

Alerta ID:	057
Fecha del reporte:	28/07/2026
Entidad:	Todas las entidades del ecosistema digital
Título:	CVE-2026-54121 Certighost
Herramienta de detección	N/A
Activo involucrado:	Microsoft Active Directory Certificate Services (AD CS)
Tipo de alerta:	Alerta
Nivel de riesgo:	Alto

Objetivo:

Informar a las organizaciones del sector salud en Colombia sobre la identificación de la vulnerabilidad **CVE-2026-54121**, denominada **Certighost**, asociada al servicio **Microsoft Active Directory Certificate Services (AD CS)**, que permite a un atacante con credenciales válidas dentro del dominio abusar del proceso de emisión de certificados digitales para obtener privilegios elevados y potencialmente comprometer la seguridad del dominio corporativo.

Esta vulnerabilidad podría afectar la **confidencialidad, integridad y disponibilidad** de los sistemas de información sanitarios, debido a que un compromiso de Active Directory puede permitir accesos no autorizados a servidores, aplicaciones clínicas, plataformas administrativas, sistemas de gestión hospitalaria, repositorios documentales y otros servicios críticos dependientes de la identidad corporativa.



El propósito de esta alerta es que las organizaciones del sector salud validen si cuentan con infraestructura basada en **Microsoft Active Directory Certificate Services (AD CS)**, revisen las versiones de sistemas Windows Server implementadas, verifiquen la aplicación de las actualizaciones de seguridad correspondientes, auditen las autoridades certificadoras internas, las plantillas de certificados y las solicitudes recientes de emisión de certificados, tanto en infraestructura propia como en ambientes administrados por terceros.

Descripción:

CVE-2026-54121, denominada **Certighost**, es una vulnerabilidad de seguridad asociada a **Microsoft Active Directory Certificate Services (AD CS)** que permite a un atacante con una cuenta válida dentro del dominio abusar de los mecanismos de emisión y validación de certificados digitales para obtener privilegios elevados dentro de una infraestructura Windows.

La característica principal de esta vulnerabilidad es que permite manipular el proceso de autenticación basado en certificados, logrando que un atacante pueda obtener certificados asociados a identidades privilegiadas o equipos críticos sin contar con la autorización correspondiente. Esto puede permitir la suplantación de identidades dentro del dominio, el acceso a recursos protegidos y el escalamiento de privilegios hasta comprometer componentes esenciales de Active Directory.

La explotación exitosa de **CVE-2026-54121** podría permitir a los atacantes ampliar su nivel de acceso dentro de la organización, realizar movimientos laterales, acceder a servidores internos, modificar configuraciones de seguridad y comprometer servicios que dependen del dominio corporativo. En entornos del sector salud, donde Active Directory suele integrarse con plataformas clínicas, sistemas administrativos, servidores de aplicaciones, gestión documental,



infraestructura de respaldo y controles de acceso, una explotación de esta vulnerabilidad podría afectar la disponibilidad y seguridad de servicios críticos para la operación asistencial.

Esta vulnerabilidad adquiere mayor relevancia debido a la publicación de pruebas de concepto que facilitan el análisis y desarrollo de técnicas de explotación, incrementando el riesgo para organizaciones que no hayan aplicado las actualizaciones de seguridad correspondientes o que no tengan controles adecuados sobre la emisión y administración de certificados digitales internos.

Consecuencias de la explotación

La explotación exitosa de la vulnerabilidad **CVE-2026-54121**, denominada **Certighost**, puede generar impactos críticos a nivel técnico y operativo en las organizaciones del sector salud, especialmente aquellas que utilizan infraestructura basada en **Microsoft Active Directory Certificate Services (AD CS)** para la gestión de identidades, autenticación y control de acceso. Entre las principales consecuencias se destacan:

Compromiso de identidades privilegiadas: el atacante podría obtener certificados digitales asociados a cuentas o equipos privilegiados, permitiendo suplantar identidades legítimas dentro del dominio corporativo y acceder a recursos restringidos.

Escalamiento de privilegios dentro del dominio: una cuenta con permisos limitados podría utilizar la vulnerabilidad para aumentar su nivel de acceso, llegando potencialmente al compromiso de controladores de dominio, servidores críticos y servicios empresariales.

