor ya obtuvo acceso inicial mediante otro sistema, una cuenta comprometida o un proveedor tecnológico.



Fase 2. Interacción remota sin autenticación

El atacante establece comunicación con el servidor vulnerable a través de la red e interactúa con la función de SharePoint afectada. Debido a la falla de autenticación, no necesita disponer de una cuenta válida, contraseña, token de sesión ni permisos asignados previamente.

El vector CVSS publicado por Microsoft y NIST confirma las siguientes condiciones de explotación:

- Vector de ataque: red.
- Complejidad del ataque: baja.
- Privilegios requeridos: ninguno.
- Interacción del usuario: no requerida.
- Alcance: permanece dentro del componente de seguridad afectado.

Fase 3. Omisión del control de autenticación

El servidor procesa una operación asociada con una función crítica sin comprobar correctamente la identidad o autorización del solicitante. Esta condición corresponde a la debilidad CWE-306, denominada “ausencia de autenticación para una función crítica”.

Como resultado, una solicitud proveniente de un actor no autenticado puede alcanzar funcionalidades que deberían estar restringidas a usuarios o procesos autorizados.

Fase 4. Elevación de privilegios

Una vez aprovechada la falla, el atacante puede obtener privilegios superiores dentro de la instancia afectada de SharePoint. El nivel exacto de acceso alcanzado no ha sido detallado públicamente por Microsoft.

Por esta razón, no debe afirmarse que CVE-2026-56164 concede automáticamente privilegios de administrador del sistema operativo, control total del servidor o ejecución remota de código.



Lo confirmado oficialmente es la elevación de privilegios a través de la red y la posibilidad de acceso no autorizado a servidores SharePoint locales.

Fase 5. Acciones posteriores a la explotación

Después de obtener acceso privilegiado, las acciones posibles dependerán de los permisos alcanzados, la configuración de SharePoint, la información almacenada y las integraciones existentes. Entre las actividades potenciales se encuentran la consulta o modificación de contenidos, cambios sobre configuraciones accesibles, manipulación de recursos documentales y uso de la instancia comprometida como punto de apoyo para intentar acceder a otros componentes.

Estas acciones corresponden a consecuencias potenciales y no a una cadena de pos-explotación confirmada públicamente para todos los incidentes. CISA clasifica la explotación como activa y automatizable, con un impacto técnico parcial. CVE-2026-56164 fue incorporada a su Catálogo de Vulnerabilidades Conocidas Explotadas el 14 de julio de 2026.

Elemento	Condición confirmada
Tipo de acceso	Remoto, a través de la red
Autenticación previa	No requerida
Privilegios previos	No requerida
Interacción del usuario	No requerida
Complejidad	Baja
Debilidad	CWE-306, ausencia de autenticación para una función crítica
Resultado confirmado	Elevación de privilegios



Elemento	Condición confirmada
Explotación activ	Sí, confirmada mediante inclusión en CISA KEV
Automatización del ataque	CISA la considera automatizable
Ejecución remota de código	No confirmada públicamente para este CVE
Malware o herramienta utilizada	No divulgado públicamente
Endpoint o solicitud específica	No divulgados públicamente
Persistencia y canal C2	No confirmados como parte inherente de esta vulnerabilidad

vulnerabilidades asociadas

A diferencia de amenazas basadas principalmente en malware o en el abuso de herramientas legítimas, esta alerta se encuentra asociada directamente con una vulnerabilidad identificada y publicada como **CVE-2026-56164**. La falla afecta a determinadas versiones locales de Microsoft SharePoint Server y puede permitir que un atacante no autenticado eleve privilegios a través de la red.

Hasta la fecha de elaboración de este boletín, Microsoft, CISA y NIST no han informado que CVE-2026-56164 deba combinarse obligatoriamente con otra vulnerabilidad para lograr su explotación. Tampoco se ha publicado una cadena oficial que relacione este CVE con vulnerabilidades adicionales, ejecución remota de código, instalación de malware, persistencia en el sistema operativo o movimiento lateral.

La vulnerabilidad se encuentra clasificada bajo la debilidad **CWE-306, Missing Authentication for Critical Function**, que corresponde a la ausencia de autenticación en una función que



debería estar restringida. Como consecuencia, una operación sensible puede ser alcanzada por un actor que no ha demostrado previamente su identidad ni dispone de permisos válidos.

