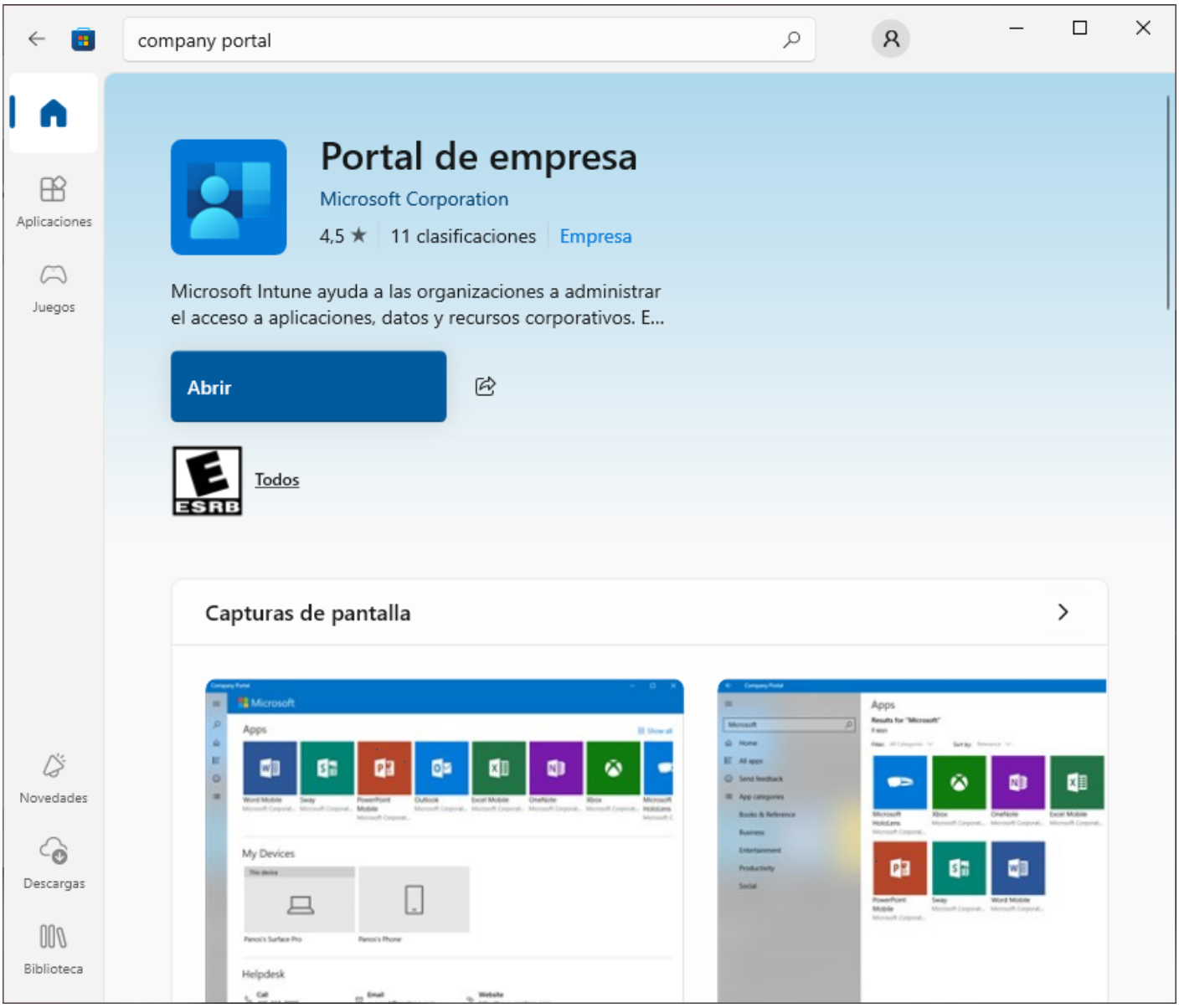
Despliegue con Microsoft Intune

Uso de Microsoft Intune en la nube como MDM para el despliegue del agente en los dispositivos de la organización.

- Inicio del agente
- Carpeta para actualizar el agente
- Paquete de actualización
- Aplicación para la actualización
- Seleccionar paquete de actualización
- Información de actualización
- Comandos de actualización
- Requerimientos de actualización
- Reglas de detección
- Supersedencia
- Asignaciones para actualización
- Eliminar asignaciones antiguas
- Sincronización de dispositivo
- Sincronizar cliente Windows
- Verificación de la actualización
- PowerShell para verificar actualización
- Actualización en listado de Aplicaciones
- Desinstalación del agente
- Asignación de desinstalación
- Sincronización de dispositivo
- Sincronizar cliente Windows
- Verificación de la desinstalación

Requisitos previos

Su organización debe tener **Microsoft Intune** previamente configurado y con las licencias para los usuarios y/o dispositivos. cada computador debe tener por consiguiente la aplicación **Company Portal** y debe estar correctamente enrolado.



Debe contar con la capacidad de realizar acciones administrativas en **Microsoft Intune** y opcionalmente en los computadores de la organización. En teoría, para llevar a cabo el despliegue de nuestro agente no se requiere realizar ninguna acción en los PC de los empleados, sin embargo, en la primera instalación de pruebas quizás quiera forzar la actualización de la política en alguno de los quipos para no tener que esperar mucho tiempo a que se haga de forma natural.

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.

