# 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 guery "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 Evolorer es un software que junto con FraudGPT detecta el fraude y la corrunción en las organizaciones

## Video con todos los pasos

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

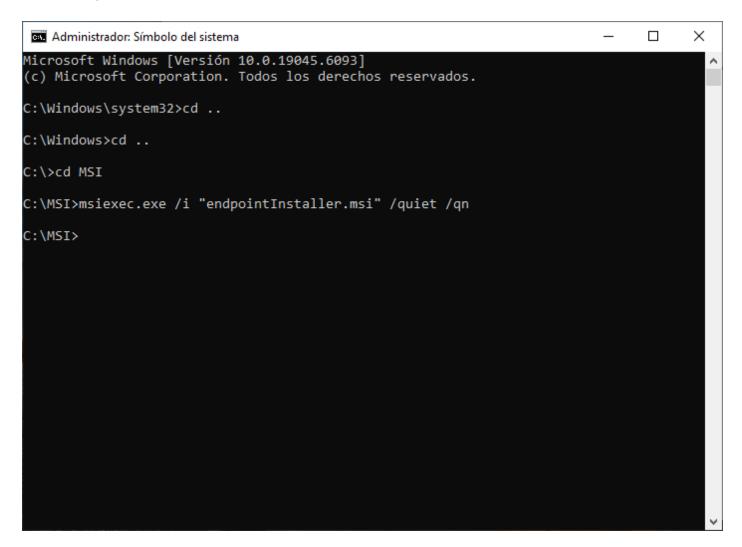
#### https://www.youtube.com/embed/87HNEWn-4Ts?si=YyKvfKAHeRWmqj6g

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 Evolution of the second supplies the fraud of t

# 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.



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

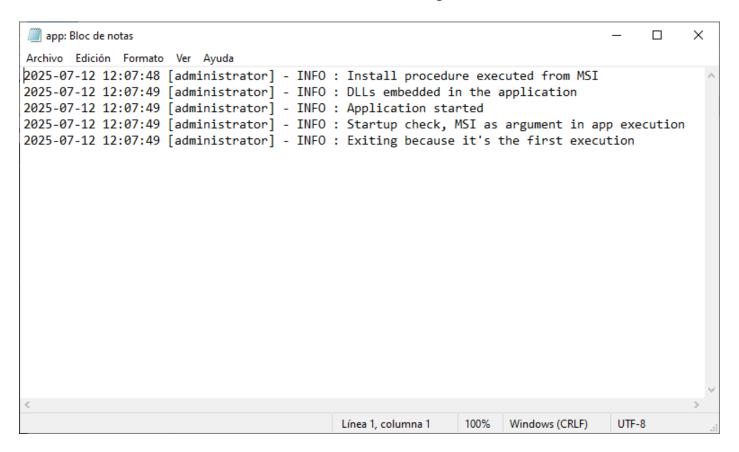
```
msiexec.exe /i "endpointInstaller.exe" /quiet /qn
```

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

The Fraud Evalorer as un software que junto con FraudCPT detects al fraude y la corrunción 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 le usuario administrador acaba de realizar la instalación del agente.

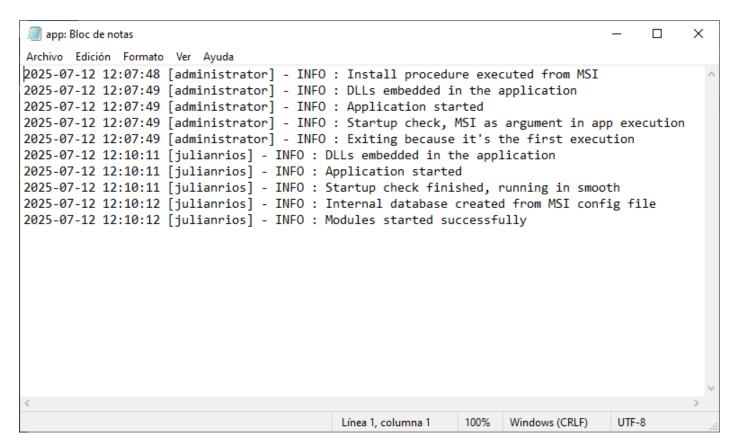


El agente solo usa el usuario **administrador** para instalar el aplicativo, no para correrlo.