Los principales elementos relacionados con la vulnerabilidad son los siguientes:

- **Ausencia de autenticación en una función crítica:** constituye la debilidad técnica directamente asociada con CVE-2026-56164. El servidor no realiza correctamente la validación de identidad antes de permitir el acceso a una función sensible.
- **Versiones de SharePoint sin actualizar:** la exposición se mantiene en las versiones afectadas que no hayan alcanzado las compilaciones corregidas publicadas por Microsoft. NIST identifica como afectados SharePoint Enterprise Server 2016, SharePoint Server 2019 y SharePoint Server Subscription Edition anteriores a las versiones solucionadas.
- **Exposición del servidor a internet:** cuando una instancia vulnerable se encuentra accesible públicamente, puede ser localizada y atacada directamente desde internet. CISA señala que la vulnerabilidad permite obtener acceso no autorizado a instancias locales de SharePoint y la considera automatizable.
- **Segmentación insuficiente de la red:** un servidor SharePoint con comunicación amplia hacia directorios, servidores de archivos, bases de datos, sistemas de respaldo u otras aplicaciones puede aumentar el alcance de un incidente. Esta condición no es parte del CVE, pero puede facilitar que un compromiso inicial afecte otros activos.
- **Permisos e integraciones excesivas:** cuentas de servicio con privilegios elevados, conexiones con directorios corporativos y aplicaciones integradas pueden ampliar las consecuencias del acceso no autorizado.
- **Monitoreo insuficiente:** la falta de centralización de registros, alertas sobre accesos anómalos, revisión de cambios administrativos y conservación adecuada de evidencias puede retrasar la identificación de una explotación.
- **Aplicación tardía de actualizaciones acumulativas:** Microsoft publicó actualizaciones de seguridad que incluyen la corrección de CVE-2026-56164 junto con otras vulnerabilidades de



SharePoint y componentes de Office. Para SharePoint Server 2019, la actualización KB5002883 corresponde a la compilación 16.0.10417.20175.

Las demás vulnerabilidades corregidas por la misma actualización acumulativa no deben presentarse como parte de una cadena de ataque de CVE-2026-56164. El hecho de que varios CVE sean corregidos mediante un mismo paquete no demuestra que sean explotados conjuntamente. Microsoft no ha publicado esa relación.

Mapeo orientativo frente a MITRE ATT&CK

Las fuentes oficiales de la vulnerabilidad no proporcionan un mapeo específico frente a MITRE ATT&CK. No obstante, para fines de gestión de detección y respuesta, puede establecerse la siguiente relación orientativa, limitada a los comportamientos confirmados o directamente compatibles con la naturaleza de la vulnerabilidad:

Táctica	Técnica / ID	Aplicación al contexto de CVE-2026-56164
Initial Access (TA0001)	Exploit Public-Facing Application, T1190	Aplica cuando el atacante explota una instancia vulnerable de SharePoint expuesta a internet para obtener acceso inicial sin disponer de credenciales. MITRE define esta técnica como el aprovechamiento de una debilidad en una aplicación accesible públicamente.
Privilege Escalation, TA0004	Exploitation for Privilege Escalation, T1068	Se relaciona con el resultado confirmado de la vulnerabilidad, debido a que el atacante aprovecha una falla de software para obtener privilegios que no le habían sido asignados.

No se deben asignar, sin evidencia adicional del incidente, técnicas relacionadas con ejecución de comandos, persistencia, inyección de procesos, descubrimiento, recolección de archivos, movimiento lateral, comando y control o exfiltración. Estas actividades podrían ocurrir durante una intrusión



posterior, pero no han sido documentadas públicamente como comportamientos inherentes o confirmados de CVE-2026-56164.

La inclusión de CVE-2026-56164 en el Catálogo de Vulnerabilidades Conocidas Explotadas de CISA confirma que la vulnerabilidad está siendo utilizada activamente. CISA estableció como acción requerida la aplicación de las mitigaciones indicadas por el fabricante, la evaluación de la exposición de los activos y, cuando no existan medidas disponibles, la suspensión del uso del producto afectado

Recomendaciones de detección y mitigación

Los equipos de operaciones de seguridad, infraestructura, administración de SharePoint y respuesta a incidentes deben tratar CVE-2026-56164 como una vulnerabilidad prioritaria, debido a que su explotación activa fue confirmada por CISA. Las medidas deben centrarse en identificar servidores vulnerables, reducir su exposición, aplicar las actualizaciones oficiales y revisar si existieron accesos no autorizados antes de la corrección.

A diferencia de una campaña de malware con indicadores específicos, hasta la fecha no se han publicado oficialmente direcciones IP, dominios, hashes, nombres de archivos, reglas YARA, rutas HTTP vulnerables ni cargas útiles asociadas exclusivamente con CVE-2026-56164. Por esta razón, la detección debe apoyarse en el análisis de comportamiento, registros del servidor, cambios administrativos y evidencia de acceso anómalo.

Medidas prioritarias de mitigación

- **Identificar todas las instalaciones locales de SharePoint:** realizar un inventario completo de servidores web front-end, servidores de aplicaciones, nodos adicionales de la granja, ambientes de pruebas, contingencia y recuperación, así como instancias administradas por proveedores. La vulnerabilidad se relaciona con SharePoint Server instalado localmente, no con el servicio SharePoint Online administrado directamente por Microsoft.