Evasión de controles de seguridad: al utilizar mecanismos legítimos de autenticación mediante certificados digitales, las actividades maliciosas podrían confundirse con accesos



autorizados, dificultando la detección por herramientas de monitoreo, SIEM, EDR o equipos SOC.

Movimiento lateral dentro de la infraestructura: un atacante con acceso privilegiado podría desplazarse hacia otros sistemas internos, incluyendo servidores de aplicaciones, bases de datos, plataformas administrativas y servicios conectados al dominio Windows.

Acceso a información sensible: la explotación podría facilitar el acceso no autorizado a información crítica de la organización, incluyendo datos personales de pacientes, registros administrativos, información financiera, credenciales internas y documentos institucionales almacenados en sistemas corporativos.

Impacto operacional en servicios críticos: el compromiso de Active Directory puede afectar la disponibilidad y operación de sistemas dependientes de la identidad corporativa, incluyendo sistemas de información hospitalaria (SIH), plataformas de laboratorio, imágenes diagnósticas, sistemas de gestión documental, aplicaciones administrativas y servicios de autenticación de usuarios.

Riesgo regulatorio y reputacional: una posible exposición o alteración de información sensible podría generar incumplimientos relacionados con la protección de datos personales establecidos en la **Ley 1581 de 2012**, además de afectar la confianza de pacientes, usuarios y entidades reguladoras frente a la capacidad de protección de la información institucional.

Modo de explotación del ataque



La explotación de la vulnerabilidad **CVE-2026-54121**, denominada **Certighost**, puede dividirse en varias fases claramente identificables dentro de un entorno basado en **Microsoft Active Directory Certificate Services (AD CS)**:

Fase 1 – Obtención de acceso inicial al dominio:

El atacante requiere inicialmente una cuenta válida dentro del entorno Windows corporativo, la cual puede provenir de credenciales comprometidas, accesos de bajo privilegio obtenidos mediante campañas de phishing, filtraciones de información o compromisos previos de equipos internos. Esta cuenta inicial permite interactuar con los servicios de Active Directory y solicitar operaciones relacionadas con certificados digitales.

Fase 2 – Abuso del servicio de certificados:

El atacante identifica una infraestructura de **Active Directory Certificate Services (AD CS)** vulnerable y aprovecha la debilidad en los mecanismos de validación de identidad para manipular el proceso de solicitud o emisión de certificados. Mediante esta técnica puede obtener certificados asociados a identidades privilegiadas o equipos críticos sin contar con la autorización legítima correspondiente.



Fase 3 – Suplantación de identidad dentro del dominio:

Una vez obtenido un certificado válido asociado a una identidad privilegiada, el atacante puede utilizarlo para autenticarse dentro del entorno corporativo como si fuera un usuario o equipo legítimo. Debido a que la autenticación utiliza mecanismos autorizados de Windows, estas acciones pueden pasar desapercibidas para controles tradicionales basados únicamente en credenciales.

Fase 4 – Escalamiento de privilegios y persistencia:

El atacante puede utilizar la identidad comprometida para elevar sus privilegios dentro del dominio, acceder a recursos adicionales y establecer mecanismos de persistencia. Esto puede incluir acceso prolongado a servidores críticos, modificación de configuraciones de seguridad o creación de nuevas rutas de acceso dentro de la infraestructura.

Fase 5 – Operaciones sobre sistemas internos:

Con privilegios elevados dentro del dominio, el atacante puede:

- Acceder a servidores, aplicaciones corporativas y sistemas críticos conectados a Active Directory.
- Realizar movimientos laterales hacia otros equipos y servicios internos.
- Acceder o modificar información sensible almacenada en servidores institucionales.



- Manipular configuraciones de seguridad, políticas de dominio o mecanismos de autenticación.
- Comprometer sistemas dependientes del dominio Windows, incluyendo plataformas clínicas y administrativas.

Categoría	Capacidades soportadas
Gestión de identidad	Obtención y uso de certificados digitales para autenticación como una identidad legítima dentro del dominio.
Escalamiento de privilegios	Posibilidad de elevar permisos desde una cuenta inicial de bajo privilegio hasta cuentas o sistemas con mayor nivel de acceso.
Movimiento lateral	Acceso a servidores, estaciones de trabajo y aplicaciones internas mediante identidades comprometidas.
Operaciones sobre archivos	Acceso potencial a carpetas compartidas, repositorios documentales y archivos institucionales según permisos adquiridos.
Control de procesos	Posible administración de servicios internos, ejecución de acciones administrativas y modificación de configuraciones del entorno Windows.



