

Instalación y desinstalación manual

En esta entrada se mostrará cómo realizar una instalación manual del agente en un PC, así como su actualización y desinstalación.

- [Requisitos previos](#)
- [Video con todos los pasos](#)
- [Instalación del agente](#)
- [Verificación de la instalación](#)
- [Reinicio del PC](#)
- [Revisión de instalación con PowerShell](#)
- [Archivos que crea el agente](#)
- [Base de datos del agente](#)
- [Entradas de registro de Windows](#)
- [Aparición en programas instalados](#)
- [Monitoreo del agente](#)
- [Inicio del agente](#)
- [Actualización del agente](#)
- [Verificación de la actualización](#)
- [PowerShell para verificar actualización](#)
- [Actualización en listado de Aplicaciones](#)
- [Desinstalación del agente](#)
- [Verificación de la desinstalación](#)

Requisitos previos

Antes de ejecutar de **manera manual** un procedimiento de instalación, actualización o desinstalación del agente es importante tener en cuenta los siguientes requisitos previos:

Debe contar con la capacidad de realizar acciones administrativas en el PC debido a que se debe abrir la consola MS-DOS en el equipo del usuario con privilegios de administrador.

Encuentre la manera de tener acceso al PC del usuario, ya sea de forma presencial (física) o de forma remota. Que la instalación sea manual no quiere decir que necesariamente requiera de una presencia física en el computador.

En la instalación manual no se requiere que el PC o el usuario pertenezcan a un dominio o que tengan un agente instalado SCCM u otro. Se puede llevar a cabo la instalación incluso en equipos con versiones de sistema operativo Home.

Debe copiar o descargar el agente de The Fraud Explorer (normalmente llamado **endpointInstaller.msi**) al PC para que se pueda llevar a cabo su instalación. Para esta instalación manual, se debe descargar de forma manual el MSI del agente de The Fraud Explorer al computador. Puede descargar el agente a través de una carpeta compartida en Onedrive o incluso accediendo a una ruta de red donde tenga el MSI compartido.

El agente de The Fraud Explorer es compatible con sistemas operativos Windows de 32 y 64 bits, desde Windows 7 en adelante, sin embargo, nuestro agente requiere que el **Framework .NET 4.8** de Microsoft esté previamente instalado en los PC donde se llevará a cabo el despliegue. El Framework .NET viene por defecto instalado en Windows y si el sistema operativo cuenta con los últimos parches es altamente probable que este requisito se cumpla de forma automática y no deba realizar nada. El único escenario donde debería instalarlo manualmente es en caso de que los sistemas operativos no estén actualizados. Puede ejecutar el siguiente comando en una consola PowerShell para saber qué versión se encuentra instalada:

```
reg query "HKLM\SOFTWARE\Microsoft\Net Framework Setup\NDP\v4\Full" /v Release
```

Si se cumplen estos requisitos, estamos listos para continuar con la aplicación de los procedimientos.

The Fraud Explorer es un software que junto con **FraudGPT** detecta el fraude y la corrupción en las organizaciones.

Video con todos los pasos

En vez de seguir los pasos documentados, también puede optar por visualizar este video.

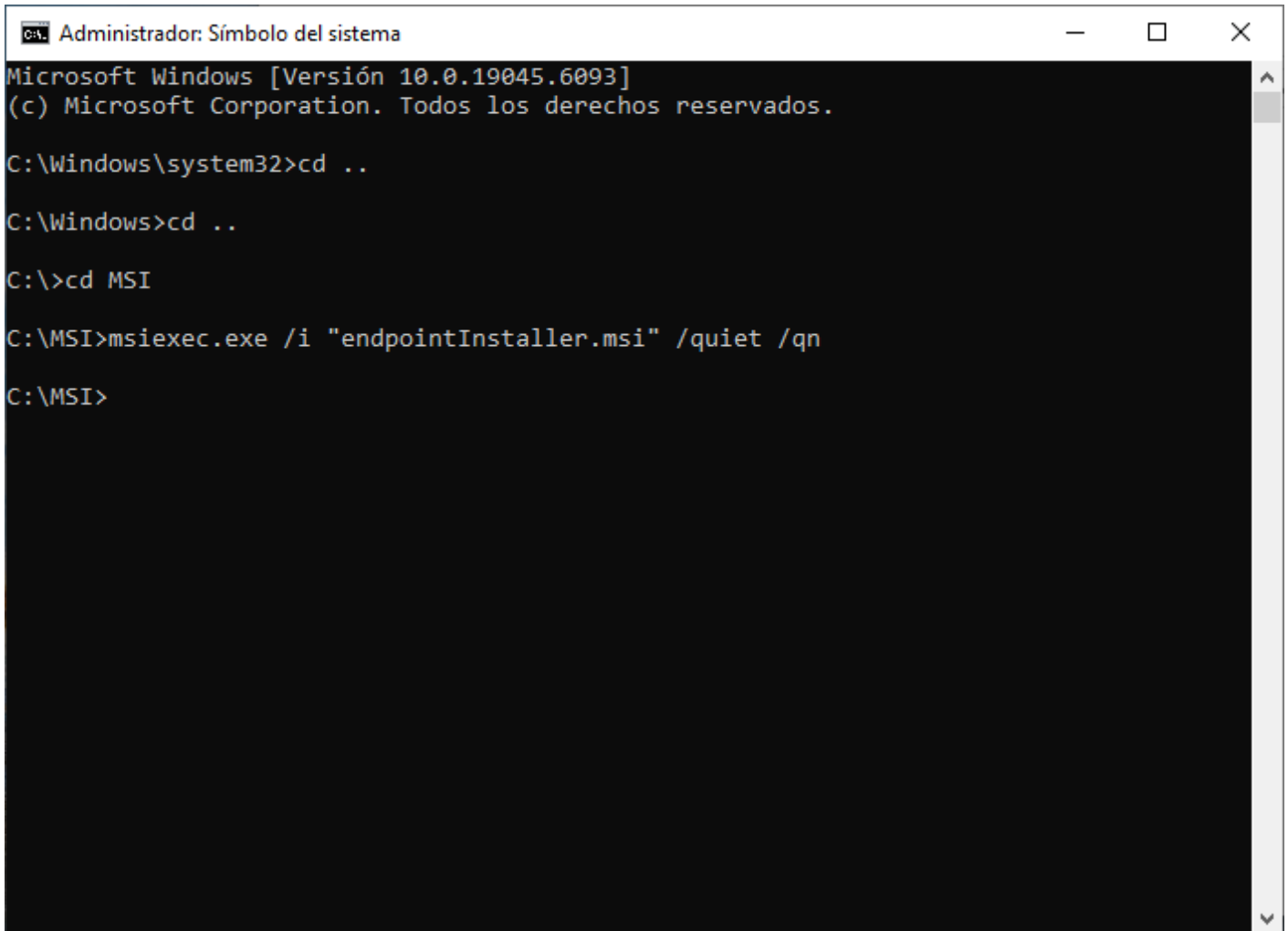
<https://www.youtube.com/embed/87HNEWn-4Ts?si=YyKvfKAHeRWmqj6g>

El video contiene todos los pasos de la guía ejecutados de forma práctica y cada uno de los pasos está separado por capítulos.

The Fraud Explorer es un software que junto con **FraudGPT** detecta el fraude y la corrupción en las organizaciones.

Instalación del agente

Abra una consola **MS-DOS** en modo administrador. Estos comandos no funcionan en una consola **MS-DOS** que no se abra en modo administrador.



```
Administrador: Símbolo del sistema
Microsoft Windows [Versión 10.0.19045.6093]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Windows\system32>cd ..

C:\Windows>cd ..

C:\>cd MSI

C:\MSI>msiexec.exe /i "endpointInstaller.msi" /quiet /qn

C:\MSI>
```

Vaya a la ruta donde ha descargado el MSI del agente de The Fraud Explorer y ejecute el siguiente comando:

