Como Investigar un Presunto Acceso No Autorizado con AnyDesk

TABLA DE CONTENIDO

- Por qué AnyDesk es una plataforma segura
  - Cifrado de extremo a extremo verificable
  - Identidad criptográfica de cada dispositivo
  - Control de acceso por diseño
  - Registro y auditoría integrados
- Escenarios en los que AnyDesk puede ser usado maliciosamente
  - Ingeniería social y usuario engañado
  - Configuración incorrecta o débil
  - Credenciales o tokens robados
  - Movimiento lateral dentro de la red
  - Abuso del acceso no atendido y persistencia
  - Sesión oculta mediante modo privacidad
- Cómo investigar un presunto acceso no autorizado
  - Paso 1: Contener la amenaza
  - Paso 2: Preservar la evidencia
  - Paso 3: Reconstruir la línea de tiempo con los registros
  - Paso 4: Determinar el alcance
  - Paso 5: Remediar y endurecer la configuración
  - Paso 6: Reportar
- Buenas prácticas para prevenir el próximo incidente
- Aviso legal

Articulo elaborado por el equipo de investigaciones de remotedesktop.mx.

Sospechar que alguien accedió a un equipo sin autorización es una situación seria, pero también es un escenario para el que AnyDesk está mejor preparado que la mayoría de las herramientas de escritorio remoto. La plataforma registra cada conexión en varios niveles —en el cliente local, en el portal de gestión y, opcionalmente, en grabaciones de sesión— lo que permite reconstruir con precisión qué ocurrió, cuándo y desde dónde.

En esta guía explicamos primero por qué AnyDesk es intrínsecamente seguro, luego los escenarios realistas en los que un acceso puede considerarse no autorizado, y finalmente un procedimiento de investigación paso a paso basado en las capacidades y los registros que la propia herramienta genera.

Por qué AnyDesk es una plataforma segura

Antes de hablar de incidentes conviene entender la arquitectura de seguridad, porque define qué puede y qué no puede ocurrir técnicamente.

Cifrado de extremo a extremo verificable

Todas las sesiones de AnyDesk se establecen sobre **TLS 1.2 con cifrado AEAD** (Authenticated Encryption with Associated Data). Esto significa que el contenido de la sesión —imagen, teclado, ratón, portapapeles y archivos transferidos— viaja cifrado y autenticado entre los dos extremos. No es posible interceptar el tráfico en tránsito para ver o modificar la sesión.

Además, el tipo de conexión, el modo de cifrado aplicado y el estado de verificación del cliente son visibles en tiempo real desde el icono de información de conexión en la barra de herramientas de la sesión. No hay que confiar en que el cifrado “está activo”: se puede comprobar.

Identidad criptográfica de cada dispositivo

Cada instalación de AnyDesk genera un **certificado RSA autofirmado y una clave privada única** en el dispositivo. De ese certificado se deriva un **fingerprint** (huella digital) que queda vinculado de forma permanente al AnyDesk-ID. En cada conexión, los servidores de AnyDesk verifican el certificado antes de asociarlo al ID.

La consecuencia práctica es importante: **nadie puede suplantar un AnyDesk-ID sin poseer la clave privada del dispositivo legítimo**. Si un ID muestra un fingerprint distinto al esperado, es una señal de alarma inmediata. El fingerprint se puede consultar en *Settings* > *About AnyDesk* > *Security* > *Fingerprint*, en la ventana de aceptación de conexión y en la barra de herramientas de sesión.

Control de acceso por diseño

AnyDesk no permite el acceso “porque sí”. Toda conexión entrante pasa por uno de estos controles:

- **Aceptación manual**: por defecto, cada solicitud de sesión muestra una ventana de aceptación que una persona debe aprobar o rechazar en el dispositivo remoto.
- **Acceso no atendido con contraseña**: solo quien conoce la contraseña puede conectar sin aprobación. Las contraseñas se almacenan con **hash con sal** (salted hashing), nunca en texto plano.
- **Autenticación de dos factores (2FA)**: el acceso no atendido puede exigir además un código de 6 dígitos de una app autenticadora.
- **Lista de Control de Acceso (ACL)**: permite definir qué AnyDesk-IDs o alias pueden siquiera iniciar una conexión. Soporta comodines como `*@tuempresa` para restringir a un namespace corporativo.
- **Perfiles de permisos**: determinan qué puede hacer quien se conecta —ver pantalla, controlar teclado y ratón, transferir archivos, usar el portapapeles, crear túneles TCP, activar el modo privacidad, etc.