Categoría	Capacidades soportadas
Reconocimiento interno	Identificación de servidores, usuarios, certificados, servicios y recursos del dominio para preparar ataques posteriores.

Vulnerabilidades asociadas

La vulnerabilidad **CVE-2026-54121**, denominada **Certighost**, se centra en el abuso de los mecanismos de autenticación basados en certificados dentro de **Microsoft Active Directory Certificate Services (AD CS)**. Su explotación combina debilidades relacionadas con la gestión de identidades, permisos de inscripción de certificados y validación de confianza dentro del dominio Windows, facilitando el escalamiento de privilegios y el compromiso de infraestructura corporativa.

Entre los mecanismos de riesgo asociados se incluyen:

Abuso de emisión de certificados digitales:

La vulnerabilidad permite que un atacante con acceso inicial al dominio pueda interactuar con la infraestructura AD CS y obtener certificados asociados a identidades privilegiadas, aprovechando configuraciones o validaciones insuficientes dentro del servicio de certificados.



Escalamiento de privilegios mediante certificados comprometidos:

Los certificados obtenidos de forma indebida pueden utilizarse para autenticarse como usuarios, equipos o servicios privilegiados, permitiendo superar controles tradicionales basados únicamente en usuario y contraseña.

Compromiso de Active Directory:

Al obtener una identidad con mayores privilegios dentro del dominio, el atacante puede acceder a recursos internos, modificar configuraciones, afectar políticas de seguridad y comprometer servicios dependientes del entorno Windows.

Ausencia de monitoreo sobre emisión y uso de certificados:

La falta de auditoría sobre solicitudes, aprobación y uso de certificados puede permitir que actividades maliciosas pasen desapercibidas, debido a que el acceso se realiza mediante mecanismos legítimos de autenticación.

Persistencia y movimiento lateral:

Los certificados comprometidos pueden proporcionar al atacante una vía de acceso prolongada dentro de la infraestructura, facilitando desplazamientos hacia servidores, estaciones de trabajo, aplicaciones críticas y sistemas conectados al dominio

Mapeo MITRE ATT&CK:

Táctica	Técnica / ID	Descripción en el contexto de SpankRAT
Initial Access (TA0001)	T1078	Uso de cuentas válidas del dominio como punto inicial para interactuar con servicios internos y AD CS.



Táctica	Técnica / ID	Descripción en el contexto de SpankRAT
Privilege Escalation (TA0004)	T1649	Abuso o falsificación de certificados de autenticación para obtener privilegios elevados dentro del dominio.
Credential Access (TA0006)	T1552	Obtención o uso indebido de material de autenticación asociado a certificados digitales.
Persistence (TA0003)	T1098	Mantenimiento del acceso mediante identidades privilegiadas o certificados comprometidos.
Defense Evasion (TA0005)	T1550.004	Uso de certificados de autenticación válidos para evadir controles basados en credenciales tradicionales.
Discovery (TA0007)	T1018	Identificación de equipos, servidores y recursos internos dentro del dominio comprometido.
Lateral Movement (TA0008)	T1021	Acceso a servidores, estaciones de trabajo y servicios internos utilizando identidades comprometidas.
Collection (TA0009)	T1114	Posible acceso a información almacenada en sistemas corporativos según los privilegios obtenidos.
Command and Control (TA0011)	T1071	Uso de canales legítimos de comunicación interna para mantener interacción con sistemas comprometidos.



Táctica	Técnica / ID	Descripción en el contexto de SpankRAT
Impact (TA0040)	T1489	Posible afectación de servicios críticos mediante compromiso de cuentas administrativas y sistemas dependientes del dominio.