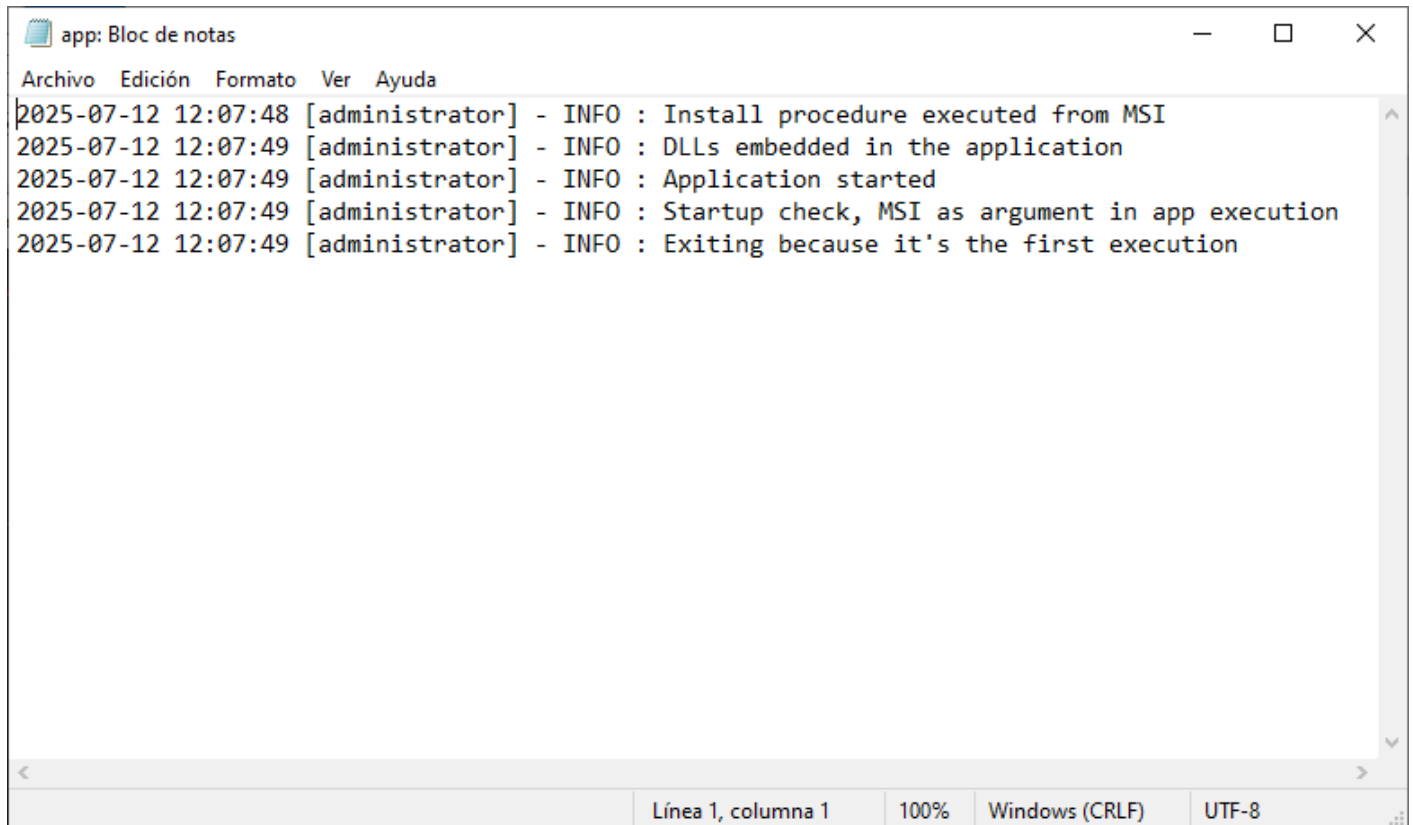
```
msiexec.exe /i "endpointInstaller.exe" /quiet /qn
```

Este comando instalará de manera silenciosa el agente en el computador del usuario.

The Fraud Explorer es un software que junto con **FraudGPT** detecta el fraude y la corrupción en las organizaciones.

Verificación de la instalación

El instalador crea sus archivos en la carpeta **C:\ProgramData\Software** y allí se encuentra un archivo de log llamado **app.log**. Si lo abre deberá ver este tipo de entradas donde se indica que el usuario administrador acaba de realizar la instalación del agente.



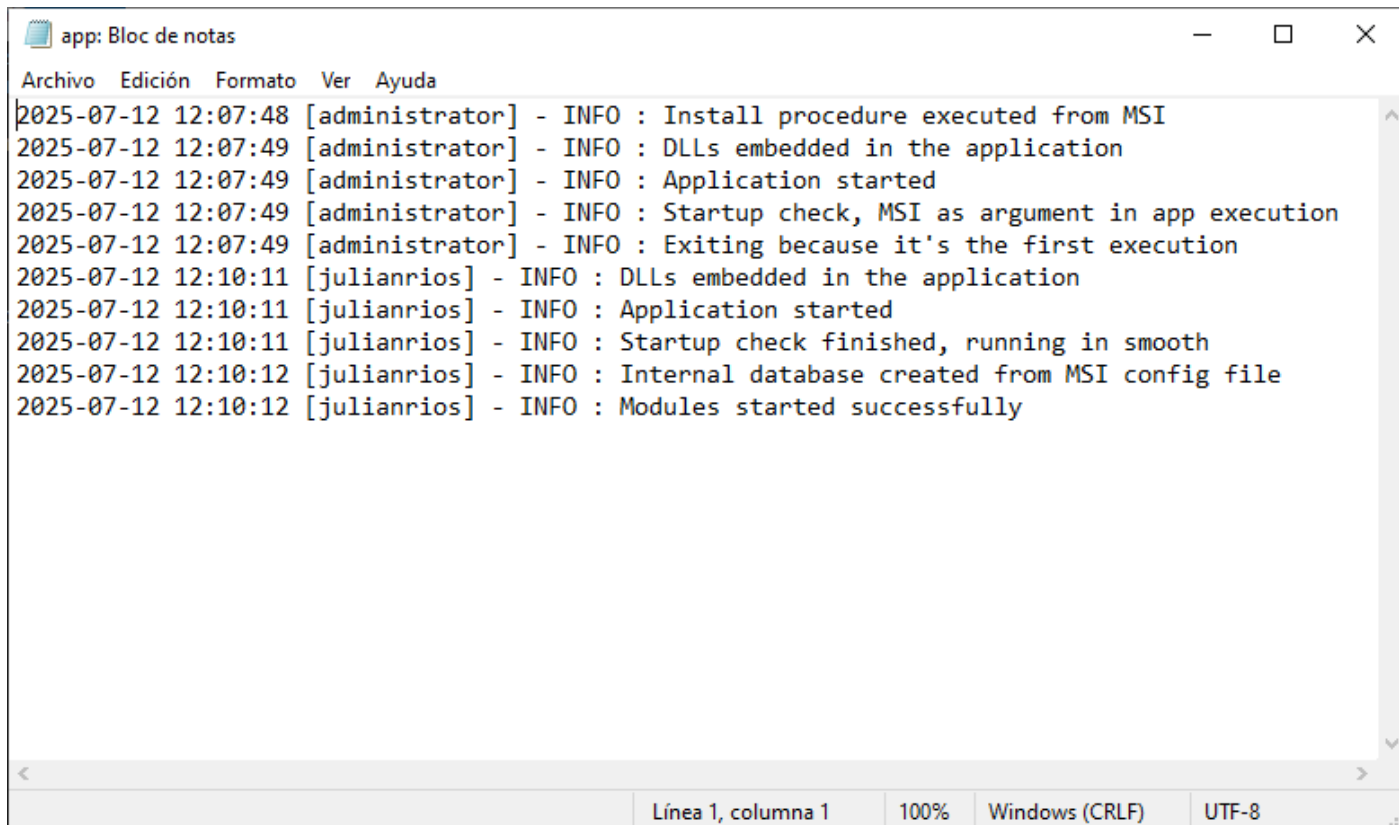
```
app: Bloc de notas
Archivo  Edición  Formato  Ver  Ayuda
2025-07-12 12:07:48 [administrator] - INFO : Install procedure executed from MSI
2025-07-12 12:07:49 [administrator] - INFO : DLLs embedded in the application
2025-07-12 12:07:49 [administrator] - INFO : Application started
2025-07-12 12:07:49 [administrator] - INFO : Startup check, MSI as argument in app execution
2025-07-12 12:07:49 [administrator] - INFO : Exiting because it's the first execution
Línea 1, columna 1  100%  Windows (CRLF)  UTF-8
```

El agente solo usa el usuario **administrador** para instalar el aplicativo, no para correrlo.

The Fraud Explorer es un software que junto con **FraudGPT** detecta el fraude y la corrupción en las organizaciones.

Reinicio del PC

Cuando se reinicia el PC, el agente arranca con los permisos del usuario restringido, como se observa en el archivo **C:\ProgramData\Software\app.log**.



```
app: Bloc de notas
Archivo Edición Formato Ver Ayuda
2025-07-12 12:07:48 [administrator] - INFO : Install procedure executed from MSI
2025-07-12 12:07:49 [administrator] - INFO : DLLs embedded in the application
2025-07-12 12:07:49 [administrator] - INFO : Application started
2025-07-12 12:07:49 [administrator] - INFO : Startup check, MSI as argument in app execution
2025-07-12 12:07:49 [administrator] - INFO : Exiting because it's the first execution
2025-07-12 12:10:11 [julianrios] - INFO : DLLs embedded in the application
2025-07-12 12:10:11 [julianrios] - INFO : Application started
2025-07-12 12:10:11 [julianrios] - INFO : Startup check finished, running in smooth
2025-07-12 12:10:12 [julianrios] - INFO : Internal database created from MSI config file
2025-07-12 12:10:12 [julianrios] - INFO : Modules started successfully
Línea 1, columna 1 100% Windows (CRLF) UTF-8
```

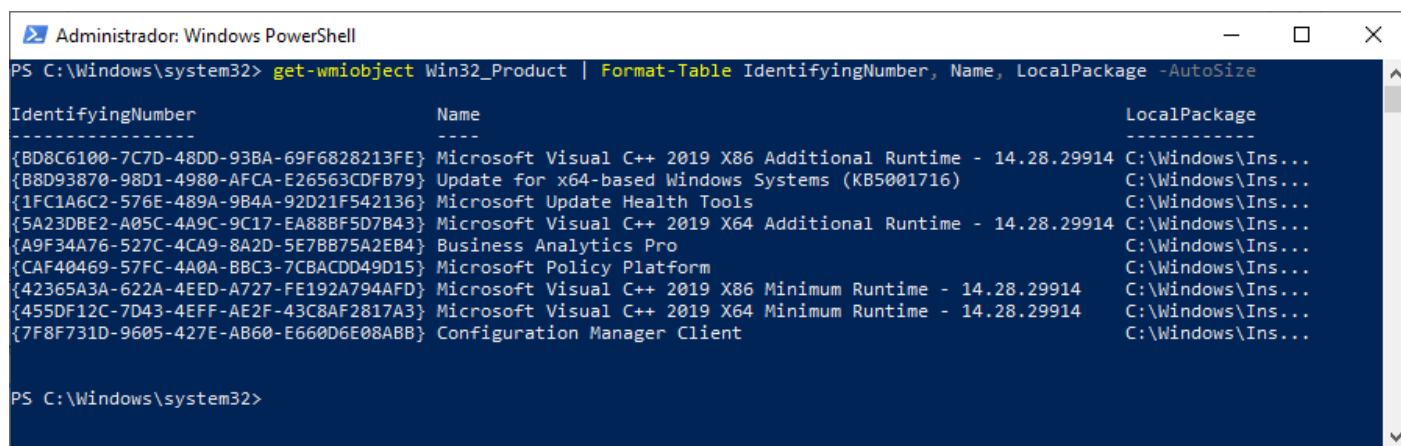
En este archivo de log se encontrará toda información relevante de inicio, parada, actualización, desinstalación e incluso errores que pueda presentar el agente durante su ejecución.