Video con todos los pasos

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

https://www.youtube.com/embed/pXzID59q4gs?si=GTaV-4JDDl3Z9Eym

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

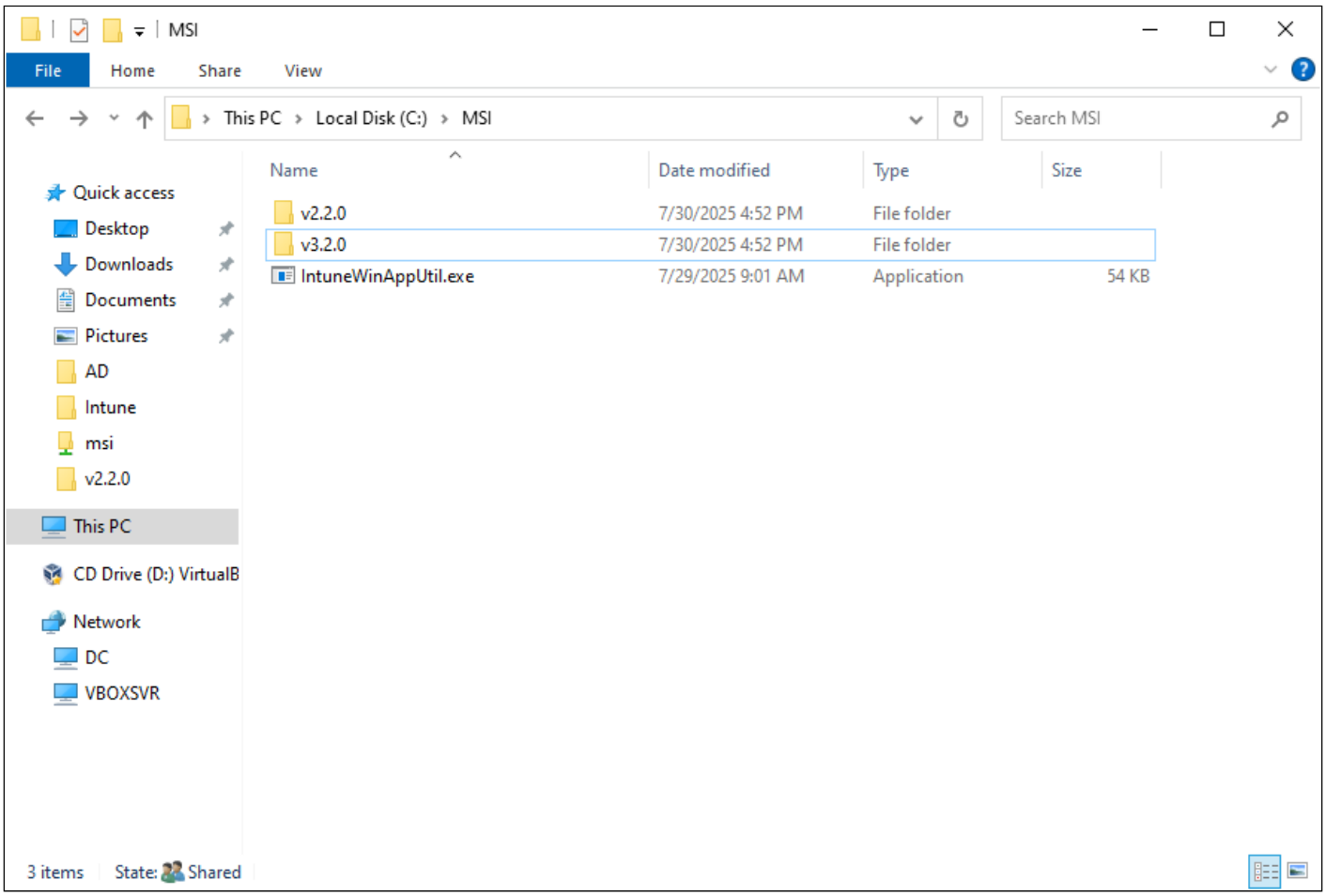
The Fraud Explorer es un software que junto con **FraudGPT** detecta el fraude y la corrupción en las organizaciones

Preparación de carpetas y archivos

Microsoft Intune necesita que le proveamos un paquete de instalación (archivo .intunewin) para poder desplegar un MSI (nuestro agente) y ese paquete lo vamos a crear primero estructurando su contenido.

En un computador cualquiera con Windows, cree una carpeta con nombre **MSI** en la unidad raíz, en ella cree una carpeta llamada **v2.2.0** (esta es la versión del agente que vamos a instalar). En el directorio **MSI** descargue la utilidad **WinApp** de Intune de la URL:

```
https://github.com/Microsoft/Microsoft-Win32-Content-Prep-Tool/raw/master/IntuneWinAppUtil.exe
```