Recomendaciones de detección y mitigación

En paralelo a las actividades de detección, se recomienda aplicar las siguientes medidas de fortalecimiento y prevención para reducir el riesgo asociado a la vulnerabilidad **CVE-2026-54121**, denominada **Certighost**, en entornos que utilizan **Microsoft Active Directory Certificate Services (AD CS)**:

1. Aplicar actualizaciones de seguridad de Microsoft:

Instalar las actualizaciones oficiales publicadas por Microsoft para los servidores Windows afectados, especialmente aquellos que ejecutan roles relacionados con **Active Directory Certificate Services (AD CS)** y controladores de dominio.

2. Identificar y proteger servidores con AD CS:

Realizar un inventario de servidores que tengan habilitado el servicio de autoridad certificadora, validando que se encuentren correctamente actualizados, monitoreados y protegidos contra accesos no autorizados.



3. Revisar permisos de emisión de certificados:

Auditar las plantillas de certificados configuradas en AD CS, limitando los permisos de inscripción únicamente a usuarios, equipos y servicios que realmente requieran esta capacidad.

4. Aplicar el principio de mínimo privilegio:

Reducir los permisos asignados a usuarios y cuentas administrativas, evitando que cuentas de bajo privilegio puedan solicitar certificados con capacidades de autenticación privilegiada.

5. Implementar autenticación multifactor (MFA):

Fortalecer los mecanismos de acceso administrativo mediante MFA, reduciendo el riesgo asociado al compromiso de credenciales utilizadas para acceder al dominio corporativo.

6. Monitorear la emisión y uso de certificados digitales:

Implementar alertas sobre solicitudes inusuales de certificados, emisiones asociadas a cuentas privilegiadas, cambios en plantillas y autenticaciones realizadas mediante certificados fuera del comportamiento esperado.

7. Fortalecer la supervisión de Active Directory:



Configurar monitoreo sobre eventos de seguridad relacionados con autenticaciones, cambios en grupos privilegiados, creación de cuentas, modificaciones de políticas y actividad anómala en controladores de dominio.

8. Implementar soluciones EDR/XDR y SIEM:

Mantener actualizadas las herramientas de detección para identificar comportamientos asociados con escalamiento de privilegios, abuso de identidades, movimientos laterales y acceso irregular a sistemas críticos.

9. Segmentar infraestructura crítica:

Limitar el acceso directo hacia controladores de dominio, servidores de certificados y sistemas sensibles, separándolos de redes generales de usuarios o dispositivos no administrados.

10. Realizar ejercicios de validación de seguridad:

Ejecutar auditorías técnicas, pruebas de penetración y ejercicios de red team orientados a evaluar la resistencia de los controles de identidad y detección frente a abuso de certificados digitales.

11. Revisar accesos de terceros y proveedores:



Validar cuentas externas, conexiones administrativas y servicios gestionados que tengan integración con Active Directory, asegurando que mantengan controles adecuados de seguridad.

Recomendaciones de prevención y mitigación

En caso de confirmar o sospechar explotación de **CVE-2026-54121**, se recomienda ejecutar el siguiente procedimiento de contención, análisis y recuperación:

- 1. Aislar sistemas potencialmente comprometidos:**
Restringir temporalmente el acceso a servidores AD CS, controladores de dominio o equipos donde se identifique actividad sospechosa, evitando la propagación del atacante dentro de la infraestructura.
- 2. Preservar evidencia técnica:**
Recolectar registros de Windows Event Logs, Active Directory, servicios de certificados, controladores de dominio, SIEM, EDR/XDR y cualquier evidencia relacionada con solicitudes o uso irregular de certificados digitales.
- 3. Revisar certificados emitidos recientemente:**
Analizar certificados generados durante el periodo de exposición, identificando aquellos asociados a usuarios, equipos o servicios que no tengan una justificación operativa.



4. **Revocar certificados sospechosos:**
Invalidar certificados emitidos de forma indebida o utilizados por identidades comprometidas, evitando que continúen siendo utilizados como mecanismo de autenticación.
5. **Restablecer credenciales comprometidas:**
Realizar cambios de contraseñas en cuentas afectadas, especialmente cuentas administrativas, cuentas de servicio y usuarios con privilegios elevados dentro del dominio.
6. **Revisar configuraciones críticas de AD CS y Active Directory:**
Validar modificaciones en plantillas de certificados, permisos de inscripción, grupos privilegiados, políticas de dominio y configuraciones de autenticación.
7. **Analizar movimientos laterales dentro de la red:**
Revisar accesos posteriores al posible compromiso, incluyendo conexiones hacia servidores clínicos, bases de datos, sistemas administrativos, plataformas hospitalarias y repositorios documentales.
8. **Evaluar afectación de sistemas críticos de salud:**
Determinar si el atacante tuvo acceso a plataformas que procesan información sensible, incluyendo historias clínicas electrónicas, sistemas de laboratorio, imágenes diagnósticas, facturación o gestión administrativa.
9. **Activar protocolos de respuesta a incidentes:**
Informar al equipo de seguridad de la información, CSIRT institucional y responsables de