The Fraud Explorer es un software que junto con **FraudGPT** detecta el fraude y la corrupción en las organizaciones.

Revisión de instalación con PowerShell

Puede ejecutar este comando en una consola de **PowerShell** para obtener mayor información sobre el producto instalado:

```
wmi-object Win32-Product | Format-Table IdentifyingNumber, Name, LocalPackage -AutoSize
```



```
Administrador: Windows PowerShell
PS C:\Windows\system32> get-wmiobject Win32_Product | Format-Table IdentifyingNumber, Name, LocalPackage -AutoSize

IdentifyingNumber      Name                                     LocalPackage
-----
{BD8C6100-7C7D-48DD-93BA-69F6828213FE} Microsoft Visual C++ 2019 X86 Additional Runtime - 14.28.29914 C:\Windows\Ins...
{B8D93870-98D1-4980-AFCA-E26563CDFB79} Update for x64-based Windows Systems (KB5001716) C:\Windows\Ins...
{1FC1A6C2-576E-489A-9B4A-92D21F542136} Microsoft Update Health Tools C:\Windows\Ins...
{5A23DBE2-A05C-4A9C-9C17-EA88BF5D7B43} Microsoft Visual C++ 2019 X64 Additional Runtime - 14.28.29914 C:\Windows\Ins...
{A9F34A76-527C-4CA9-8A2D-5E7BB75A2EB4} Business Analytics Pro C:\Windows\Ins...
{CAF40469-57FC-4A0A-BBC3-7CBACDD49D15} Microsoft Policy Platform C:\Windows\Ins...
{42365A3A-622A-4EED-A727-FE192A794AFD} Microsoft Visual C++ 2019 X86 Minimum Runtime - 14.28.29914 C:\Windows\Ins...
{455DF12C-7D43-4EFF-AE2F-43C8AF2817A3} Microsoft Visual C++ 2019 X64 Minimum Runtime - 14.28.29914 C:\Windows\Ins...
{7F8F731D-9605-427E-AB60-E660D6E08ABB} Configuration Manager Client C:\Windows\Ins...

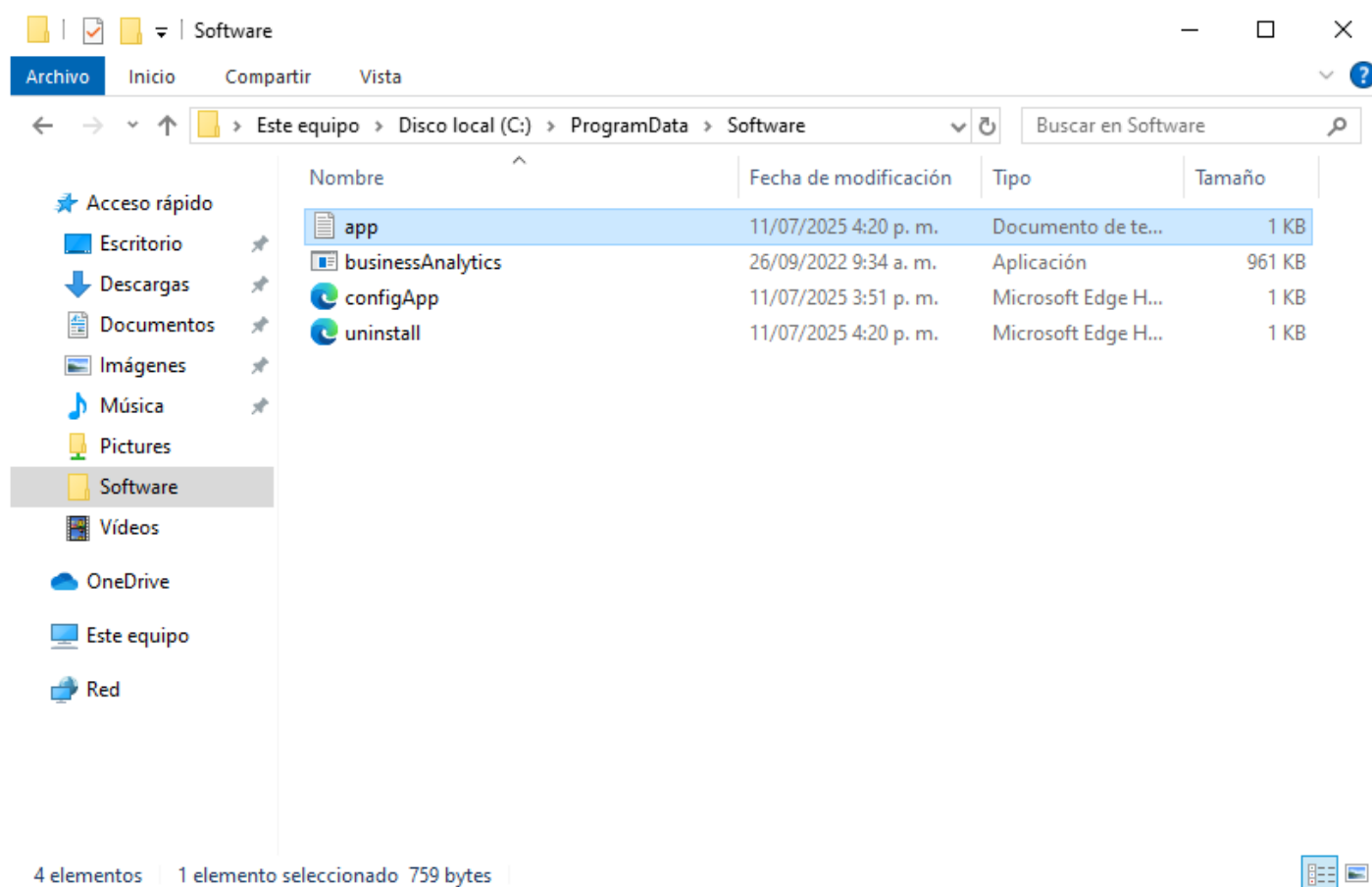
PS C:\Windows\system32>
```

En esta pantalla se muestra información de valor como el ID del producto y la ruta local que ha creado Windows para almacenar en caché el MSI del agente.

The Fraud Explorer es un software que junto con **FraudGPT** detecta el fraude y la corrupción en las organizaciones.

Archivos que crea el agente

En la carpeta **C:\ProgramData\Software** se almacena el archivo ejecutable del agente de The Fraud Explorer llamado **businessAnalytics.exe**. Junto a él también se encuentra un archivo de los llamado **app.log**, un archivo de configuración llamado **configApp.xml** y un archivo con instrucciones internas para la desinstalación llamado **uninstall.xml**.