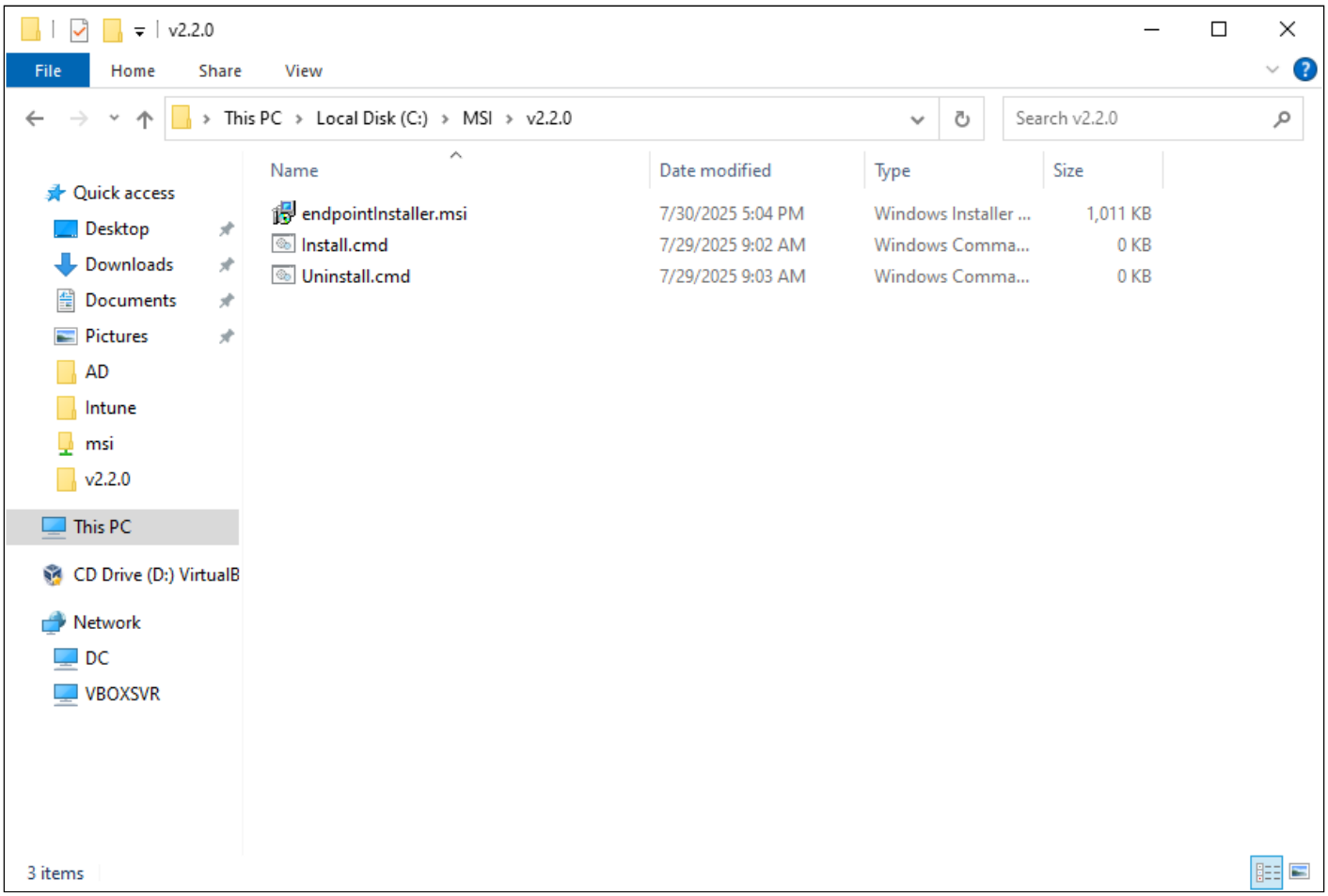


Al final la estructura de carpetas debe lucir así, con una carpeta **MSI** en la raíz y dentro de ella una carpeta **v2.2.0** y el archivo ejecutable **IntuneWinAppUtil.exe**. Si este paso se hizo correctamente ya estamos listos para continuar.

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

Empaquetado del agente

En la carpeta que se creó con nombre **v2.2.0**, coloque el agente **endpointInstaller.msi** y cree dos archivos en blanco, uno llamado **Install.cmd** y otro **Uninstall.cmd**.



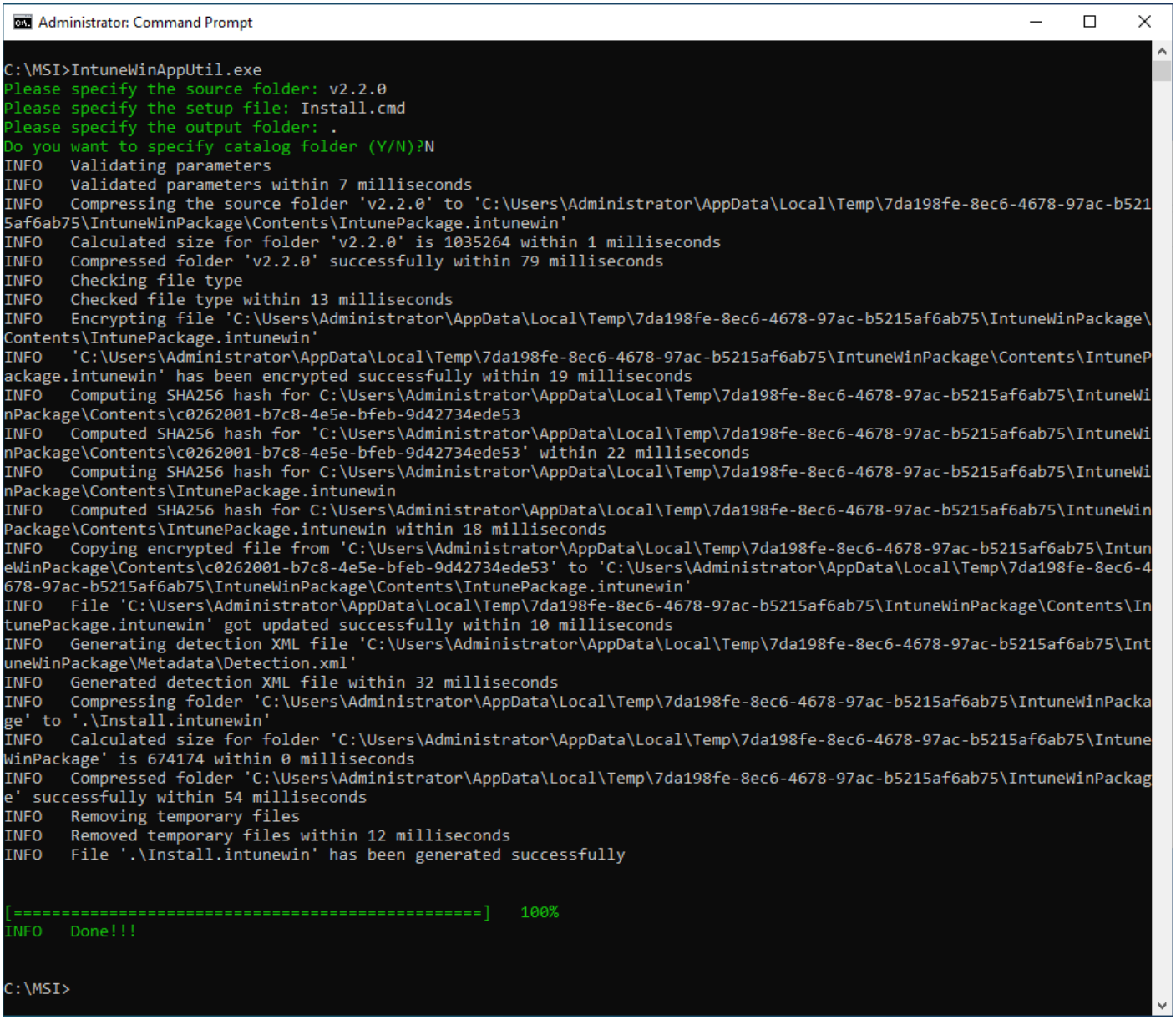
Esta estructura es necesaria para crear el empaquetado que soporta **Microsoft Intune**. Si esto está listo, podemos continuar con el siguiente paso.