Registro y auditoría integrados

A diferencia de muchas herramientas, AnyDesk genera evidencia de forma nativa: un archivo local `connection_trace.txt` por cada solicitud entrante, archivos de traza por sesión, un historial de sesiones centralizado en my.anydesk II, registros de actividad administrativa y grabaciones de sesión opcionales. Esta telemetría es la base de cualquier investigación.

Escenarios en los que AnyDesk puede ser usado maliciosamente

Que la herramienta sea segura no significa que no pueda ser mal utilizada. La gran mayoría de los accesos no autorizados con AnyDesk no explotan una vulnerabilidad del software, sino que abusan de la confianza del usuario o de una configuración débil. Estos son los escenarios más frecuentes.

Ingeniería social y usuario engañado

Es el vector más común. Un atacante se hace pasar por soporte técnico de Microsoft, del banco, de la empresa o incluso del propio AnyDesk, y convence a la víctima de que instale AnyDesk y le entregue su ID o acepte la conexión. Una vez dentro, el atacante opera con los mismos permisos que tendría un técnico legítimo.

AnyDesk es explícito al respecto: **ninguna empresa legítima llama sin que tú lo hayas solicitado, y AnyDesk nunca pide tu contraseña ni inicia contacto**. Si la conexión fue aceptada manualmente por el usuario engañado, el registro lo mostrará como una sesión aceptada —no como una intrusión técnica.

Configuración incorrecta o débil

Un acceso no autorizado puede ser consecuencia directa de una mala configuración:

- **Contraseña de acceso no atendido débil** o reutilizada, que un atacante adivina o conoce.
- **Acceso no atendido habilitado sin 2FA** en un dispositivo expuesto.
- **ACL vacía o demasiado permisiva**, que permite conexiones desde cualquier ID.
- **Perfil de permisos "Full Access"** asignado por defecto, que da control total a quien conecta.
- **Tokens de inicio de sesión guardados** en un dispositivo que luego se compromete.
- **Versión portable o desactualizada**, sin las protecciones del servicio instalado.

Credenciales o tokens robados

Si un atacante obtiene la contraseña de acceso no atendido (por phishing, por estar anotada, por reutilización tras una filtración) o un token de inicio de sesión guardado, puede conectar sin que nadie acepte nada. En los registros aparecerá como una autenticación válida —la diferencia está en *quién* se conectó y *desde dónde*.

Movimiento lateral dentro de la red

En un entorno corporativo, un atacante que ya comprometió un equipo puede usar AnyDesk —o instalarlo— para moverse lateralmente a otros equipos de la organización, especialmente si se reutilizan contraseñas de acceso no atendido o si el namespace/ACL no está restringido. AnyDesk instalado como servicio y con inicio automático facilita la persistencia.

Abuso del acceso no atendido y persistencia

Un insider o un atacante con acceso físico momentáneo puede habilitar el acceso no atendido, establecer su propia contraseña o guardar un token, y luego volver a conectar cuando quiera sin que el usuario lo note. También puede crear un cliente personalizado (custom client) con acceso preconfigurado.

Sesión oculta mediante modo privacidad

El modo privacidad (Screen Privacy) oscurece la pantalla del dispositivo remoto y bloquea la entrada local. Es una función legítima para trabajar con datos confidenciales, pero si un atacante la activa, el

usuario frente al equipo no ve lo que el intruso está haciendo. Requiere que el perfil de permisos lo permita —otra razón para revisar los permisos concedidos.

Cómo investigar un presunto acceso no autorizado

La investigación debe seguir un orden: **contener, preservar evidencia, analizar, determinar alcance y remediar**. No borres nada ni desinstales AnyDesk antes de recopilar los registros — destruirías la evidencia principal.

Paso 1: Contener la amenaza

Si sospechas que hay una sesión activa o que el acceso sigue abierto:

1. **Cierra la sesión activa** desde el cliente o desde my.anydesk II: en la pestaña *Sessions*, filtra por estado *Open*, selecciona la sesión y pulsa **Close Session**. El dispositivo local mostrará que la sesión fue cerrada por el administrador.
2. **Bloquea nuevas conexiones** temporalmente: configura la ACL para permitir solo tus IDs de confianza, o desactiva el acceso no atendido mientras investigas.
3. **Cambia la contraseña de acceso no atendido** y selecciona **Clear all tokens** para invalidar todos los tokens de inicio de sesión guardados. Cambiar la contraseña invalida automáticamente todos los tokens emitidos.
4. Si el compromiso es serio, **desconecta el equipo de la red** (no lo apagues) para preservar el estado y la evidencia volátil.