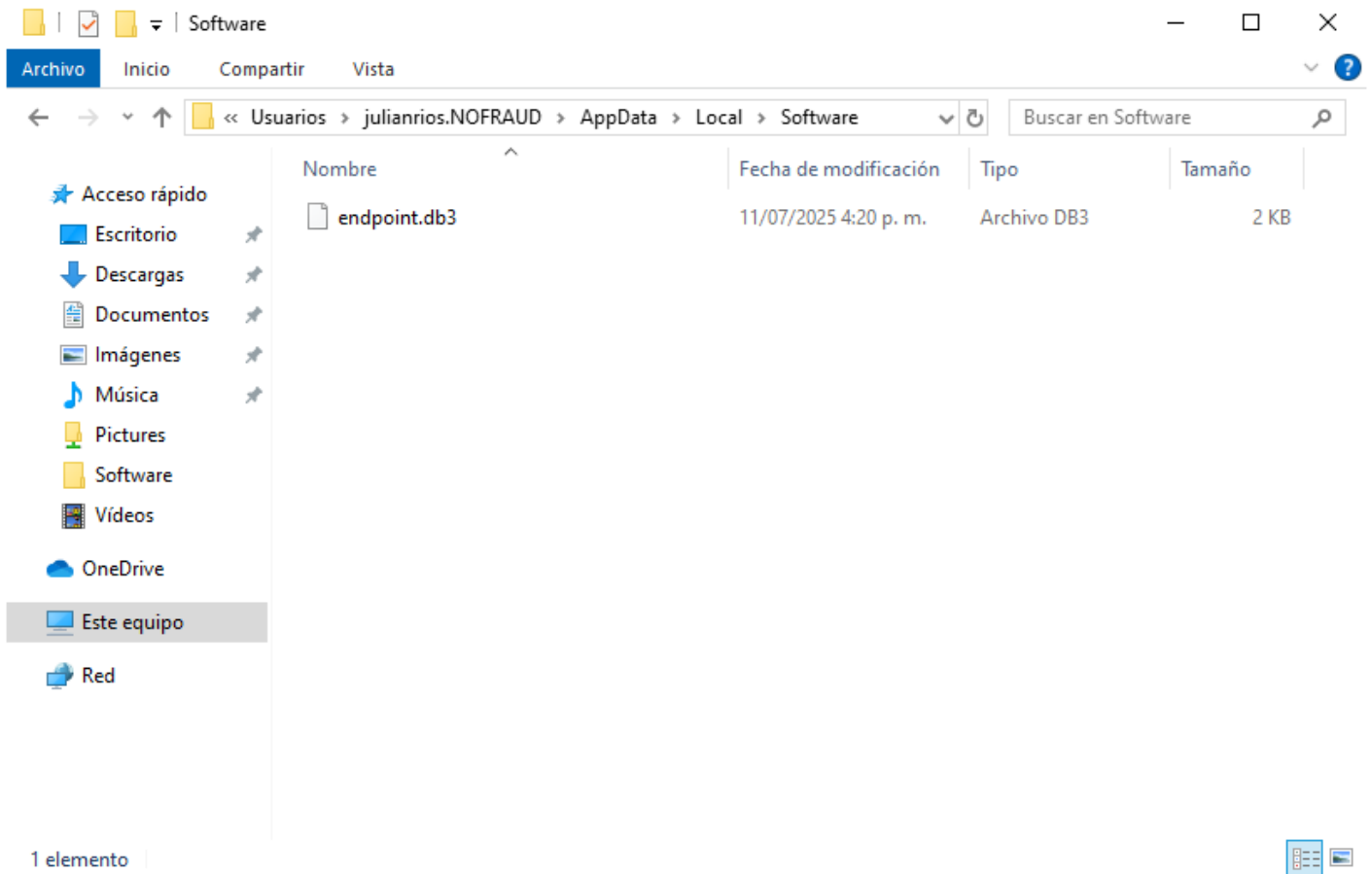


En caso de tener que agregar excepciones en el antivirus, el contenido de esta carpeta debería incluirse en las reglas de excepción o para la regla de ejecución el binario **businessAnalytics.exe**.

The Fraud Explorer es un software que junto con **FraudGPT** detecta el fraude y la corrupción en las organizaciones.

Base de datos del agente

Internamente el agente de The Fraud Explorer almacena su configuración en un archivo cifrado llamado **endpoint.db3** y localizado en la carpeta **C:\Users\empleado\AppData\Local\Software**. Esta carpeta depende al final del usuario que será monitoreado.

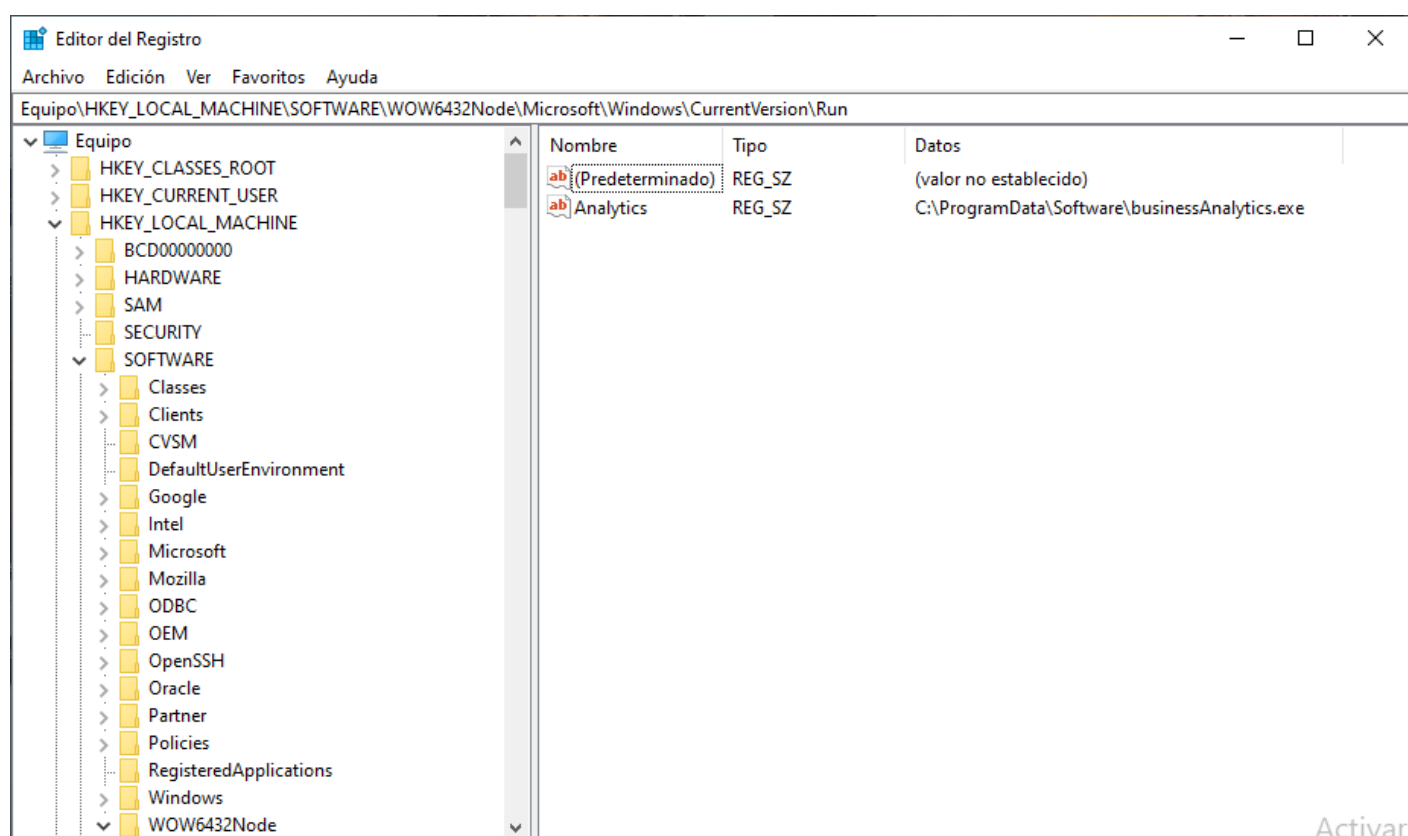


En este archivo se almacena configuración como la dirección del servidor, las llaves de cifrado para la comunicación con la consola central y otra información relevante para su funcionamiento.

The Fraud Explorer es un software que junto con FraudGPT detecta el fraude y la corrupción en las organizaciones.

Entradas de registro de Windows

El agente de The Fraud Explorer crea una entrada en el registro de Windows en la ruta **HKEY_LOCAL_MACHINE, SOFTWARE, WOW6432Node, Microsoft, Windows, CurrentVersion, Run**.