Creación del paquete IntuneWin

Abra una consola **MS-DOS** y navegue hasta la carpeta raíz **MSI**. Una vez allí ejecute el comando:

```
IntuneWinAppUtil.exe
```

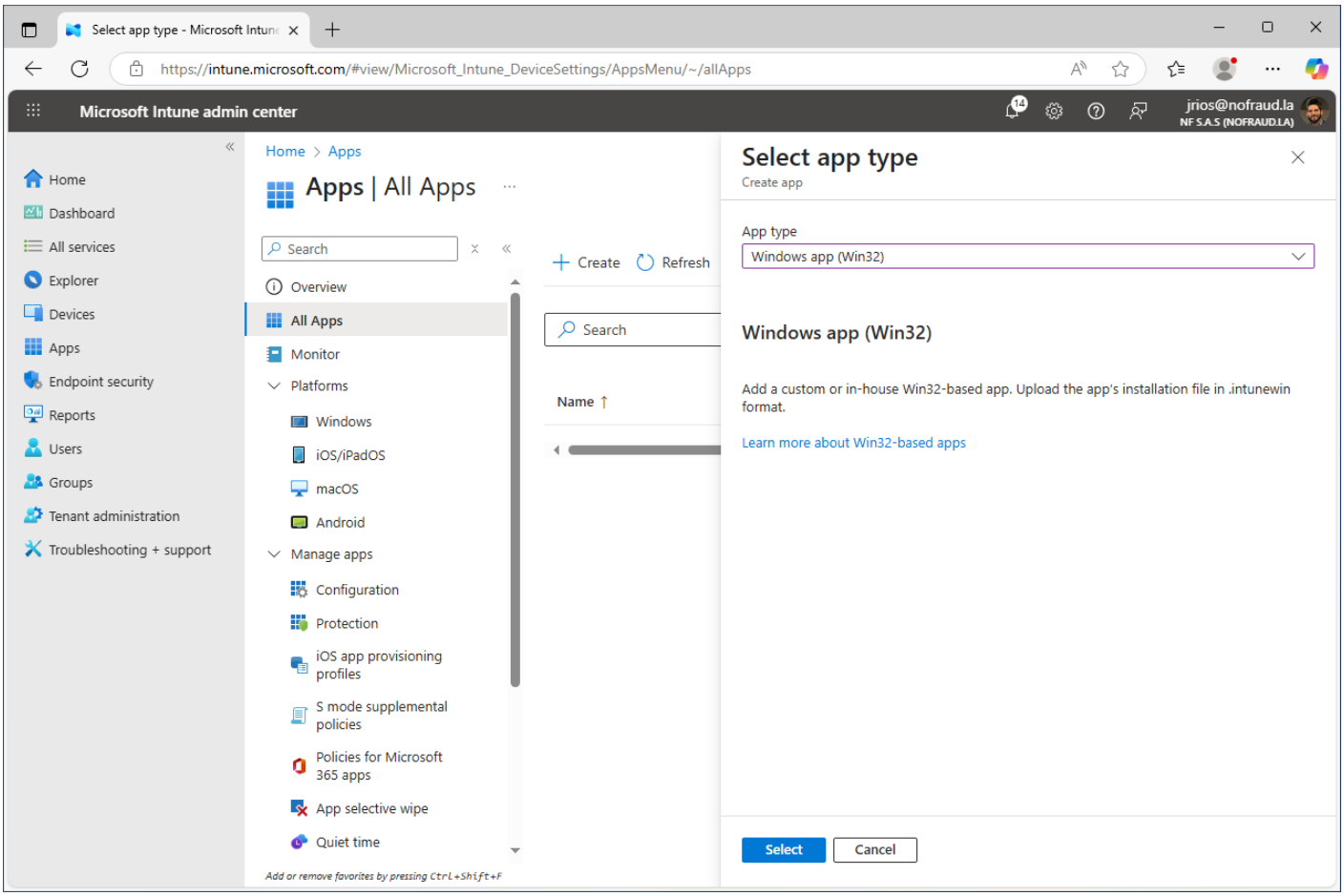
Este comando ejecuta la utilidad de **Microsoft Intune** que creará el paquete de instalación con extensión .intunewin, compatible con la metodología de despliegue de este producto. Cuando se le pregunte por el **source folder** escriba v2.2.0, cuando se le pregunte por el **setup file** escriba Install.cmd, cuando se le pregunte por el **output folder** escriba un punto y cuando se le pregunte por el **catalog folder** escriba N.



Esto creará un archivo llamado **Install.intunewin** en la carpeta **MSI**. Este archivo es el paquete de instalación compatible con **Microsoft Intune** de nuestro agente en su versión 2.2.0. Renombre este archivo a **endpointInstaller-v2.2.0.intunewin** para mayor recordación.