The Fraud Evolorer es un software que junto con FraudCPT detecta el fraude y la corrunción 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.



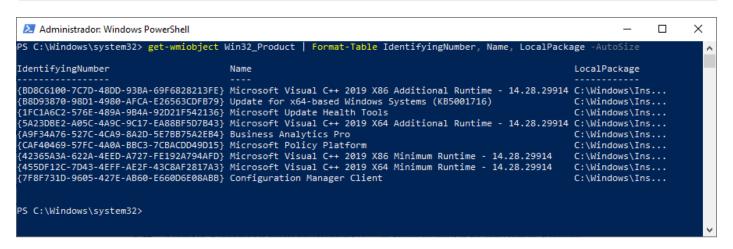
En este archivo de log se encontrará toda información relevante de inicio, parada, actualización, desinstalación e incluso errores que pueda presentar el agente durante su ejecución.

The Fraud Evolorer es un software que junto con FraudGPT detecta el fraude y la corrunción 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

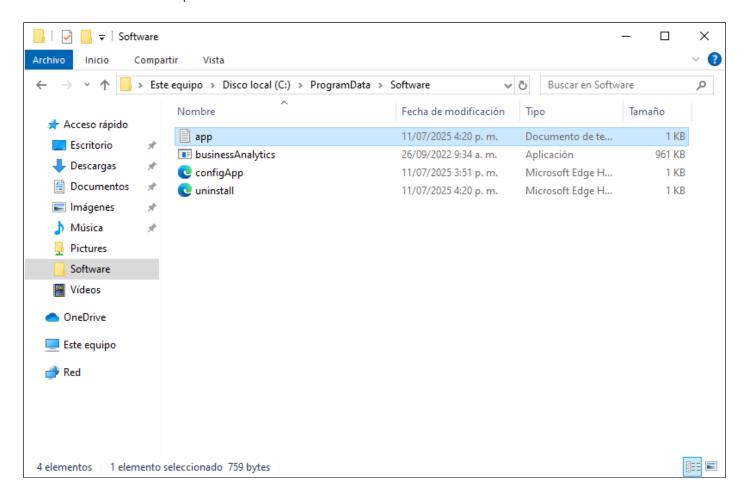


En esta pantalla se muestra información de valor como el ID del producto y la ruta local que ha creado Windows para almacenar en caché el MSI del agente.

The Fraud Evalorer es un software que junto con FraudCPT detects el fraude y la corrunción 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**.

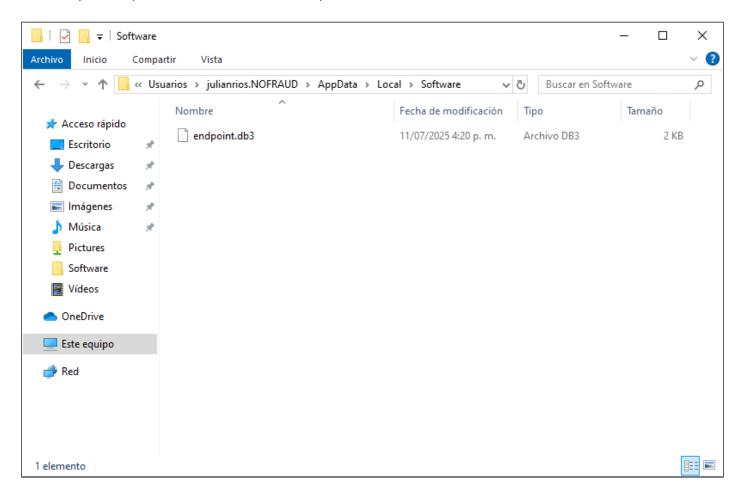


En caso de tener que agregar excepciones en el antivirus, el contenido de esta carpeta debería incluirse en las reglas de excepción o para la regla de ejecución el binario **businessAnalytics.exe** 

The Fraud Evolution as un coffware que junto con FraudGPT detecta el fraude y la corrunción 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.