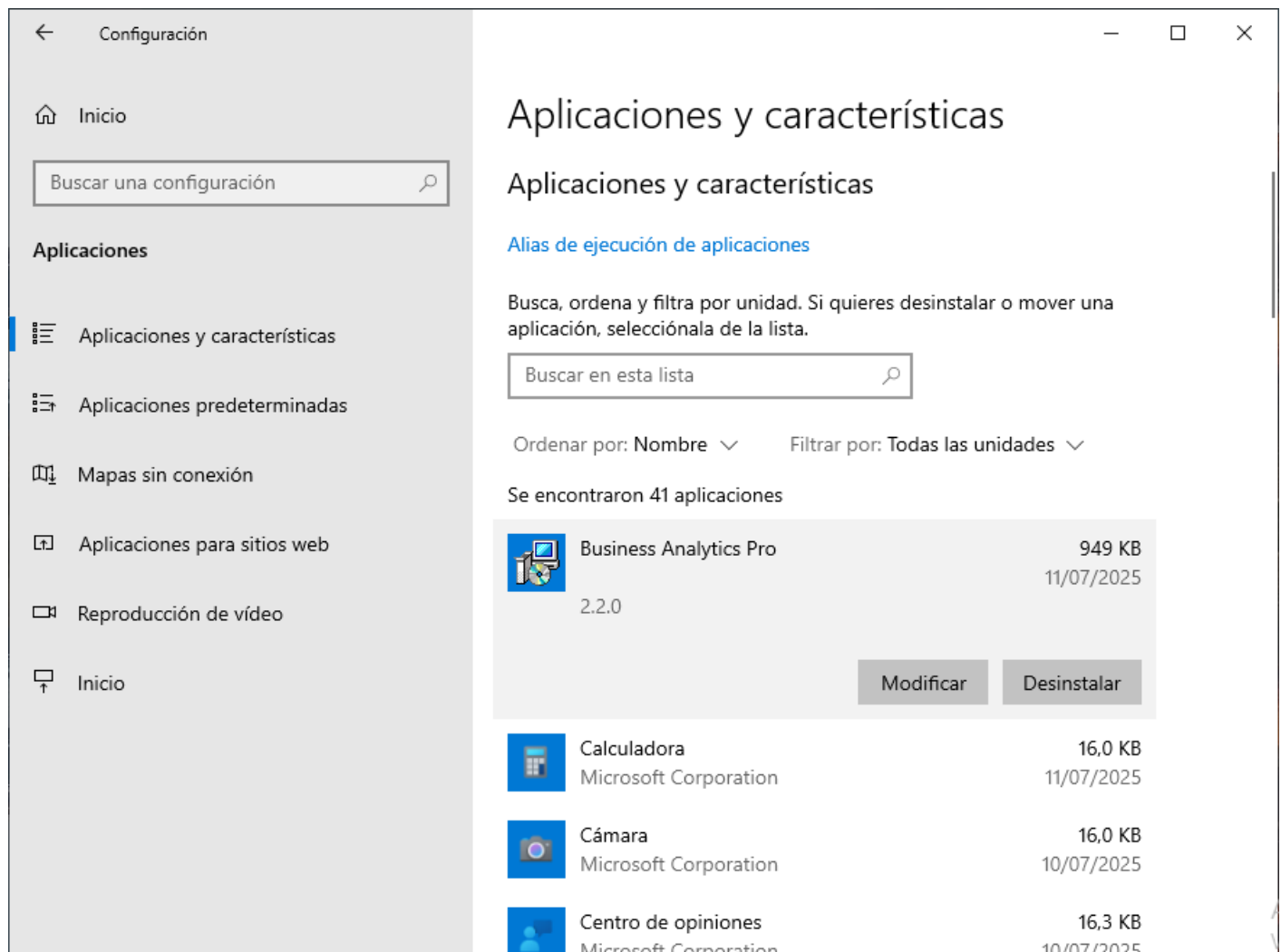


Esta entrada garantiza que el agente inicie cada vez que el dispositivo sea reiniciado. El agente de The Fraud Explorer no crea ninguna otra entrada en el registro de Windows aparte de esta.

The Fraud Explorer es un software que junto con FraudGPT detecta el fraude y la corrupción en las organizaciones

Aparición en programas instalados

Si se entra al panel de control y allí se ingresa a las aplicaciones y características del equipo, se verá que aparece el agente de The Fraud Explorer con el nombre **Business Analytics**.



Junto con el nombre de la aplicación aparece también la versión del agente. Cuando se realiza una actualización, no se crean entradas nuevas sino que se re-emplaza la actual con la nueva versión.

The Fraud Explorer es un software que junto con FraudGPT detecta el fraude y la corrupción en las organizaciones.

Monitoreo del agente

En el PC del usuario, se puede abrir el **Administrador de tareas** y en la pestaña **Detalles** buscar el ejecutable **businessAnalytics.exe**.

Administrador de tareas						
Archivo Opciones Vista						
Procesos Rendimiento Historial de aplicaciones Inicio Usuarios Detalles Servicios						
Nombre	PID	Estado	Nombre d...	CPU	Memoria (...)	Virtualización ...
AggregatorHost.exe	4700	En ejecución		00	1.676 K	
ApplicationFrameHo...	9024	En ejecución	julianrios	00	3.756 K	Deshabilitada
businessAnalytics.exe	5536	En ejecución	julianrios	00	17.692 K	Deshabilitada
CcmExec.exe	932	En ejecución		00	11.392 K	
conhost.exe	3768	En ejecución	Administr...	00	4.844 K	No permitida
csrss.exe	552	En ejecución		00	560 K	
csrss.exe	648	En ejecución		00	716 K	
ctfmon.exe	5708	En ejecución	julianrios	00	2.480 K	Deshabilitada
dllhost.exe	4288	En ejecución		00	776 K	
dllhost.exe	7164	En ejecución	julianrios	00	1.908 K	Deshabilitada
dwm.exe	1668	En ejecución		00	43.148 K	
explorer.exe	5572	En ejecución	julianrios	00	75.828 K	Deshabilitada
explorer.exe	5960	En ejecución	julianrios	00	6.132 K	Deshabilitada
FileCoAuth.exe	1792	En ejecución	julianrios	00	28 K	Deshabilitada
fontdrvhost.exe	940	En ejecución		00	76 K	
fontdrvhost.exe	948	En ejecución		00	972 K	
Interrupciones del si...	-	En ejecución	SYSTEM	00	0 K	
Menos detalles				Finalizar tarea		

El ejecutable se arranca con los privilegios del usuario que será monitoreado. Se pueden ver además los consumos de recursos que hace el agente. Cuando recién arranca, el agente puede consumir 17 MB de memoria RAM, pero una vez termina de arrancar su uso es de aproximadamente 8 MB.

The Fraud Explorer es un software que junto con **FraudGPT** detecta el fraude y la corrupción en las organizaciones.

Inicio del agente

Al crear la entrada en el registro de Windows, automáticamente el agente puede verse en la misma ventana del **Administrador de tareas**, en la pestaña **Inicio**.

Administrador de tareas

ArchivoOpcionesVista

ProcesosRendimientoHistorial de aplicacionesInicioUsuariosDetallesServicios

Último tiempo de BIOS: 0.0 segundos

Nombre	Anunciante	Estado	Impacto de ini...
Business Analytics Pro	Software Analytics	Habilitado	Alto
Enlace Móvil	Microsoft Corporation	Habilitado	No medido
Microsoft 365 Copilot	Microsoft Corporation	Deshabilitado	Ninguno
Microsoft Edge	Microsoft Corporation	Habilitado	Alto
Microsoft OneDrive	Microsoft Corporation	Habilitado	Alto
VirtualBox Guest Additions T...	Oracle and/or its affiliates	Habilitado	Medio
Windows Security notificati...	Microsoft Corporation	Habilitado	Bajo

Menos detalles

Deshabilitar

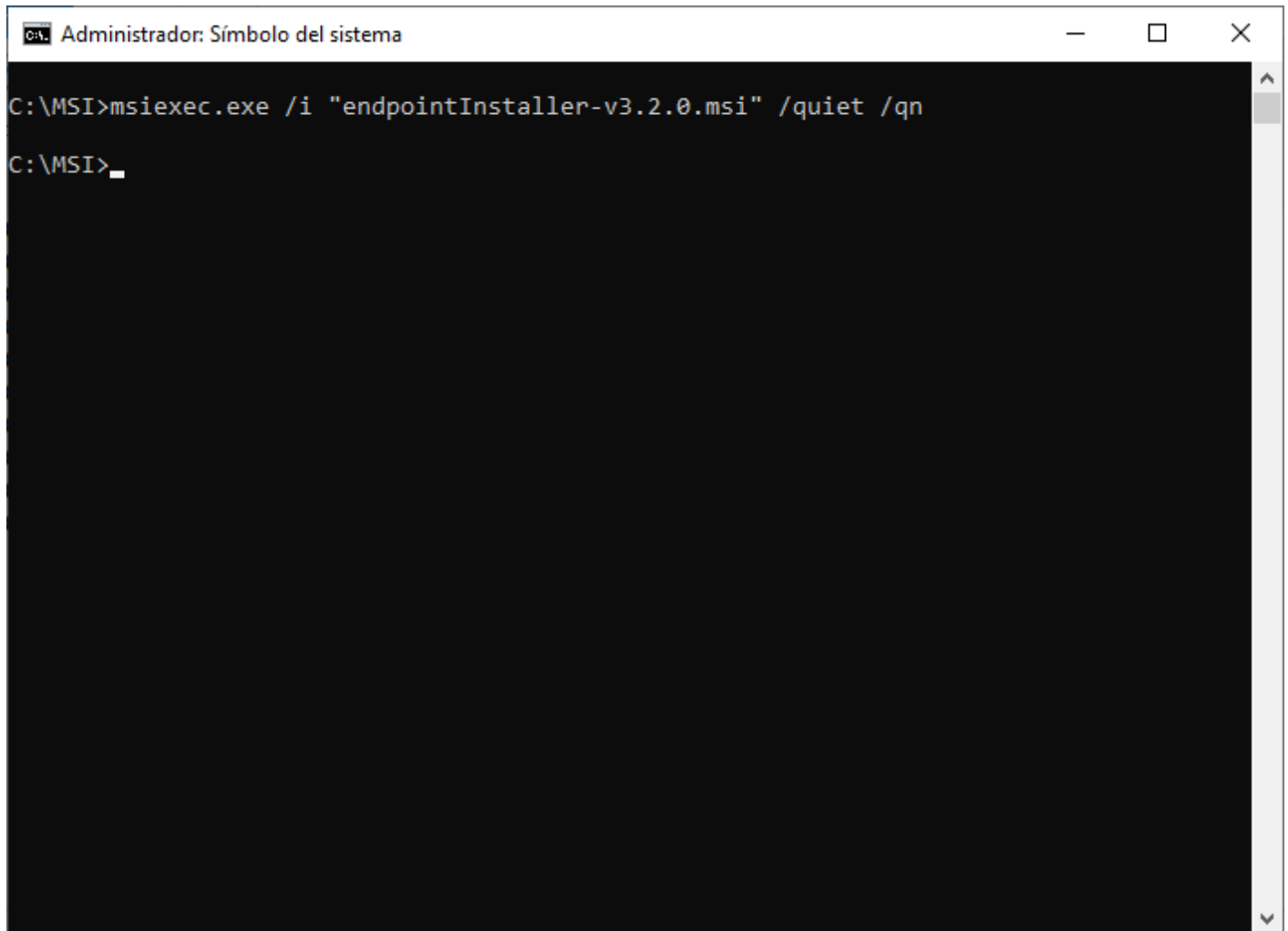
En esta ventana se muestran todas las aplicaciones que arrancan cuando el usuario inicia sesión con su cuenta en Windows. El agente de The Fraud Explorer no arranca como servicio y no interfiere en el proceso de arranque de sistema operativo.