Creación de una aplicación

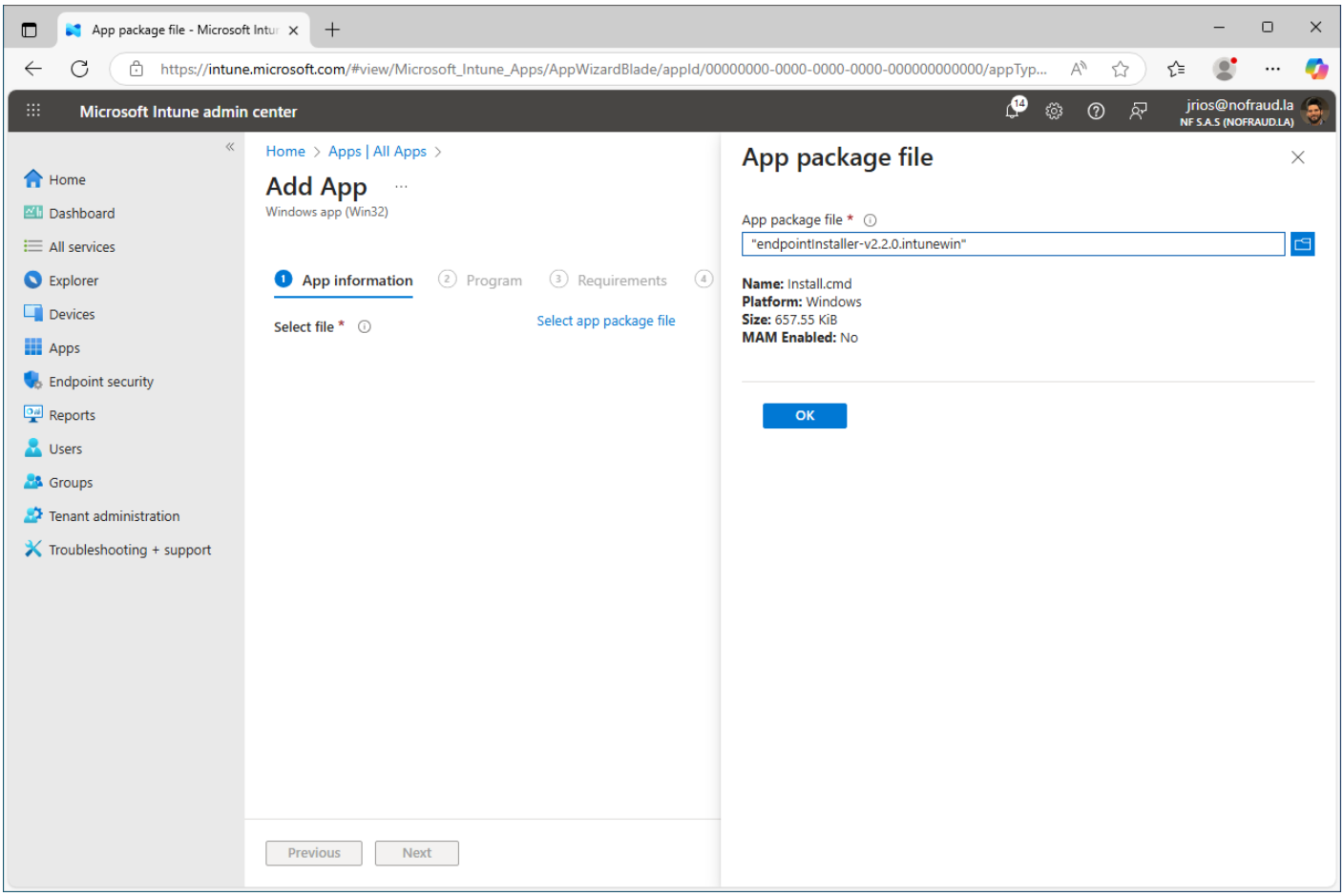
Ingrese a la consola administrativa de **Microsoft Intune**. Una vez allí, en la parte izquierda seleccione **Apps**, luego **All Apps** y de clic en **Create**.



Luego seleccione el tipo de aplicación **Windows app (Win32)** y de clic en el botón **Select**.

Añadir el paquete IntuneWin

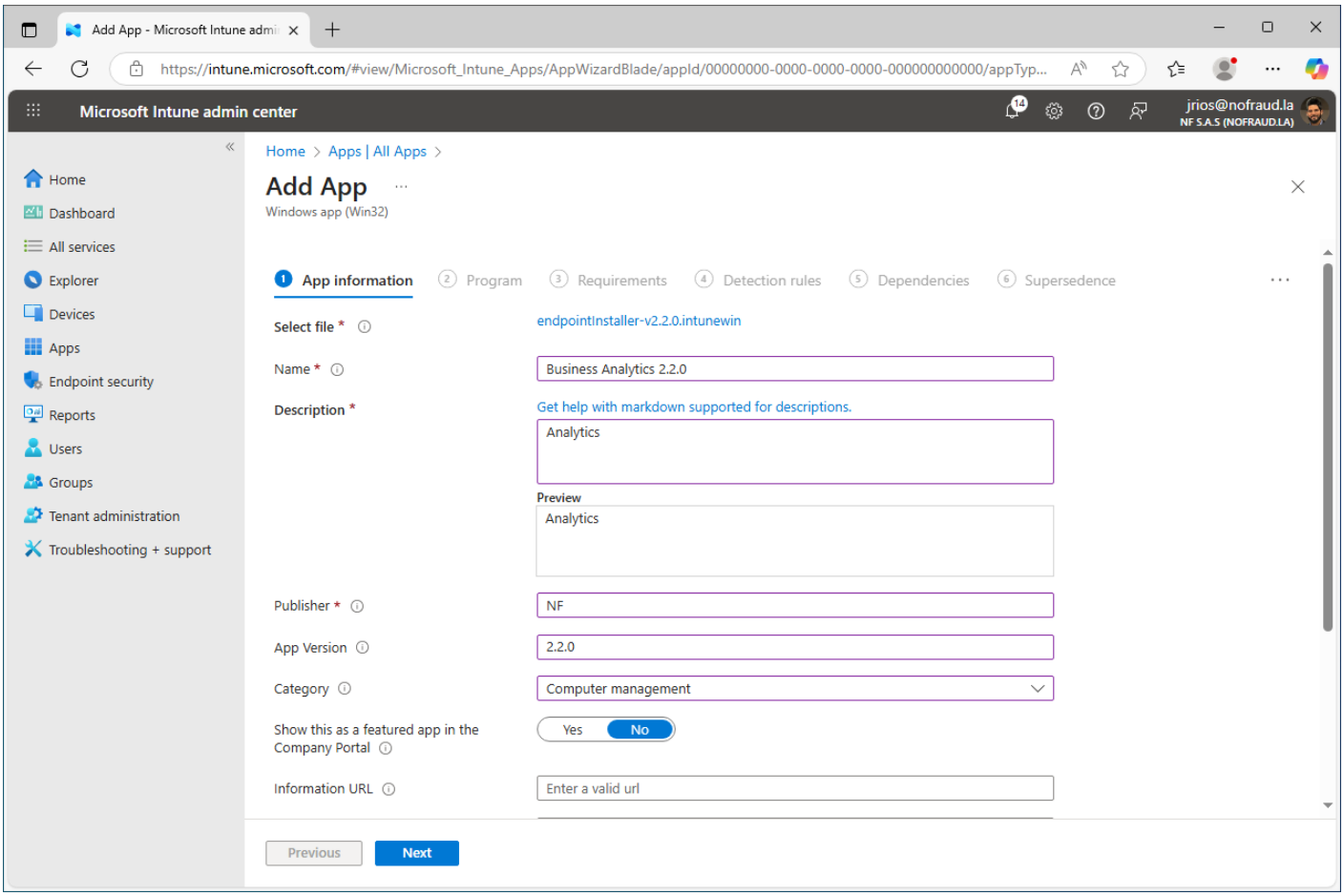
Navegue en sus archivos y carpetas para seleccionar el archivo **endpointInstaller-v2.2.0.intunewin** y añádalo como paquete de instalación.