Paso 2: Preservar la evidencia

Antes de analizar, copia los registros a una ubicación segura. AnyDesk genera varias fuentes de evidencia:

- **`connection_trace.txt`**: el registro local de conexiones entrantes. Está en la misma carpeta que los archivos de configuración del cliente (en Windows, `%appdata%\AnyDesk\`). Registra la fecha y hora de cada solicitud, si fue aceptada o rechazada, y quién la envió.
- **Archivos de traza `ad.trace` y `ad_svc.trace`**: se generan en cada sesión y contienen diagnóstico detallado. En Windows están en `%appdata%\AnyDesk\ad.trace` (interfaz) y `%programdata%\AnyDesk\ad_svc.trace` (servicio, solo si está instalado). En macOS/Linux instalado: `/var/log/anydesk.trace`.
- **Historial de sesiones en my.anydesk II**: exporta o documenta la pestaña *Sessions*.
- **Grabaciones de sesión** (`.anydesk`): si la grabación estaba activada, son la evidencia más directa de lo que ocurrió.

- **Registros de actividad** (Activity Logs, licencia Ultimate Cloud): cambios en usuarios, roles, grupos, permission sets y custom clients.

> **Cadena de custodia:** copia los archivos sin modificarlos, anota la fecha/hora del sistema y conserva los originales. Si el incidente puede derivar en acción legal, trabaja sobre copias y documenta cada paso.

Paso 3: Reconstruir la línea de tiempo con los registros

3.1 Revisar `connection_trace.txt`

Es la primera fuente. Cada solicitud de conexión entrante queda registrada con:

- **Fecha y hora exacta** de la solicitud.
- **Cómo se resolvió**: aceptada manualmente, aceptada por acceso no atendido o rechazada.
- **Quién la envió**: el AnyDesk-ID/alias del cliente que inició la conexión.

Esto responde de inmediato a la pregunta clave: **¿la sesión fue aceptada por una persona o entró por contraseña?** Si fue aceptada manualmente, el vector probable es ingeniería social o un insider. Si entró por acceso no atendido, el vector es una contraseña/token comprometido o una configuración débil.

3.2 Consultar el historial de sesiones en my.anydesk II

En el portal my.anydesk II, la pestaña **Sessions** muestra todas las sesiones entre clientes con:

- **Source address**: el AnyDesk-ID que inició la sesión.
- **Destination address**: el dispositivo que la recibió.
- **State**: estado de la sesión (Open, Closed, Error, Unknown).
- **Start time / End time**: inicio y fin exactos, que permiten calcular la duración.

Filtra por el dispositivo afectado y busca sesiones que no reconozcas: horarios fuera de lo habitual, IDs de origen desconocidos, duraciones anómalas o sesiones que coincidan con el momento del incidente. El detalle de cada sesión muestra además la duración y el estado de licencia de ambos extremos.

3.3 Analizar los archivos de traza

Los `ad.trace` y `ad_svc.trace` contienen el detalle técnico de cada sesión: establecimiento de la conexión, autenticación, parámetros negociados y eventos durante la sesión. Sirven para confirmar el método de autenticación usado y correlacionar eventos. Si necesitas ayuda para interpretarlos,

puedes adjuntarlos a un ticket de soporte de AnyDesk desde *Settings* > *About AnyDesk* > *Send Support Information*.

3.4 Revisar las grabaciones de sesión

Si la grabación automática estaba habilitada (*Settings* > *Recording*), cada sesión genera un archivo `.anydesk` con el nombre en formato `<incoming/outgoing> <nombre_otro> (<ID_otro>)-<nombre_tuyo> (<ID_tuyo>).anydesk`. Se reproducen con el propio cliente AnyDesk (Session Player) y muestran **exactamente lo que el intruso hizo**: qué abrió, qué escribió, qué archivos tocó. Es la evidencia más concluyente para determinar el impacto.

> **Nota:** si AnyDesk está instalado, el nombre del cliente en el archivo aparece como `SYSTEM`, porque es el usuario SYSTEM quien inicia el servicio.

3.5 Revisar los Activity Logs (Ultimate Cloud)

Si tu organización tiene licencia Ultimate Cloud, los **Activity Logs** en *User Management* > *Activity Log* registran quién hizo qué y cuándo en la administración: creación/edición/eliminación de usuarios, grupos, roles, permission sets y custom clients, incluidos los cambios hechos por la REST API. Esto es clave para detectar si el atacante creó un usuario, modificó permisos o generó un custom client para persistencia. Soportan búsqueda, filtros por usuario/acción/plataforma, rango de fechas y exportación a CSV.