- **Verificar las versiones y compilaciones instaladas:** comparar la versión de cada servidor con las compilaciones corregidas por Microsoft. Deben considerarse vulnerables las instalaciones anteriores a las siguientes versiones:

Producto	Compilación corregida	Actualización
SharePoint Enterprise Server 2016	16.0.5561.1001	KB5002891
SharePoint Server 2019	16.0.10417.20175	KB5002883
SharePoint Server Subscription Edition	16.0.19725.20434	KB5002882

Microsoft confirma que KB5002883 corresponde a la compilación 16.0.10417.20175 de SharePoint Server 2019 y que KB5002882 corresponde a la compilación 16.0.19725.20434 de SharePoint Server Subscription Edition.

- **Aplicar inmediatamente las actualizaciones de seguridad:** instalar el paquete correspondiente en todos los servidores que forman parte de la granja. No debe actualizarse únicamente el servidor publicado en internet, debido a que una granja con nodos en niveles diferentes puede quedar en un estado inconsistente o continuar expuesta.
- **Seguir las instrucciones específicas del fabricante:** verificar previamente si la granja utiliza SharePoint Workflow Manager o Classic Workflow Manager. Microsoft establece requisitos adicionales para estos componentes antes de instalar determinadas actualizaciones. En SharePoint Server Subscription Edition también se documenta una acción posterior a la ejecución de PSConfig relacionada con una validación de defensa en profundidad. Estas instrucciones deben seguirse directamente desde el artículo oficial correspondiente a cada versión.
- **Completar la configuración posterior a la instalación:** ejecutar las herramientas de configuración indicadas por Microsoft y confirmar que todos los servidores de la granja



quedaron actualizados correctamente. La presencia del archivo de actualización en Windows no demuestra por sí sola que la granja haya completado todo el proceso.

- **Verificar el estado operativo después de actualizar:** validar el acceso a los sitios, la Administración Central, los servicios de búsqueda, flujos de trabajo, aplicaciones de servicio, integraciones, autenticación y funcionalidades críticas utilizadas por la entidad.
- **Restringir temporalmente la exposición:** cuando la actualización no pueda aplicarse de inmediato, limitar el acceso al servidor mediante firewall, VPN, proxy inverso o listas de direcciones autorizadas. La restricción temporal reduce el riesgo, pero no reemplaza la instalación del parche.
- **Eliminar exposiciones innecesarias a internet:** revisar si la Administración Central, servicios internos, interfaces de gestión, puertos de administración o sitios que no necesitan acceso público se encuentran publicados externamente.
- **Segmentar los servidores SharePoint:** restringir la comunicación desde la granja hacia otros segmentos de la red. Solo deben permitirse conexiones necesarias con bases de datos, directorios, servicios de aplicaciones, sistemas de respaldo y componentes autorizados.
- **Aplicar el principio de mínimo privilegio:** revisar cuentas de servicio, identidades de grupos de aplicaciones, administradores de granja, administradores locales y permisos sobre bases de datos. Deben eliminarse privilegios que no sean estrictamente necesarios.
- **Limitar las conexiones administrativas:** restringir RDP, PowerShell Remoting, WinRM, SMB y otras interfaces de administración a estaciones seguras, redes de gestión y personal autorizado.

Recomendaciones de detección y búsqueda de amenazas

- **Conservar y centralizar los registros:** recopilar los logs de IIS, Unified Logging Service, ULS, Windows Event Log, SQL Server, firewall, WAF, proxy inverso, balanceador y sistemas de autenticación. Microsoft señala que los registros ULS permiten recopilar y filtrar información generada por los componentes de SharePoint.



- **Aumentar temporalmente la retención de registros:** evitar que los logs relacionados con el periodo previo a la actualización sean sobrescritos. Debe conservarse suficiente información para reconstruir solicitudes, sesiones, errores y modificaciones ocurridas desde antes de la divulgación pública de la vulnerabilidad.
- **Buscar solicitudes HTTP anómalas:** revisar accesos provenientes de direcciones IP desconocidas, múltiples intentos contra rutas de SharePoint, secuencias de respuestas 401, 403, 404 o 500 seguidas de respuestas exitosas, métodos HTTP poco habituales y solicitudes realizadas fuera de los horarios normales.
- **Identificar actividad sin autenticación:** priorizar la revisión de solicitudes que hayan alcanzado funciones sensibles sin una sesión autenticada, especialmente cuando provengan de internet o de segmentos internos que normalmente no administran SharePoint.
- **Revisar cambios administrativos:** buscar incorporaciones inesperadas a los grupos de administradores de granja, administradores de colecciones de sitios, administradores locales, propietarios de sitios o grupos con control total.
- **Supervisar modificaciones de permisos:** generar alertas cuando se modifiquen permisos sobre sitios, bibliotecas, listas, documentos o elementos que contengan información clínica, administrativa, financiera o contractual.
- **Revisar cuentas nuevas o reactivadas:** identificar usuarios creados, habilitados o incorporados a grupos privilegiados sin una solicitud de cambio válida.
- **Monitorear alteraciones en la configuración:** revisar cambios sobre aplicaciones web, proveedores de autenticación, mapeos de acceso alternativo, soluciones desplegadas, características, servicios, grupos de aplicaciones y archivos de configuración.
- **Verificar la integridad del sistema de archivos:** inspeccionar los directorios de instalación de SharePoint, rutas de aplicaciones web de IIS y archivos de configuración en busca de archivos nuevos o modificados sin autorización. Debe prestarse atención a páginas ASPX, ensamblados, scripts y archivos con fechas o propietarios anómalos. Esta medida es una



práctica general de búsqueda de compromiso y no constituye un indicador específico publicado para CVE-2026-56164.