Automáticamente se detectará que el paquete es válido y corresponde al formato propietario de **Microsoft intune**.

Información de la aplicación

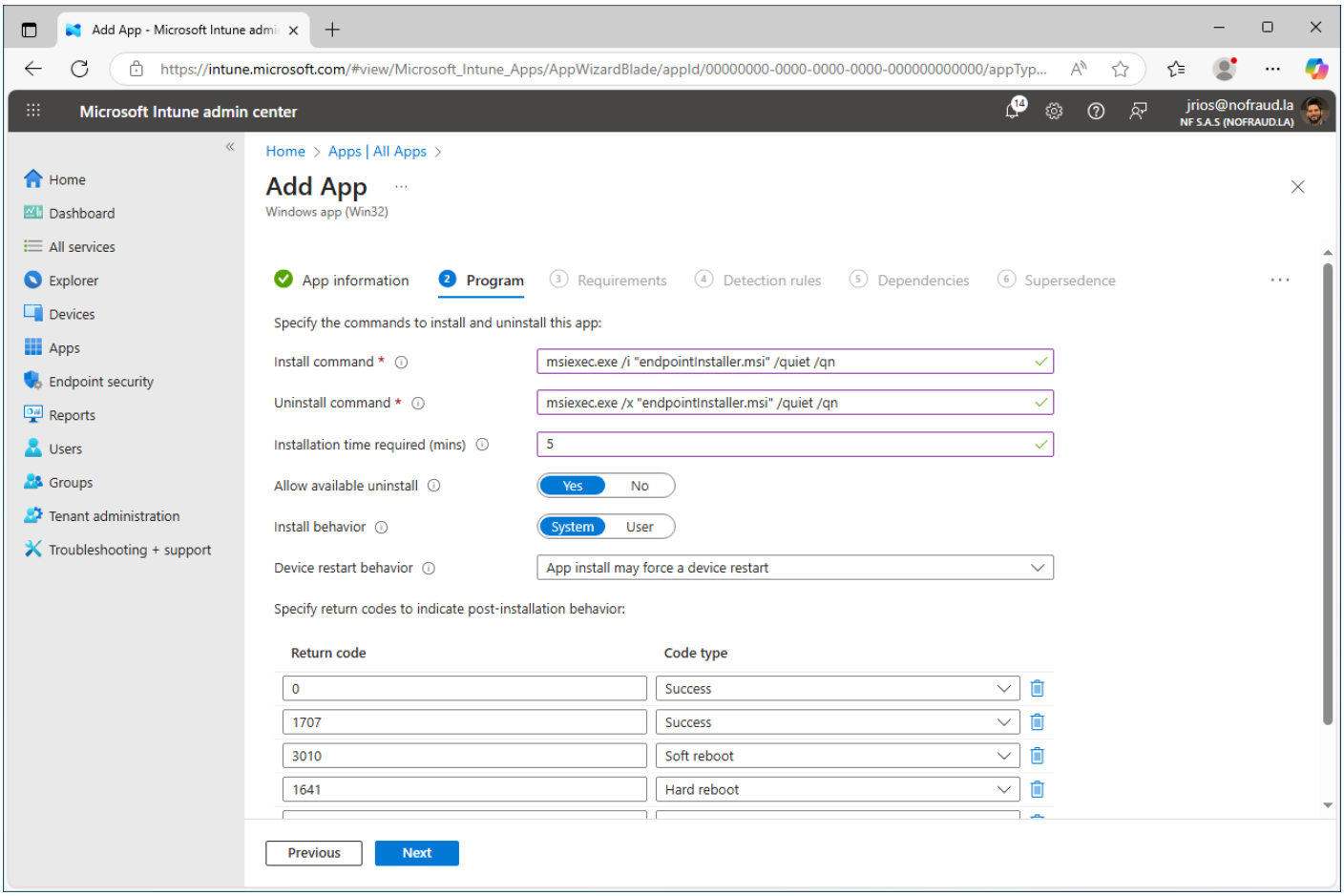
Escriba el nombre Business Analytics y llene la descripción y otros campos con datos informativos.



Asegúrese de que la opción de **mostrar esta aplicación en el portal de empresa** esté deshabilitada.