En caso de tener problemas con el arranque de Windows, puede descartar directamente que sea el agente de The Fraud Explorer, porque el agente se ejecuta en la etapa final cuando se ha cargado completamente el explorador de Windows.

The Fraud Explorer es un software que junto con **FraudGPT** detecta el fraude y la corrupción en las organizaciones.

Actualización del agente

Para actualizar el agente deberá abrir una consola de **MS-DOS** en modo **administrador** y ejecutar exactamente el mismo comando que se usó para instalarlo, con la diferencia que acá deberá especificar el MSI de la nueva versión del agente.



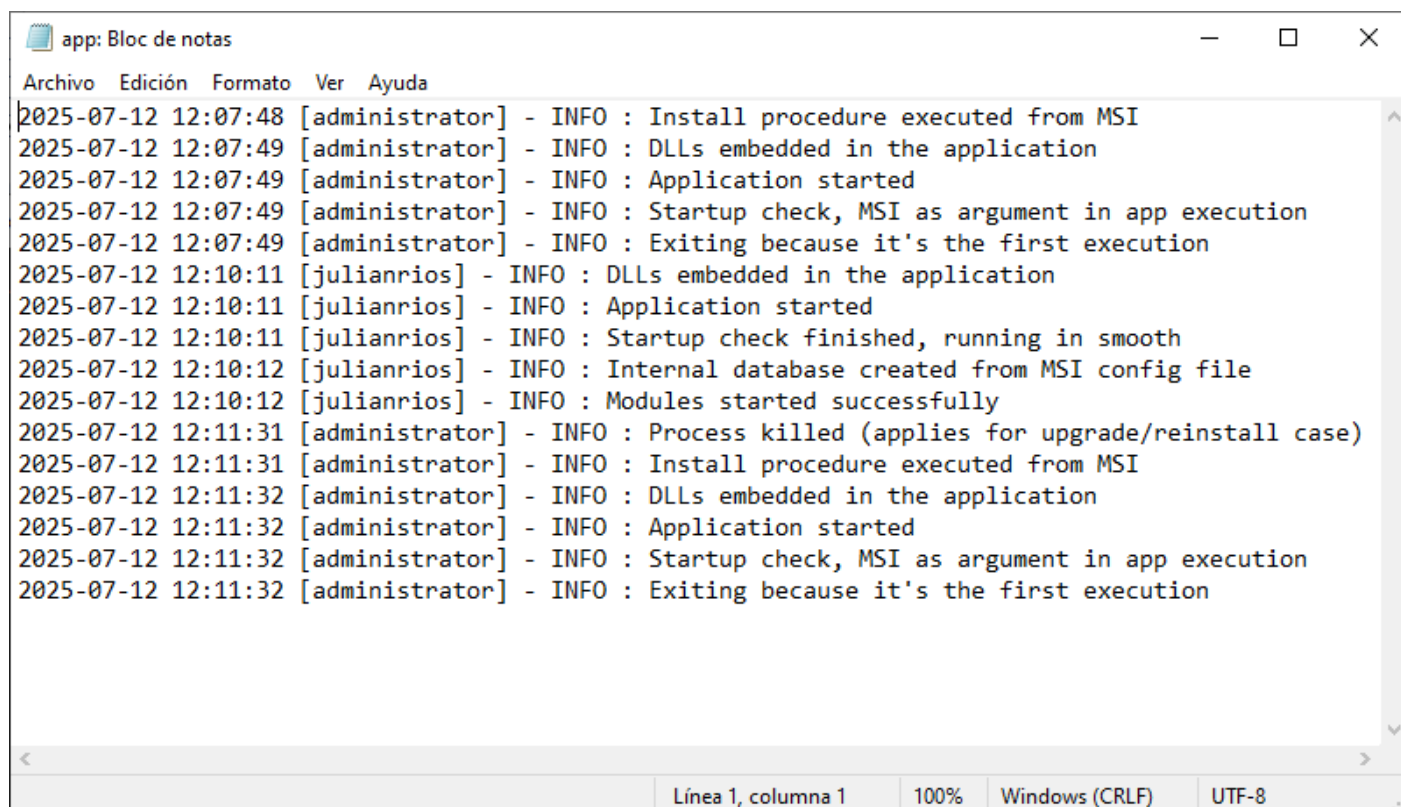
```
C:\MSI>msiexec.exe /i "endpointInstaller-v3.2.0.msi" /quiet /qn
C:\MSI>
```

Internamente el MSI busca versiones anteriores del mismo agente, lo reemplaza y copia los nuevos archivos a la carpeta **C:\ProgramData\Software** donde normalmente se almacenan.

The Fraud Explorer es un software que junto con **FraudGPT** detecta el fraude y la corrupción en las organizaciones.

Verificación de la actualización

En el archivo C:\ProgramData\Software\app.log se observará el proceso de actualización ejecutado.



```
app: Bloc de notas
Archivo  Edición  Formato  Ver  Ayuda
2025-07-12 12:07:48 [administrator] - INFO : Install procedure executed from MSI
2025-07-12 12:07:49 [administrator] - INFO : DLLs embedded in the application
2025-07-12 12:07:49 [administrator] - INFO : Application started
2025-07-12 12:07:49 [administrator] - INFO : Startup check, MSI as argument in app execution
2025-07-12 12:07:49 [administrator] - INFO : Exiting because it's the first execution
2025-07-12 12:10:11 [julianrios] - INFO : DLLs embedded in the application
2025-07-12 12:10:11 [julianrios] - INFO : Application started
2025-07-12 12:10:11 [julianrios] - INFO : Startup check finished, running in smooth
2025-07-12 12:10:12 [julianrios] - INFO : Internal database created from MSI config file
2025-07-12 12:10:12 [julianrios] - INFO : Modules started successfully
2025-07-12 12:11:31 [administrator] - INFO : Process killed (applies for upgrade/reinstall case)
2025-07-12 12:11:31 [administrator] - INFO : Install procedure executed from MSI
2025-07-12 12:11:32 [administrator] - INFO : DLLs embedded in the application
2025-07-12 12:11:32 [administrator] - INFO : Application started
2025-07-12 12:11:32 [administrator] - INFO : Startup check, MSI as argument in app execution
2025-07-12 12:11:32 [administrator] - INFO : Exiting because it's the first execution
```

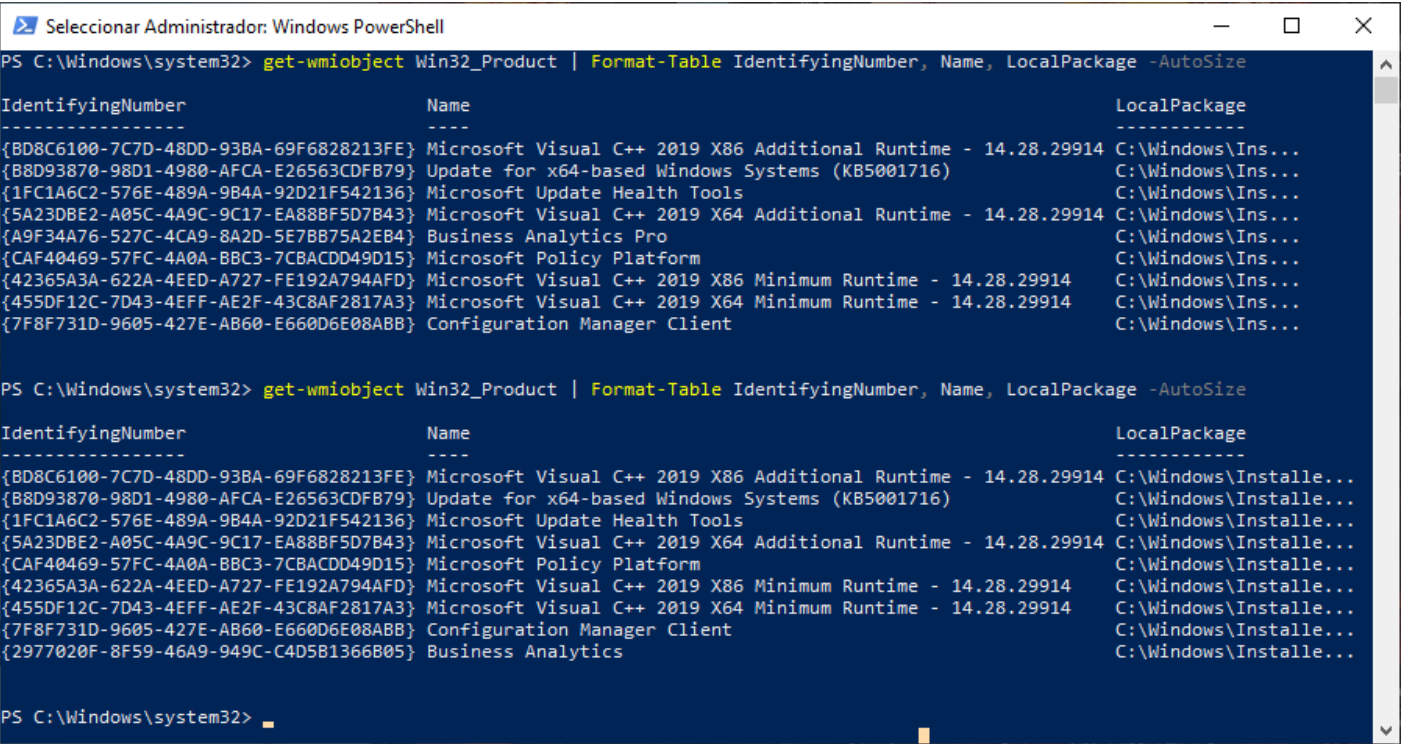
Se puede comprobar que se actualizó por la presencia de la entrada **Process killed (applies for upgrade/reinstall case)**.