- **Revisar actividad de procesos:** identificar procesos iniciados por los grupos de aplicaciones de SharePoint o por IIS que no correspondan con el comportamiento normal del servidor. Deben investigarse intérpretes de comandos, herramientas administrativas, conexiones remotas y procesos desconocidos.
- **Monitorear conexiones salientes:** los servidores SharePoint normalmente deben presentar un patrón de comunicación relativamente estable. Deben investigarse conexiones hacia direcciones externas no autorizadas, puertos inusuales, destinos recientemente registrados o transferencias de datos atípicas.
- **Correlacionar eventos mediante identificadores de SharePoint:** utilizar los identificadores de correlación presentes en los registros ULS para relacionar errores, solicitudes y eventos asociados con una misma operación. Microsoft documenta el uso del CorrelationId para vincular información distribuida entre diferentes registros.
- **Establecer alertas por desactivación del monitoreo:** detectar eliminación de logs, reducción no autorizada de los niveles de auditoría, detención de agentes de seguridad o modificación de las políticas de retención.

Acciones ante indicios de explotación

- Aislar el servidor afectado de internet y limitar su comunicación con la red interna, sin apagarlo de manera inmediata cuando sea necesario conservar evidencia volátil.
- Preservar los registros de IIS, ULS, Windows, SQL Server, firewall, proxy, WAF y autenticación antes de realizar actividades que puedan sobrescribirlos.
- Capturar la información necesaria para el análisis forense, incluyendo procesos, conexiones de red, sesiones, tareas, servicios, archivos recientes y cambios en la configuración.
- Revisar todos los servidores de la granja, no únicamente el nodo donde fue detectada la actividad sospechosa.



- Restablecer las credenciales de cuentas administrativas, cuentas de servicio e identidades que hayan estado disponibles para el servidor comprometido.
- Revisar secretos, certificados, claves, tokens e integraciones utilizados por SharePoint y reemplazarlos cuando exista posibilidad de exposición.
- Validar las modificaciones realizadas sobre documentos, permisos, sitios, configuraciones, soluciones y bases de datos.
- Restaurar desde copias conocidas como seguras cuando no sea posible garantizar la integridad del servidor.
- Notificar el incidente al equipo institucional de respuesta, al responsable de seguridad de la información, al área jurídica y al responsable de protección de datos personales, según el alcance identificado.

Consideraciones adicionales

La instalación de la actualización corrige la vulnerabilidad, pero no elimina accesos, cuentas, archivos o configuraciones que un atacante haya establecido antes de su aplicación. Por este motivo, las entidades que hayan tenido servidores vulnerables expuestos a internet deben realizar una revisión de compromiso, incluso cuando el parche ya haya sido instalado.

No se recomienda crear reglas de bloqueo basadas en rutas, hashes o direcciones IP obtenidas de fuentes no verificadas. La ausencia de indicadores oficiales específicos obliga a priorizar controles conductuales, revisión de cambios y análisis integral de registros

Recomendaciones de prevención y mitigación

1. En paralelo con las actividades de detección y búsqueda de posibles indicadores de compromiso, se recomienda implementar las siguientes medidas de fortalecimiento, prevención y reducción de la superficie de ataque:
2. **Aplicar las actualizaciones de seguridad publicadas por Microsoft:** actualizar todas las instancias afectadas de SharePoint Enterprise Server 2016, SharePoint Server 2019 y SharePoint Server Subscription Edition. La actualización debe instalarse en todos los



servidores que integran la granja, no únicamente en el nodo expuesto a internet. CVE-2026-56164 presenta explotación activa confirmada, por lo que su atención debe considerarse prioritaria.

3. **Completar el proceso de actualización de la granja:** después de instalar los paquetes de seguridad, ejecutar las herramientas de configuración indicadas por Microsoft, como el Asistente para configuración de productos de SharePoint o PSConfig, cuando corresponda. Posteriormente, verificar que todos los nodos presenten la compilación corregida y que no existan servidores con niveles de actualización diferentes.
4. **Reducir la exposición directa a internet:** restringir el acceso público únicamente a las aplicaciones web que realmente lo requieran. Los servidores administrativos, la Administración Central de SharePoint, las interfaces de gestión y los ambientes de pruebas o contingencia no deben estar publicados directamente en internet. Cuando no sea posible actualizar de inmediato, se recomienda retirar temporalmente el servidor de la exposición pública o limitar el acceso mediante VPN, firewall, proxy inverso o listas de direcciones autorizadas. Esta medida es temporal y no reemplaza la actualización.
5. **Implementar segmentación de red:** separar los servidores web, servidores de aplicaciones y bases de datos de SharePoint de las redes de usuarios, dispositivos médicos y sistemas clínicos. Solo deben habilitarse los flujos estrictamente necesarios entre los componentes de la granja. Microsoft recomienda controlar mediante firewall qué servidores pueden acceder a SQL Server y restringir las comunicaciones que no sean necesarias, incluyendo los puertos utilizados por las bases de datos.
6. **Restringir el acceso a SQL Server:** permitir conexiones a las bases de datos de SharePoint únicamente desde los servidores autorizados de la granja y desde estaciones administrativas controladas. Los demás activos deben tener bloqueado el acceso a los puertos de SQL Server. No se deben publicar las bases de datos directamente hacia internet ni hacia segmentos de usuarios.