Comando de instalación

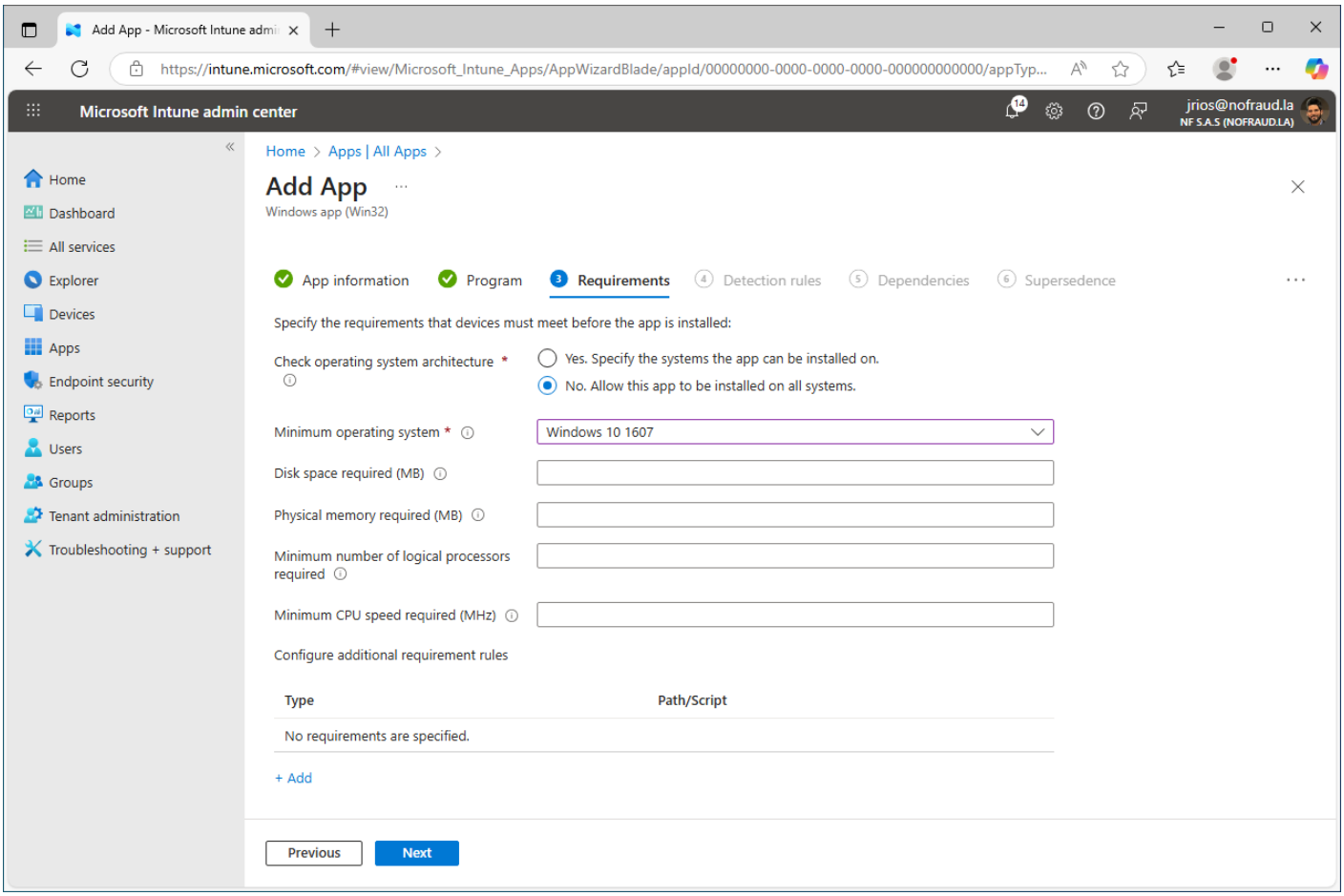
Escriba el comando de instalación y desinstalación como se muestra en la imagen. Asegúrese de que endpointInstaller.msi esté dentro de comillas dobles.



Cambie a 5 minutos el tiempo necesario de instalación para la aplicación y asegúrese de que el **Install Behavior** este marcado en **System**.

Requisitos de instalación

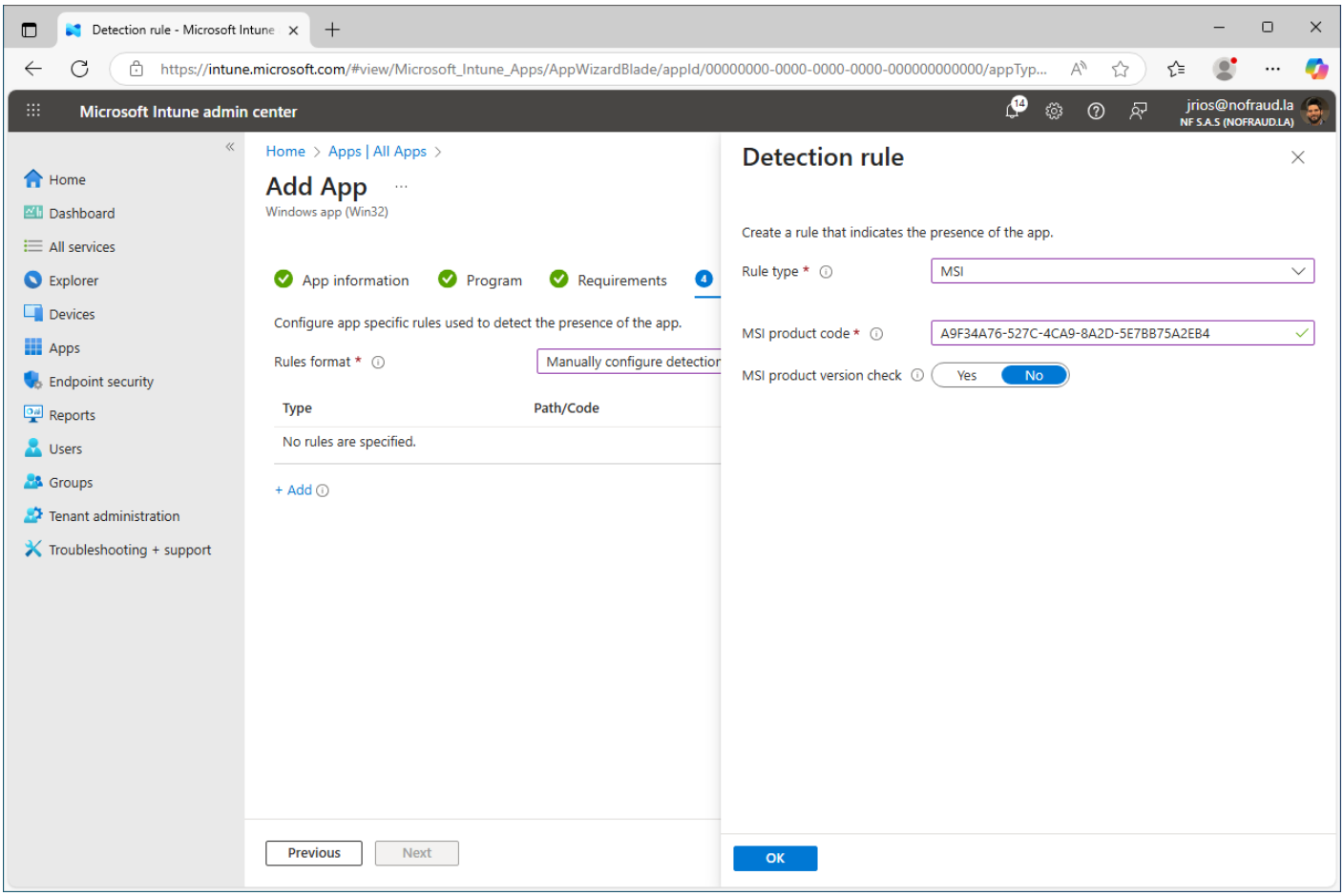
Microsoft Intune requiere que se le especifique cuál es la versión del sistema operativo compatible con nuestra aplicación. En este caso elegimos Windows 10 en su versión 1607, que es la versión mínima que soporta **Microsoft Intune**.