The Fraud Explorer es un software que junto con **FraudGPT** detecta el fraude y la corrupción en las organizaciones

PowerShell para verificar actualización

Si se vuelve a ejecutar el siguiente comando en el **PowerShell**, se dará cuenta de que la versión anterior ya no existe y se ha reemplazado por la nueva versión:

```
get-wmiobject Win32_Product | Format-Table IdentifyingNumber, Name, LocalPackage -AutoSize
```

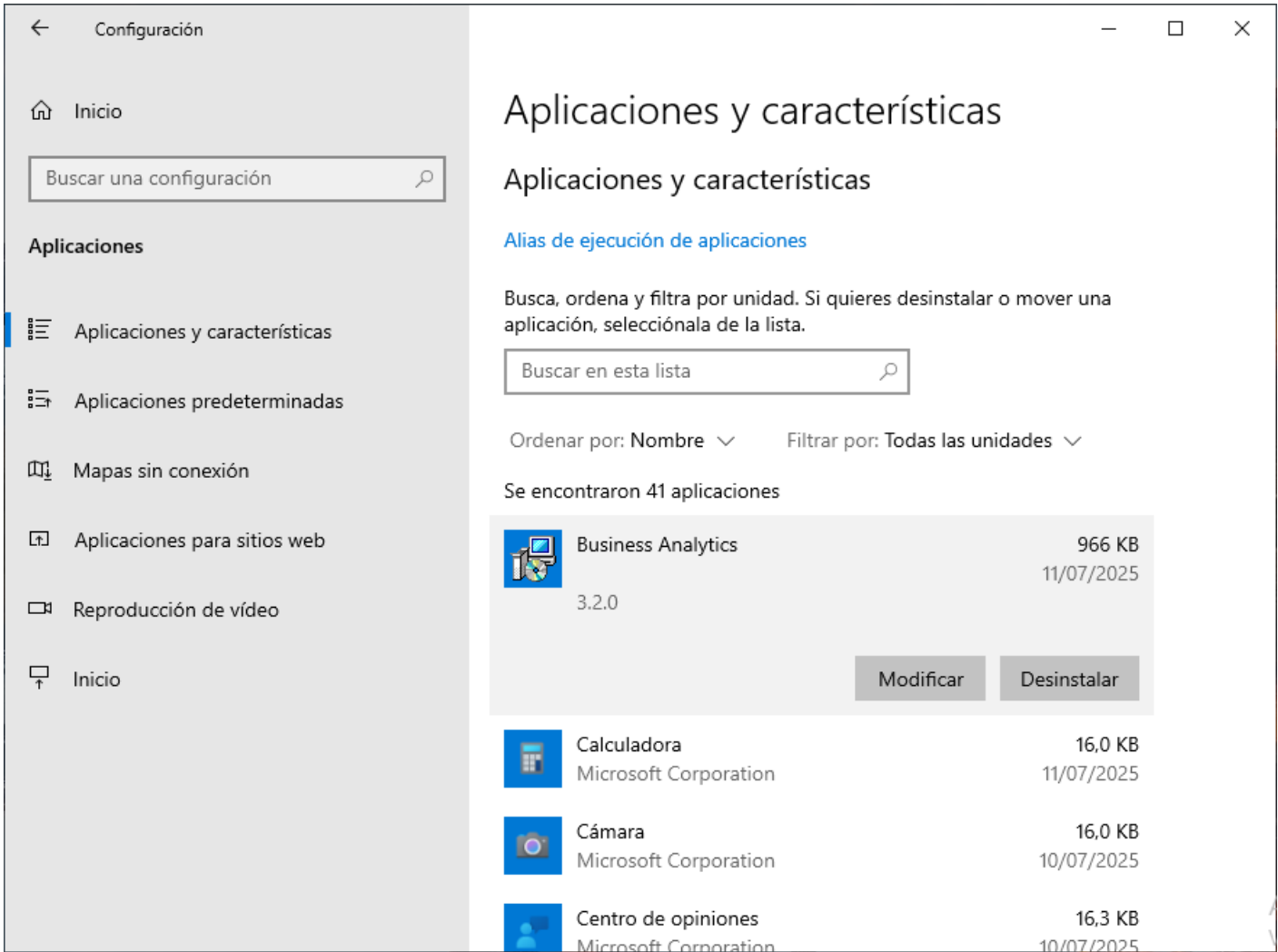


Adicionalmente se muestra el nuevo código del producto, que es diferente al anterior.

The Fraud Explorer es un software que junto con FraudGPT detecta el fraude y la corrupción en las organizaciones

Actualización en listado de Aplicaciones

Adicionalmente, si abre el Panel de control en el PC del usuario y da clic en **Aplicaciones y características**, verá que solo existe una entrada en el listado de aplicaciones referente al agente de The Fraud Explorer.



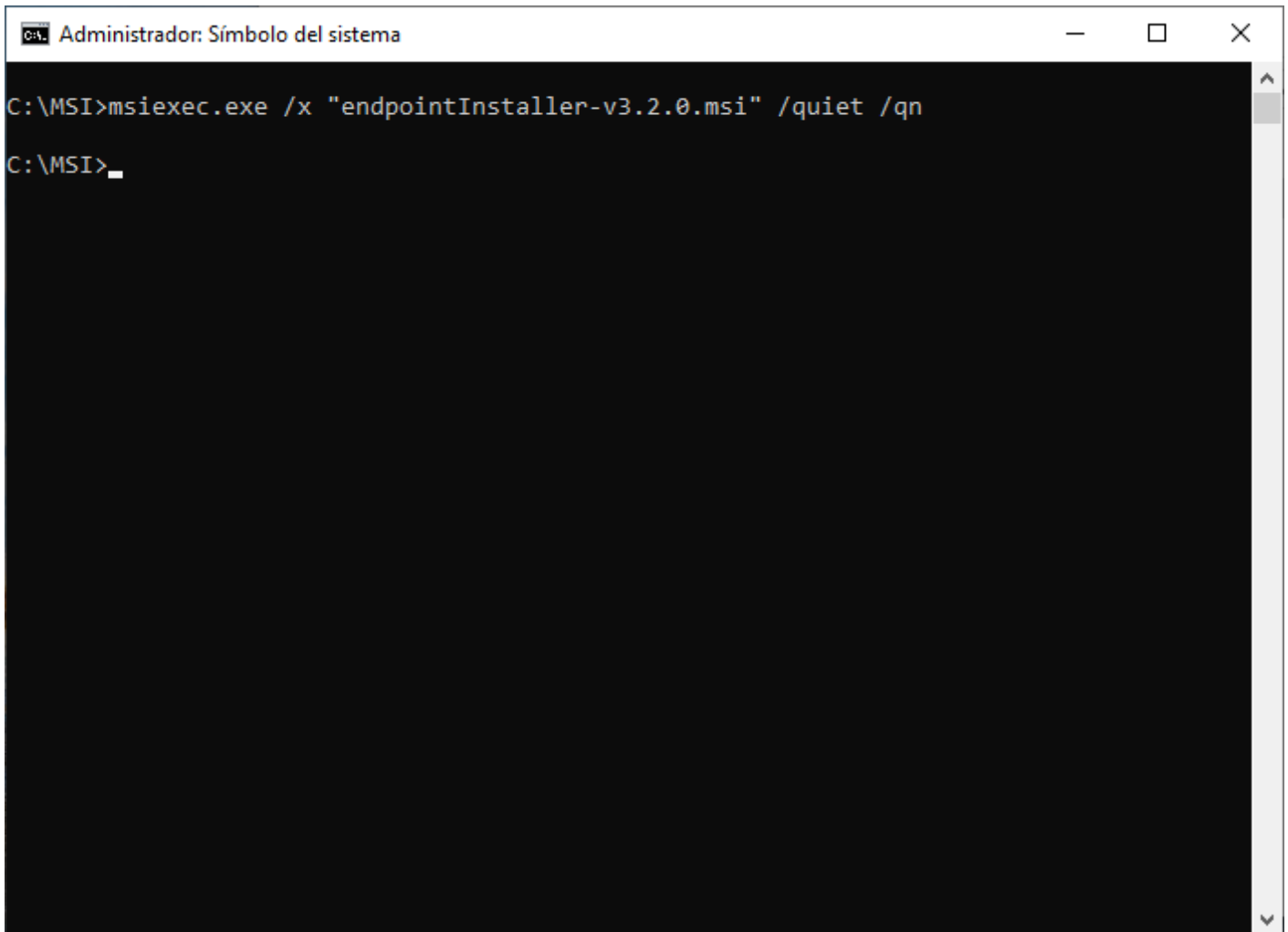
Se podrá ver adicionalmente que la versión cambió y se muestra la versión del nuevo agente.

The Fraud Explorer es un software que junto con FraudGPT detecta el fraude y la corrupción en las organizaciones.