cumplimiento normativo, especialmente si existe posibilidad de exposición de datos personales o información clínica.

10. Restaurar controles de seguridad:

Aplicar actualizaciones pendientes, fortalecer configuraciones de AD CS, renovar certificados comprometidos, revisar controles de acceso y validar la integridad de los sistemas afectados.

11. Ejecutar auditoría posterior al incidente:

Realizar un análisis de causa raíz para identificar fallas de configuración, brechas de monitoreo y oportunidades de mejora que reduzcan la probabilidad de futuros compromisos.

Recomendaciones de respuesta ante compromiso

- En caso de confirmarse o sospecharse explotación de **CVE-2026-54121, denominada Certighost**, se recomienda ejecutar el siguiente procedimiento de contención, análisis y erradicación:
- **Aislar sistemas relacionados con Active Directory Certificate Services (AD CS):**
Restringir temporalmente el acceso a servidores de autoridad certificadora, controladores de dominio y equipos donde se identifique actividad sospechosa, con el fin de evitar escalamiento de privilegios y movimientos laterales dentro de la infraestructura.
- **Captura de registros y artefactos clave:**
Recolectar eventos de seguridad de Windows, registros de Active Directory, logs de AD CS, controladores de dominio, plataformas SIEM/EDR/XDR y cualquier evidencia asociada



con solicitudes, emisión o uso irregular de certificados digitales para realizar análisis forense.

- **Revisión y revocación de certificados comprometidos:**

Identificar certificados emitidos de manera sospechosa, asociados a usuarios, equipos o servicios no autorizados, y proceder con su revocación para impedir que continúen siendo utilizados como mecanismo de autenticación.

- **Restablecimiento de credenciales comprometidas:**

Realizar cambio de contraseñas de usuarios afectados, especialmente cuentas administrativas, cuentas de servicio y usuarios con privilegios elevados dentro del dominio. Evaluar la renovación de credenciales asociadas a sistemas críticos.

- **Revisión de configuraciones críticas de AD CS y Active Directory:**

Validar que no existan modificaciones no autorizadas en plantillas de certificados, permisos de inscripción, grupos privilegiados, políticas de dominio, configuraciones de autenticación o parámetros de seguridad de la infraestructura Windows.

- **Monitoreo de autenticaciones y actividad de red:**

Analizar accesos recientes realizados mediante certificados, conexiones desde equipos no habituales, autenticaciones administrativas anómalas y patrones de tráfico que indiquen reconocimiento interno, persistencia o movimiento lateral.

- **Evaluación de sistemas internos potencialmente comprometidos:**

Revisar servidores, bases de datos, aplicaciones clínicas, sistemas administrativos,



plataformas de gestión hospitalaria y otros servicios dependientes del dominio Windows para determinar si fueron accedidos o modificados durante la ventana de exposición.

- **Comunicación y reporte del incidente:**

Notificar al equipo de seguridad de la información, CSIRT institucional y responsables de gestión de riesgo tecnológico. Cuando exista afectación de información personal o datos clínicos, evaluar los procesos de reporte establecidos por la normativa colombiana de protección de datos y las obligaciones regulatorias aplicables.

- **Restauración y remediación de infraestructura:**

Aplicar las actualizaciones de seguridad correspondientes, revocar certificados comprometidos, fortalecer controles de emisión de certificados, restablecer configuraciones seguras y validar la integridad de los sistemas afectados antes de devolverlos a operación normal.

- **Auditoría posterior al incidente:**

Realizar un análisis de causa raíz para determinar cómo ocurrió el compromiso, identificar controles insuficientes, revisar la efectividad de las medidas implementadas y fortalecer la estrategia de seguridad para prevenir futuras explotaciones relacionadas con identidad digital.