7. **Aplicar el principio de mínimo privilegio:** revisar las cuentas de servicio, grupos de administradores de granja, administradores locales y roles de SQL Server. Las cuentas de aplicaciones de servicio no deben disponer de privilegios de administrador local ni de roles elevados en SQL Server, salvo que exista un requisito técnico expresamente documentado. Microsoft recomienda usar cuentas administrativas individuales e identificables para facilitar la trazabilidad de las acciones realizadas.
8. **Separar las cuentas administrativas de las cuentas de uso cotidiano:** los administradores de SharePoint deben utilizar cuentas exclusivas para instalación, mantenimiento y actualización. Estas cuentas no deben emplearse para correo electrónico, navegación web ni labores ofimáticas. Siempre que la arquitectura lo permita, se debe aplicar autenticación multifactor a los accesos administrativos, VPN, escritorios remotos y plataformas de gestión.
9. **Restringir el inicio de sesión de las cuentas de servicio:** impedir que las cuentas utilizadas por grupos de aplicaciones y servicios de SharePoint inicien sesión localmente o mediante Escritorio Remoto. Microsoft recomienda aplicar las opciones “Denegar inicio de sesión local” y “Denegar inicio de sesión a través de Servicios de Escritorio Remoto” a las cuentas de aplicaciones de servicio que no requieran acceso interactivo.
10. **Limitar los servicios y protocolos administrativos:** restringir RDP, WinRM, PowerShell Remoting, SMB y acceso remoto al registro únicamente a redes de administración, estaciones seguras y personal autorizado. Estas interfaces no deben quedar accesibles desde internet ni desde redes de usuarios generales.
11. **Controlar las conexiones salientes:** configurar el firewall para que los servidores SharePoint solo puedan comunicarse con destinos necesarios y autorizados, como servicios de actualización, bases de datos, directorios, correo o integraciones institucionales. Las conexiones hacia internet deben ser registradas, filtradas y supervisadas.
12. **Proteger los directorios y archivos críticos:** evitar modificaciones no autorizadas en las rutas de instalación de SharePoint, los directorios de IIS, archivos web.config, ensamblados,



páginas ASPX y carpetas de configuración. No se deben cambiar indiscriminadamente los permisos establecidos por SharePoint, debido a que alteraciones incorrectas pueden afectar el funcionamiento, el registro de eventos y las tareas administrativas de la plataforma.

13. **Utilizar un firewall de aplicaciones web:** cuando SharePoint deba permanecer publicado, implementar un WAF o proxy inverso que permita limitar métodos HTTP, controlar tamaños de solicitudes, aplicar reglas de reputación, registrar tráfico y bloquear patrones anómalos. El WAF constituye una medida adicional y no sustituye la aplicación de los parches.
14. **Mantener habilitados los registros de seguridad:** conservar los logs de IIS, ULS, Windows, SQL Server, firewall, balanceador, WAF y sistemas de autenticación. Los registros deben enviarse a una plataforma centralizada y contar con una retención suficiente para investigaciones posteriores. No deben almacenarse únicamente en el servidor SharePoint.
15. **Fortalecer la supervisión de cambios:** establecer alertas ante modificaciones de administradores de granja, permisos de colecciones de sitios, aplicaciones web, cuentas de servicio, grupos locales, archivos de configuración y soluciones desplegadas. Todo cambio administrativo debe estar respaldado por una solicitud autorizada.
16. **Implementar protección EDR o XDR en los servidores:** mantener agentes de seguridad actualizados y configurados para detectar creación de procesos inusuales, intérpretes de comandos iniciados desde IIS, cambios en archivos críticos, conexiones salientes anómalas y manipulación de servicios. Las exclusiones requeridas por SharePoint deben ser mínimas, documentadas y revisadas periódicamente.
17. **Mantener copias de seguridad protegidas:** respaldar las bases de datos, configuraciones y contenidos críticos de SharePoint. Las copias deben mantenerse separadas del entorno productivo, protegidas contra modificación y sometidas a pruebas periódicas de restauración. Una copia conectada permanentemente a la misma infraestructura puede resultar afectada durante un incidente.