Desinstalación del agente

En una consola **MS-DOS** en modo **administrador** deberá ejecutar el comando:

```
msiexec.exe /x "endpointInstaller-v3.2.0.msi" /quiet /qn
```



```
C:\MSI>msiexec.exe /x "endpointInstaller-v3.2.0.msi" /quiet /qn
C:\MSI>
```

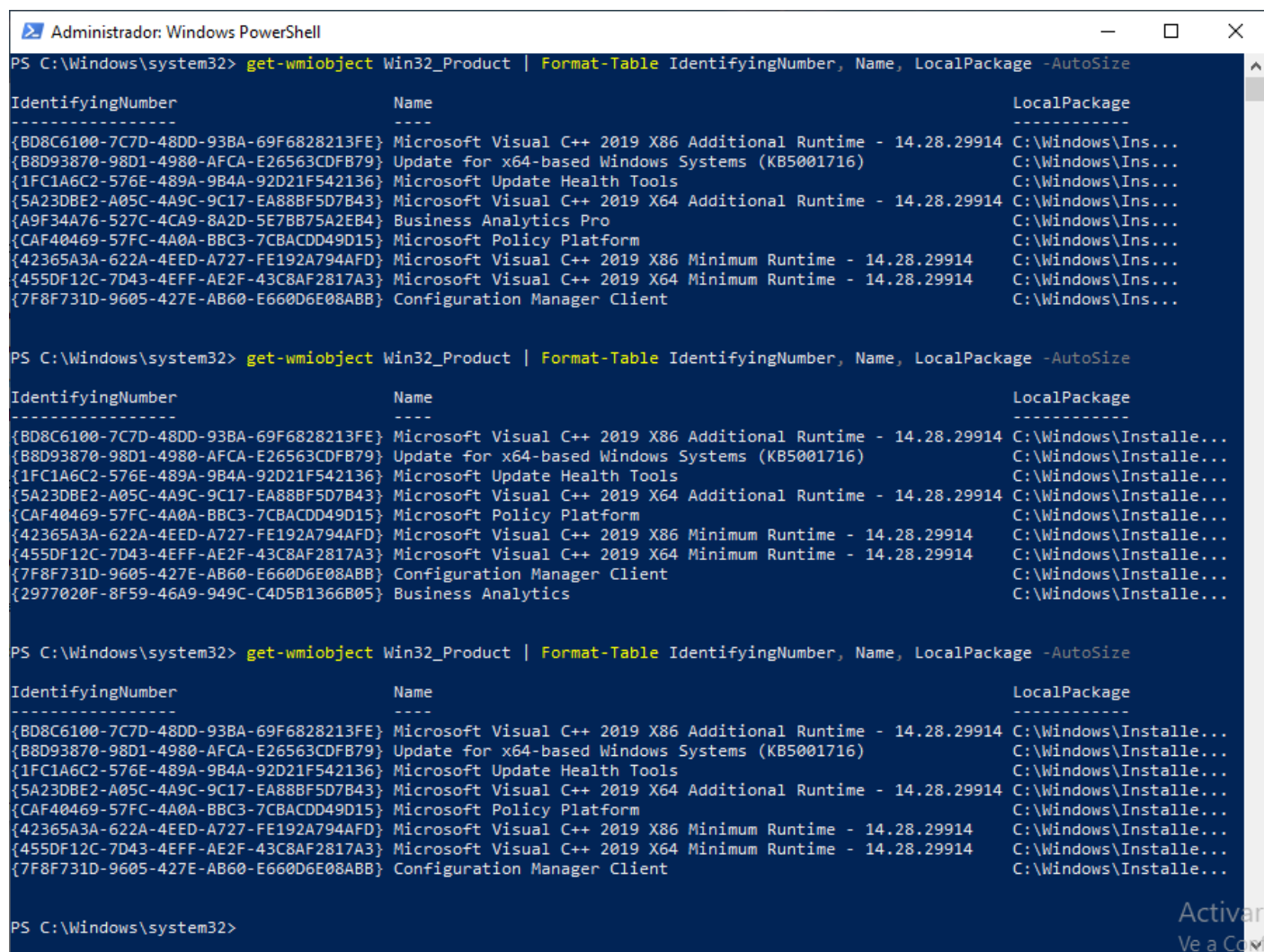
Este comando desinstalará el agente en modo silencioso, eliminando todos los archivos asociados al agente, incluyendo la base de datos y la entrada en el registro de Windows.

The Fraud Explorer es un software que junto con **FraudGPT** detecta el fraude y la corrupción en las organizaciones.

Verificación de la desinstalación

Para verificar en un PC de usuario, se puede volver a ejecutar el comando en la consola de **PowerShell** que muestra el listado de las aplicaciones instaladas:

```
get-wmiobject Win32_Product | Format-Table IdentifyingNumber, Name, LocalPackage -AutoSize
```



The screenshot shows a Windows PowerShell window titled 'Administrador: Windows PowerShell'. The command `get-wmiobject Win32_Product | Format-Table IdentifyingNumber, Name, LocalPackage -AutoSize` is entered and executed three times. The output is a table with three columns: IdentifyingNumber, Name, and LocalPackage. The first two executions show the same list of installed products, including Microsoft Visual C++ runtimes, Windows updates, and Business Analytics. The third execution shows the same list, but the 'LocalPackage' column for 'Business Analytics' is truncated, indicating it has been removed or is no longer present in the system.

IdentifyingNumber	Name	LocalPackage
{BD8C6100-7C7D-48DD-93BA-69F6828213FE}	Microsoft Visual C++ 2019 X86 Additional Runtime - 14.28.29914	C:\Windows\Ins...
{B8D93870-98D1-4980-AFCA-E26563CDFB79}	Update for x64-based Windows Systems (KB5001716)	C:\Windows\Ins...
{1FC1A6C2-576E-489A-9B4A-92D21F542136}	Microsoft Update Health Tools	C:\Windows\Ins...
{5A23DBE2-A05C-4A9C-9C17-EA88BF5D7B43}	Microsoft Visual C++ 2019 X64 Additional Runtime - 14.28.29914	C:\Windows\Ins...
{A9F34A76-527C-4CA9-8A2D-5E7BB75A2EB4}	Business Analytics Pro	C:\Windows\Ins...
{CAF40469-57FC-4A0A-BBC3-7CBACDD49D15}	Microsoft Policy Platform	C:\Windows\Ins...
{42365A3A-622A-4EED-A727-FE192A794AFD}	Microsoft Visual C++ 2019 X86 Minimum Runtime - 14.28.29914	C:\Windows\Ins...
{455DF12C-7D43-4EFF-AE2F-43C8AF2817A3}	Microsoft Visual C++ 2019 X64 Minimum Runtime - 14.28.29914	C:\Windows\Ins...
{7F8F731D-9605-427E-AB60-E660D6E08ABB}	Configuration Manager Client	C:\Windows\Ins...

IdentifyingNumber	Name	LocalPackage
{BD8C6100-7C7D-48DD-93BA-69F6828213FE}	Microsoft Visual C++ 2019 X86 Additional Runtime - 14.28.29914	C:\Windows\Installe...
{B8D93870-98D1-4980-AFCA-E26563CDFB79}	Update for x64-based Windows Systems (KB5001716)	C:\Windows\Installe...
{1FC1A6C2-576E-489A-9B4A-92D21F542136}	Microsoft Update Health Tools	C:\Windows\Installe...
{5A23DBE2-A05C-4A9C-9C17-EA88BF5D7B43}	Microsoft Visual C++ 2019 X64 Additional Runtime - 14.28.29914	C:\Windows\Installe...
{CAF40469-57FC-4A0A-BBC3-7CBACDD49D15}	Microsoft Policy Platform	C:\Windows\Installe...
{42365A3A-622A-4EED-A727-FE192A794AFD}	Microsoft Visual C++ 2019 X86 Minimum Runtime - 14.28.29914	C:\Windows\Installe...
{455DF12C-7D43-4EFF-AE2F-43C8AF2817A3}	Microsoft Visual C++ 2019 X64 Minimum Runtime - 14.28.29914	C:\Windows\Installe...
{7F8F731D-9605-427E-AB60-E660D6E08ABB}	Configuration Manager Client	C:\Windows\Installe...
{2977020F-8F59-46A9-949C-C4D5B1366805}	Business Analytics	C:\Windows\Installe...

IdentifyingNumber	Name	LocalPackage
{BD8C6100-7C7D-48DD-93BA-69F6828213FE}	Microsoft Visual C++ 2019 X86 Additional Runtime - 14.28.29914	C:\Windows\Installe...
{B8D93870-98D1-4980-AFCA-E26563CDFB79}	Update for x64-based Windows Systems (KB5001716)	C:\Windows\Installe...
{1FC1A6C2-576E-489A-9B4A-92D21F542136}	Microsoft Update Health Tools	C:\Windows\Installe...
{5A23DBE2-A05C-4A9C-9C17-EA88BF5D7B43}	Microsoft Visual C++ 2019 X64 Additional Runtime - 14.28.29914	C:\Windows\Installe...
{CAF40469-57FC-4A0A-BBC3-7CBACDD49D15}	Microsoft Policy Platform	C:\Windows\Installe...
{42365A3A-622A-4EED-A727-FE192A794AFD}	Microsoft Visual C++ 2019 X86 Minimum Runtime - 14.28.29914	C:\Windows\Installe...
{455DF12C-7D43-4EFF-AE2F-43C8AF2817A3}	Microsoft Visual C++ 2019 X64 Minimum Runtime - 14.28.29914	C:\Windows\Installe...
{7F8F731D-9605-427E-AB60-E660D6E08ABB}	Configuration Manager Client	C:\Windows\Installe...

Como se observa, después de ejecutar el comando de desinstalación, ya no aparece la aplicación Business Analytics.