Conclusiones



La vulnerabilidad **CVE-2026-54121**, denominada **Certighost**, representa una amenaza relevante para las organizaciones del sector salud debido a su impacto potencial sobre la infraestructura de identidad basada en **Microsoft Active Directory Certificate Services (AD CS)**, componente utilizado ampliamente para gestionar autenticación, certificados digitales y control de acceso dentro de redes corporativas.

A diferencia de vulnerabilidades orientadas únicamente a la explotación directa de servicios expuestos a Internet, esta amenaza afecta uno de los componentes más críticos de los entornos Windows empresariales: la confianza digital. Un atacante que logre aprovechar esta condición puede utilizar mecanismos legítimos de autenticación mediante certificados para ocultar su actividad y obtener acceso progresivo a recursos internos.

El compromiso exitoso de la infraestructura AD CS puede facilitar el escalamiento de privilegios, la suplantación de identidades, el movimiento lateral dentro de la red y el acceso a sistemas críticos como plataformas de historia clínica electrónica, servidores de aplicaciones, bases de datos clínicas, sistemas administrativos, repositorios documentales y servicios tecnológicos esenciales para la operación hospitalaria.

Adicionalmente, configuraciones inseguras de autoridades certificadoras, permisos excesivos para solicitar certificados, ausencia de monitoreo sobre emisión de certificados y controles insuficientes de identidad incrementan significativamente la posibilidad de que un atacante mantenga persistencia dentro del entorno corporativo sin ser detectado oportunamente.

En este contexto, la protección de los servicios de identidad y autenticación se convierte en un elemento fundamental para la seguridad tecnológica del sector salud. La gestión adecuada de privilegios, la administración segura de certificados digitales, el monitoreo continuo de Active Directory y la aplicación oportuna de actualizaciones de seguridad son controles esenciales para reducir el riesgo.



Finalmente, se concluye que la mitigación efectiva de **CVE-2026-54121** no depende únicamente de la instalación del parche correspondiente, sino de una estrategia integral de seguridad basada en la protección de identidades, la reducción de privilegios, la auditoría permanente de certificados y la capacidad de detectar comportamientos anómalos dentro del dominio corporativo.

Fuentes:



- Microsoft Security Response Center (MSRC) – Security Update Guide: Boletín oficial de Microsoft con información técnica, productos afectados y actualizaciones de seguridad relacionadas con CVE-2026-54121 en componentes de Windows y Active Directory Certificate Services (AD CS). Disponible en: <https://msrc.microsoft.com/update-guide>
- CISA – Known Exploited Vulnerabilities Catalog: Catálogo oficial de vulnerabilidades explotadas activamente, utilizado para validar el nivel de riesgo y prioridad de remediación de vulnerabilidades con evidencia de explotación en entornos reales. Disponible en: <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>
- Microsoft Security Blog – Active Directory Certificate Services Security Guidance: Documentación técnica y recomendaciones de Microsoft relacionadas con la protección de Active Directory Certificate Services, gestión de certificados digitales y fortalecimiento de controles de identidad. Disponible en: <https://www.microsoft.com/security/blog/>
- National Vulnerability Database (NVD) – CVE-2026-54121: Registro público de vulnerabilidades con información técnica, clasificación de severidad, productos afectados y referencias asociadas a la vulnerabilidad Certighost. Disponible en: <https://nvd.nist.gov/>





Boletín informativo Vulnerabilidad Microsoft Active Directory Certificate Services (AD CS)

CSIRTSALUD-AV- 20260728-57

TLP: CLEAR

- BleepingComputer – Certighost CVE-2026-54121 Public Exploit Analysis:
Análisis de la publicación de pruebas de concepto, impacto potencial y riesgo asociado al abuso de Active
Directory Certificate Services. Disponible en:
<https://www.bleepingcomputer.com/news/security/>
- MITRE ATT&CK Framework for Enterprise:
Referencia de tácticas y técnicas asociadas con abuso de certificados, escalamiento de privilegios,
movimiento lateral y compromiso de identidades dentro de entornos Windows corporativos. Disponible
en:
<https://attack.mitre.org/>

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.