18. **Validar la seguridad de proveedores y terceros:** solicitar a los proveedores que administren, alojen o soporten SharePoint evidencia de actualización, versión instalada, fecha de aplicación del parche, revisión de registros y medidas de contención. No debe asumirse que los ambientes tercerizados están actualizados sin una verificación formal.
19. **Revisar periódicamente la necesidad de exposición:** evaluar si las funciones actualmente publicadas pueden trasladarse a redes privadas, servicios administrados o arquitecturas con menor exposición. Los sitios que ya no sean utilizados deben cerrarse y retirarse de forma controlada.
20. **Establecer un procedimiento de respuesta específico:** definir responsables para aislar servidores, preservar evidencia, restablecer credenciales, revisar integraciones, restaurar información y comunicar incidentes. La aplicación del parche no elimina modificaciones o accesos persistentes que hayan sido establecidos antes de la actualización.
21. **No utilizar indicadores no verificados:** evitar incorporar a los controles institucionales direcciones IP, dominios, hashes, rutas o reglas de detección atribuidas a CVE-2026-56164 cuando no provengan de Microsoft, CISA u otras fuentes técnicas confiables. Actualmente, las fuentes oficiales confirman la explotación activa, pero no han publicado una lista completa de indicadores específicos de la campaña.
22. La prioridad debe concentrarse en actualizar, reducir la exposición pública y verificar la integridad de las instancias que permanecieron vulnerables. Las medidas de segmentación, mínimo privilegio y monitoreo disminuyen las consecuencias de una explotación, pero no corrigen por sí mismas CVE-2026-56164.

Recomendaciones de respuesta ante compromiso

En caso de confirmarse o sospecharse la explotación de CVE-2026-56164 en una instancia de Microsoft SharePoint Server, se recomienda ejecutar el siguiente procedimiento de análisis,



contención, erradicación y recuperación. La vulnerabilidad debe tratarse como prioritaria debido a que CISA confirmó su explotación activa contra servidores SharePoint instalados localmente.

Activar el procedimiento institucional de respuesta a incidentes: informar al CISO, al equipo de respuesta, a infraestructura, al administrador de SharePoint, al responsable de continuidad, al área jurídica y al responsable de protección de datos personales. Se debe designar un coordinador del incidente y registrar todas las decisiones y acciones realizadas.

Determinar el alcance inicial del incidente: identificar todos los servidores que integran la granja de SharePoint, incluyendo servidores web front-end, servidores de aplicaciones, Administración Central, bases de datos, balanceadores, ambientes de contingencia, pruebas y recuperación. También deben revisarse los sistemas de autenticación, proveedores tecnológicos e integraciones relacionadas.

Aislar los servidores sospechosos: retirar temporalmente la instancia afectada de internet o del balanceador de carga y restringir su comunicación con la red interna. Cuando sea técnicamente posible, el aislamiento debe realizarse mediante EDR, firewall o segmentación de red. No se recomienda apagar inmediatamente el servidor, debido a que pueden perderse procesos, conexiones, sesiones y otros elementos de memoria necesarios para el análisis forense.

Preservar la evidencia volátil: antes de reiniciar, actualizar o modificar el servidor, capturar la memoria RAM, procesos en ejecución, conexiones de red, sesiones activas, puertos abiertos, tablas de enrutamiento, tareas programadas, servicios, usuarios conectados y demás artefactos disponibles. La captura debe realizarse mediante herramientas autorizadas y por personal capacitado.

Recolectar imágenes y registros forenses: obtener una imagen o instantánea de los discos de los servidores comprometidos y conservar, como mínimo, los siguientes registros:



- Registros ULS de SharePoint.
- Eventos de seguridad, sistema y aplicaciones de Windows.
- Telemetría de EDR o XDR.
- Registros de SQL Server.
- Logs de firewall, WAF, proxy inverso y balanceador.
- Registros de Active Directory y sistemas de autenticación.
- Historial de actualizaciones y cambios administrativos.
- Registros de acceso remoto, RDP, WinRM y PowerShell.

La evidencia debe almacenarse de forma segura, calcularse su hash y mantener una cadena de custodia que permita demostrar su integridad.

Evitar la eliminación manual de artefactos: no se deben borrar inmediatamente cuentas, archivos, páginas ASPX, ensamblados, tareas, servicios o configuraciones sospechosas. La eliminación prematura puede destruir evidencia y dificultar la determinación del alcance real. Estos elementos deben documentarse, copiarse y analizarse antes de su remoción.

Revisar accesos y cambios no autorizados: examinar la creación o modificación de cuentas, administradores de granja, administradores locales, propietarios de sitios, permisos, aplicaciones web, soluciones desplegadas, características, archivos de configuración y grupos de aplicaciones. También deben verificarse cambios sobre documentos, bibliotecas, listas y bases de datos.

Contener las identidades comprometidas: deshabilitar temporalmente las cuentas sospechosas, cerrar sesiones activas y revocar accesos administrativos. Se deben restablecer las credenciales de administradores, cuentas de servicio e identidades que pudieron quedar expuestas. Los cambios en cuentas de servicio de SharePoint deben realizarse mediante los procedimientos soportados por Microsoft, debido a que modificar directamente sus contraseñas puede afectar la operación de la granja.