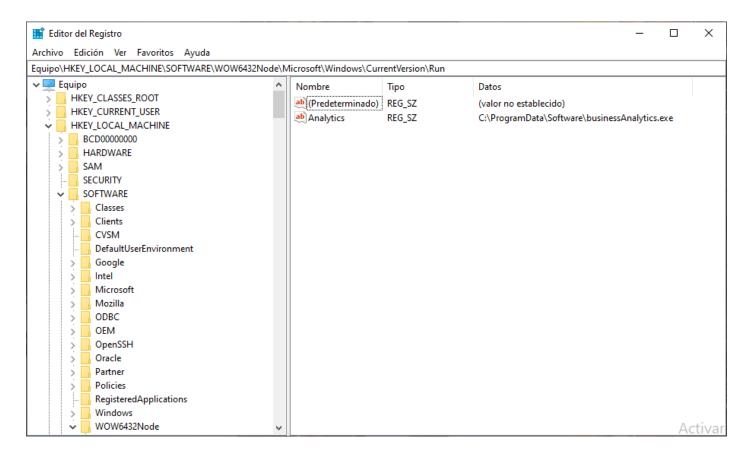


En este archivo se almacena configuración como la dirección del servidor, las llaves de cifrado para la comunicación con la consola central y otra información relevante para su funcionamiento.

The Fraud Evolorer es un software que junto con FraudGPT detecta el fraude y la corrunción 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.

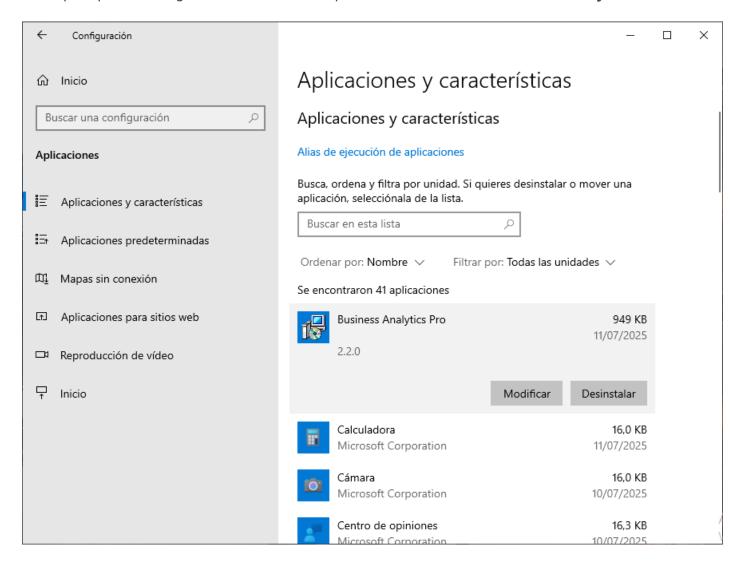


Esta entrada garantiza que el agente inicie cada vez que el dispositivo sea reiniciado. El agente de The Fraud Explorer no crea ninguna otra entrada en el registro de Windows aparte de esta.

The Fraud Evolution of the continue of the Fraud Evolution of the Fr

# Aparición en programas instalados

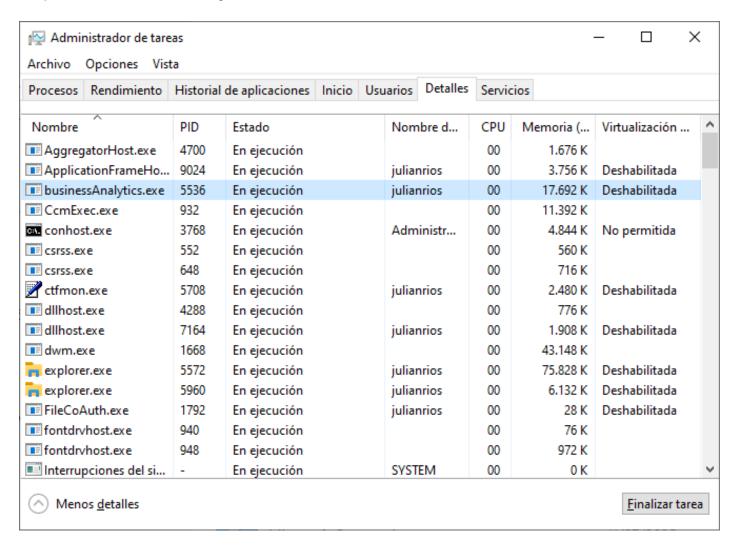
Si se entra al panel de control y allí se ingresa a las aplicaciones y características del equipo, se verá que aparece el agente de The Fraud Explorer con el nombre **Business Analytics**.