Paso 4: Determinar el alcance

Una vez identificada la sesión no autorizada, determina qué tan lejos llegó:

- **¿Qué hizo el intruso?** Revisa la grabación de sesión, el historial de archivos transferidos y los artefactos del sistema operativo (archivos recientes, programas instalados, logs de Windows).
- **¿A qué otros equipos pudo llegar?** Si reutilizabas la contraseña de acceso no atendido o el namespace era amplio, asume movimiento lateral y revisa las sesiones de *todos* los dispositivos en my.anydesk II.
- **¿Dejó persistencia?** Busca nuevos usuarios, custom clients, tokens guardados, cambios en permission sets o en la ACL, y AnyDesk configurado para inicio automático.
- **¿Qué credenciales pudo ver?** Si accedió a gestores de contraseñas, correo o documentos, considera comprometidas esas credenciales y rótalas.

Correlaciona los tiempos de AnyDesk con los **registros del sistema operativo** (Event Viewer en Windows: inicios de sesión, creación de procesos, instalación de servicios) para tener una imagen completa.

Paso 5: Remediar y endurecer la configuración

Tras entender el vector, ciérralo:

- **Contraseñas**: cambia la de acceso no atendido por una de 12+ caracteres y activa **2FA**. Rota cualquier credencial que el intruso pudo ver.
- **Tokens**: usa **Clear all tokens** para revocar todos los inicios de sesión guardados.
- **ACL**: restringe las conexiones entrantes a IDs/alias conocidos o a tu namespace (`*@tuempresa`). Es la defensa más efectiva: aunque alguien conozca la contraseña, no podrá conectar si no está en la lista.
- **Perfiles de permisos**: asigna el mínimo privilegio. No uses “Full Access” por defecto; desactiva transferencia de archivos, túneles TCP y modo privacidad si no se necesitan.
- **Acceso interactivo**: si el dispositivo no debe recibir solicitudes manuales, configura *Interactive Access* en *Never show incoming session requests* para que solo entre por acceso no atendido autenticado.
- **Grabación de sesiones**: activa la grabación automática de sesiones entrantes para tener evidencia futura.
- **Actualización**: instala la última versión de AnyDesk y úsala como servicio instalado, no portable.
- **Offboarding**: si el origen fue un exempleado, elimina su cliente del portal, resetea la clave de licencia, cambia las contraseñas que conocía y bloquéalo en la ACL.

Paso 6: Reportar

- **A AnyDesk**: reporta el abuso a través del portal de soporte. AnyDesk coopera con las autoridades y bana a los usuarios que violan los términos de uso.
- **A las autoridades**: si hubo fraude, robo o acceso ilegítimo, conserva toda la evidencia (connection_trace, sesiones, grabaciones) y repórtalo a la autoridad competente. Los registros de AnyDesk con fecha, hora e ID de origen son evidencia útil.

Buenas prácticas para prevenir el próximo incidente

- **Nunca compartas tu AnyDesk-ID ni aceptes conexiones** de quien te contacte sin que tú lo hayas iniciado. Ninguna empresa legítima hace cold calling.
- **Verifica el fingerprint** cuando conectes o aceptes: si no coincide con el esperado, no continúes.
- **Contraseña fuerte + 2FA** en todo acceso no atendido.
- **ACL restrictiva** limitada a tu namespace o IDs de confianza.
- **Mínimo privilegio** en los perfiles de permisos.

- **Revisa periódicamente** la pestaña Sessions de my.anydesk II para detectar conexiones que no reconoces.
- **Activa la grabación de sesiones** en equipos sensibles.

Si quieres reducir la probabilidad de llegar a este escenario, aplica las medidas de nuestra guia de hardening de AnyDesk para empresas.

Aviso legal

Esta guía tiene fines informativos y de buenas prácticas. No constituye asesoría legal ni forense profesional. En caso de un incidente de seguridad real —especialmente si involucra datos personales, fraude o acceso ilegítimo— consulta con un profesional de respuesta a incidentes y con las autoridades competentes. AnyDesk es una marca registrada de AnyDesk Software GmbH.

¿Quieres revisar la seguridad de tu despliegue de AnyDesk? Descarga la última versión desde anydesk.com/es/downloads y aplica las medidas de endurecimiento de esta guía.