Rotar secretos y credenciales técnicas: evaluar el cambio de claves de API, contraseñas de bases de datos, secretos de aplicaciones, certificados, claves privadas, tokens e identidades utilizadas por las integraciones de SharePoint. La rotación debe priorizar los elementos que estuvieron almacenados, utilizados o accesibles desde el servidor comprometido.

Aplicar bloqueos derivados del análisis: bloquear en firewall, WAF, proxy, DNS, EDR y SIEM las direcciones IP, dominios, rutas, archivos o patrones que hayan sido identificados durante la investigación. No deben incorporarse indicadores atribuidos al CVE que provengan de fuentes no verificadas o que no guarden relación con la evidencia del incidente.

Realizar búsqueda de amenazas en toda la infraestructura: revisar si las mismas direcciones, cuentas, solicitudes, archivos o comportamientos aparecen en otros servidores. La investigación debe incluir sistemas de identidad, servidores de archivos, bases de datos, plataformas administrativas y demás activos con los que SharePoint tenga comunicación.

Aplicar las actualizaciones oficiales en toda la granja: instalar la corrección correspondiente en todos los nodos afectados y completar el proceso mediante las herramientas de configuración de SharePoint indicadas por Microsoft. No debe mantenerse en producción un servidor que no pueda actualizarse o que permanezca en una compilación vulnerable.

Reconstruir los servidores cuando no pueda garantizarse su integridad: si se confirma acceso no autorizado, modificación de componentes críticos, persistencia o ausencia de registros suficientes, la opción más segura es reinstalar o reconstruir los servidores desde imágenes confiables. Limpiar manualmente algunos archivos no garantiza la erradicación completa.

Validar las copias de seguridad antes de restaurar: comprobar que las copias de bases de datos, configuraciones y contenidos fueron generadas antes del compromiso y que no contienen cambios maliciosos. La restauración debe realizarse en un entorno controlado y someterse a validación técnica y de seguridad.

Recuperar el servicio de forma gradual: reincorporar los servidores únicamente después de verificar su actualización, configuración, integridad, conectividad y funcionamiento. Se



recomienda iniciar con acceso restringido, aumentar el monitoreo y habilitar progresivamente usuarios e integraciones.

Mantener vigilancia reforzada: durante el periodo posterior a la recuperación, supervisar accesos no autenticados, errores anómalos, cambios de privilegios, conexiones salientes, modificaciones de archivos y actividad administrativa. Cualquier reaparición de los indicadores debe generar una nueva contención.

Evaluar la afectación de información personal: determinar si existió consulta, modificación, pérdida, uso o acceso no autorizado a datos personales o sensibles, especialmente historias clínicas, datos de identificación, información financiera o documentos laborales.

Reportar el incidente a las autoridades competentes: ColCERT dispone de un canal oficial para reportar incidentes y vulnerabilidades. El reporte debe incluir información de contacto, sistemas afectados, direcciones IP, aplicaciones involucradas, fecha y hora, zona horaria, tipo de incidente y descripción técnica. ColCERT señala que los incidentes o vulnerabilidades pueden reportarse directamente a contacto@colcert.gov.co.

Aplicar los canales correspondientes para entidades públicas: las entidades sujetas a los lineamientos de Gobierno Digital deben gestionar y reportar los incidentes conforme a su clasificación y a los procedimientos del CSIRT Gobierno y ColCERT. El proceso oficial contempla las fases de planificación, detección, contención, erradicación, recuperación y actividades posteriores al incidente.

Reportar incidentes de datos personales a la SIC cuando corresponda: cuando el incidente implique adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento a datos personales, la entidad debe evaluar su obligación de reporte ante la Superintendencia de Industria y Comercio. La SIC establece un plazo de quince días hábiles desde que el incidente sea detectado y puesto en conocimiento del área encargada de atenderlo, utilizando el Registro Nacional de Bases de Datos o el módulo dispuesto para los responsables y encargados no obligados a registrar bases de datos.



Documentar las actividades posteriores al incidente: elaborar un informe con la línea de tiempo, causa raíz, activos afectados, información comprometida, acciones realizadas, tiempo de indisponibilidad y controles que fallaron. Los resultados deben convertirse en un plan de mejoramiento con responsables y fechas de cumplimiento.

Actualizar los planes de continuidad y recuperación: revisar los procedimientos de contingencia, comunicaciones, respaldos, restauración y operación alternativa. Cuando el incidente afecte procesos asistenciales o administrativos esenciales, debe evaluarse la activación del plan de continuidad del negocio y del plan de recuperación ante desastres.

La aplicación de la actualización de seguridad corrige la vulnerabilidad, pero no elimina accesos, cuentas, archivos o configuraciones que hayan sido establecidos antes del parcheo. Cuando no pueda demostrarse la integridad de un servidor, debe prevalecer su reconstrucción desde una fuente confiable.