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.

## 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**.

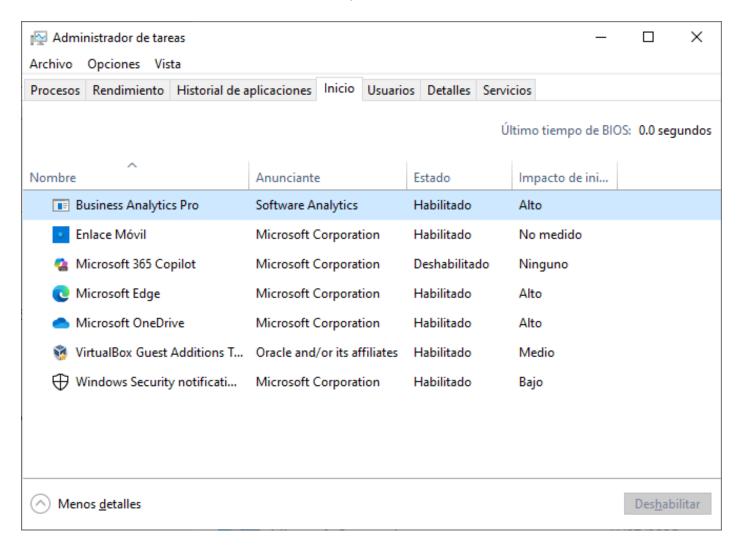


El ejecutable se arranca con los privilegios del usuario que será monitoreado. Se pueden ver además los consumos de recursos que hace el agente. Cuando recién arranca, el agente puede consumir 17 MB de memoria RAM, pero una vez termina de arrancar su uso es de aproximadamente 8 MB.

The Fraud Evalorer of un coffware que junto con FraudCPT detects el fraude y la corrunción 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**.



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.

# 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.

```
Administrador. Símbolo del sistema — X

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

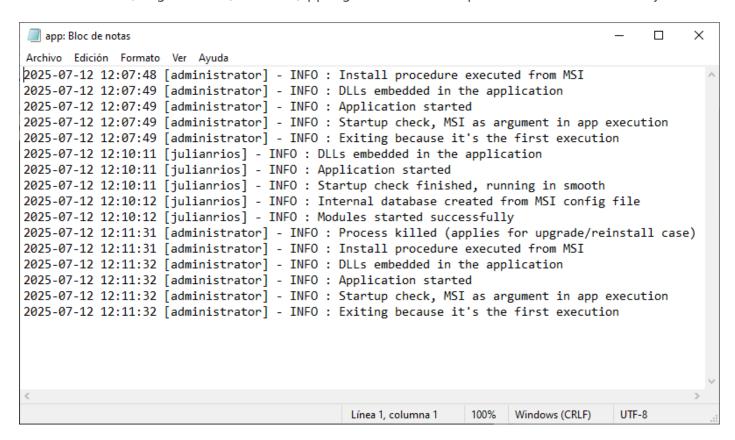
C:\MSI>_
```

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 Evolution as un software que junto con FraudGPT detecta el fraude y la corrunción en las organizaciones