Conclusiones

CVE-2026-56164 representa un riesgo relevante para las organizaciones del sector salud colombiano que utilicen versiones locales de Microsoft SharePoint Server. Aunque Microsoft la clasifica con severidad media, su inclusión en el Catálogo de Vulnerabilidades Conocidas Explotadas de CISA confirma que está siendo utilizada activamente, por lo que debe tratarse como una vulnerabilidad de atención prioritaria.

La posibilidad de que un atacante remoto y no autenticado eleve privilegios dentro de una instancia vulnerable puede afectar repositorios documentales, intranets, procesos administrativos, información contractual, datos personales y otros recursos institucionales. El impacto puede aumentar cuando SharePoint se encuentra expuesto a internet, posee



integraciones con servicios corporativos o mantiene comunicaciones amplias con otros sistemas internos.

La principal medida de reducción del riesgo es la aplicación inmediata de las actualizaciones oficiales de Microsoft en todos los servidores de la granja. Sin embargo, el parcheo no permite descartar por sí solo un compromiso previo. Las entidades que hayan mantenido servidores vulnerables expuestos deben revisar registros, cuentas, permisos, configuraciones, archivos modificados y conexiones anómalas, además de rotar las credenciales y secretos que pudieron quedar expuestos.

Para el sector salud, la atención de esta vulnerabilidad debe integrarse con los planes de continuidad operativa, protección de datos personales y gestión de incidentes. Una explotación exitosa podría afectar tanto la seguridad de la información como la disponibilidad de procesos institucionales esenciales, generar obligaciones de reporte y deteriorar la confianza de pacientes, usuarios, empleados y entidades de control.

Fuentes:



- Microsoft Security Response Center. *CVE-2026-56164: Microsoft SharePoint Server Missing Authentication for Critical Function Vulnerability*. 14 de julio de 2026. Disponible en: <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-56164>
- Cybersecurity and Infrastructure Security Agency, CISA. *CISA Adds Four Known Exploited Vulnerabilities to Catalog*. 14 de julio de 2026. Disponible en: <https://www.cisa.gov/news-events/alerts/2026/07/14/cisa-adds-four-known-exploited-vulnerabilities-catalog>



- Cybersecurity and Infrastructure Security Agency, CISA. *CISA Urges SharePoint Hardening After New Exploitations*. 14 de julio de 2026. Disponible en: <https://www.cisa.gov/news-events/alerts/2026/07/14/cisa-urges-sharepoint-hardening-after-new-exploitations>
- Cybersecurity and Infrastructure Security Agency, CISA. *Known Exploited Vulnerabilities Catalog: CVE-2026-56164*. 14 de julio de 2026. Disponible en: https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2026-56164
- National Institute of Standards and Technology, NIST. *National Vulnerability Database: CVE-2026-56164 Detail*. Publicado el 14 de julio de 2026. Disponible en: <https://nvd.nist.gov/vuln/detail/CVE-2026-56164>
- CVE Program. *CVE Record: CVE-2026-56164*. 14 de julio de 2026. Disponible en: <https://www.cve.org/CVERecord?id=CVE-2026-56164>
- Microsoft Support. *July 2026 Updates for Microsoft Office*. Julio de 2026. Disponible en: <https://support.microsoft.com/en-us/servicing/office/update/2026/5105810>
- Microsoft Support. *Description of the Security Update for SharePoint Server 2016: July 14, 2026, KB5002891*. 14 de julio de 2026. Disponible en: <https://support.microsoft.com/en-us/servicing/office/update/2026/5002891>
- Microsoft Support. *Description of the Security Update for SharePoint Server 2019: July 14, 2026, KB5002883*. 14 de julio de 2026. Disponible en: <https://support.microsoft.com/en-us/servicing/office/update/2026/5002883>
- Microsoft Support. *Description of the Security Update for SharePoint Server Subscription Edition: July 14, 2026, KB5002882*. 14 de julio de 2026. Disponible en: <https://support.microsoft.com/en-us/servicing/office/update/2026/5002882>



- Microsoft Learn. *Security Hardening for SharePoint Server*. Consultado el 16 de julio de 2026. Disponible en: <https://learn.microsoft.com/en-us/sharepoint/security-for-sharepoint-server/security-hardening>
- Microsoft Learn. *View Diagnostic Logs in SharePoint Server*. Consultado el 16 de julio de 2026. Disponible en: <https://learn.microsoft.com/en-us/sharepoint/administration/view-diagnostic-logs>
- MITRE ATT&CK. *Exploit Public-Facing Application, Technique T1190*. Consultado el 16 de julio de 2026. Disponible en: <https://attack.mitre.org/techniques/T1190/>
- MITRE ATT&CK. *Exploitation for Privilege Escalation, Technique T1068*. Consultado el 16 de julio de 2026. Disponible en: <https://attack.mitre.org/techniques/T1068/>
- Equipo de Respuesta a Emergencias Cibernéticas de Colombia, ColCERT. *Reportar un incidente*. Última actualización: 4 de noviembre de 2025. Disponible en: <https://www.colcert.gov.co/800/w3-article-198656.html>

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.