# Verificación de la actualización

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



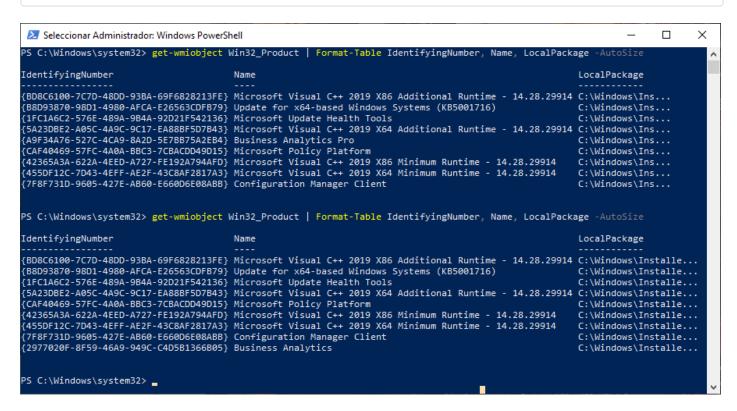
Se puede comprobar que se actualizó por la presencia de la entrada **Process killed (applies for upgrade/reinstall case)**.

The Fraud Explorer as un software que junto con FraudCPT 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

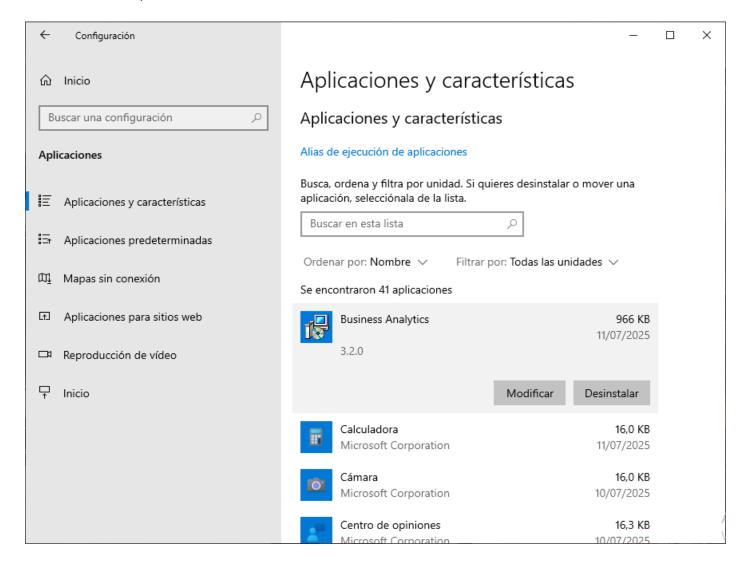


Adicionalmente se muestra el nuevo código del producto, que es diferente al anterior.

The Fraud Evnlorer as un software que junto con FraudCPT detects el fraude y la corrunción 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.

# Desinstalación del agente

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

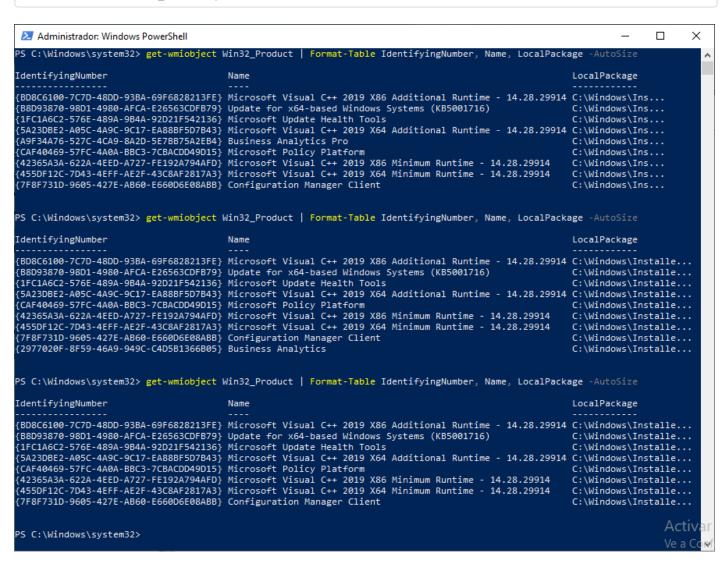
Este comando desinstalará el agente en modo silencioso, eliminando todos los archivos asociados al agente, incluyendo la base de datos y la entrada en el registro de Windows.

The Fraud Evolorer es un software que junto con FraudCPT detecta el fraude y la corrunción 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



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