Se deja en blanco cualquier otra información, como espacio en disco, memoria o procesadores y se da clic en **Next**.

Regla de detección

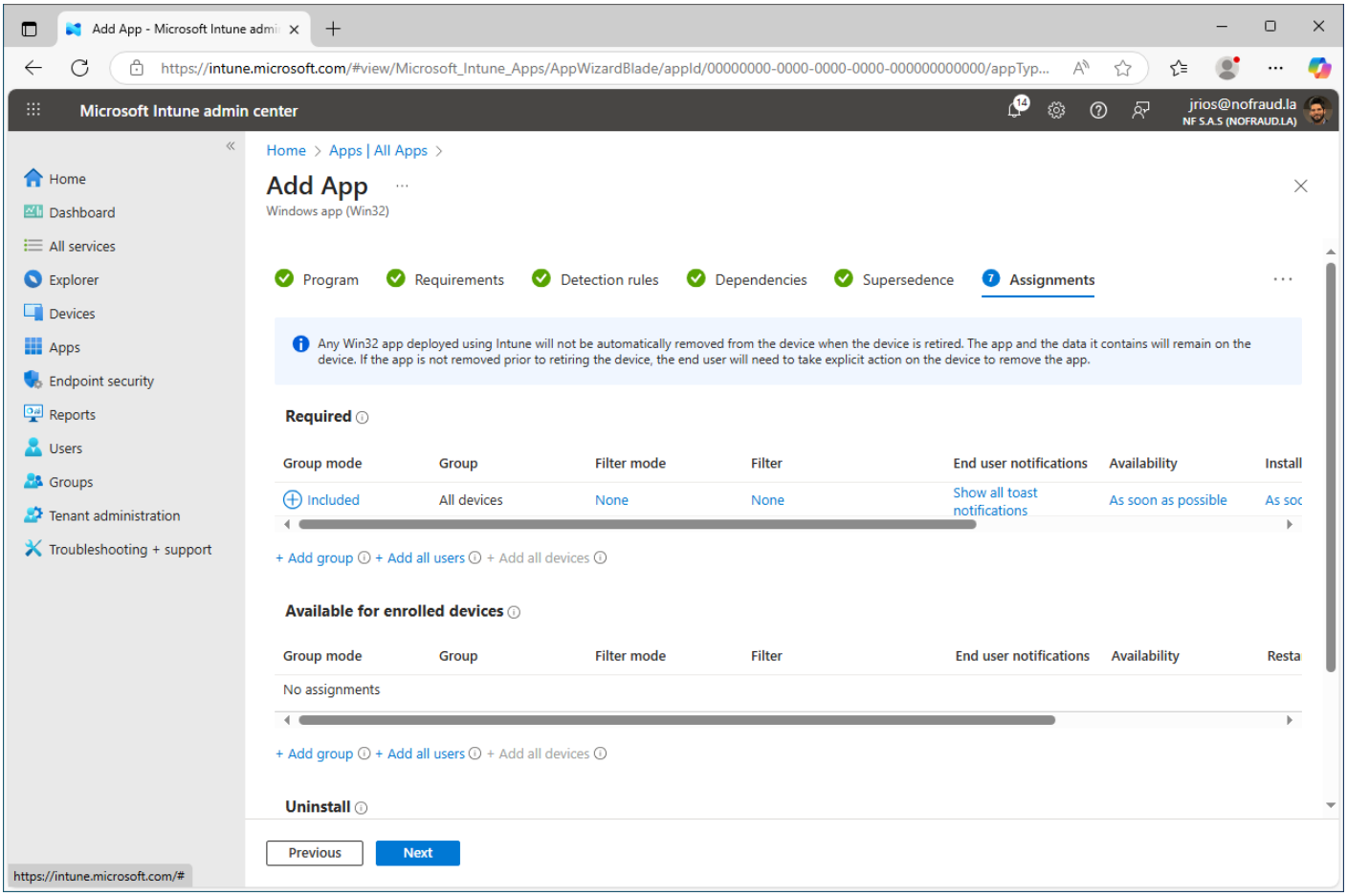
La regla de detección se usa para que Microsoft Intune pueda identificar si la aplicación está instalada o no en los computadores. En esta ocasión se debe seleccionar que la regla estará basada en el código del producto del MSI del agente antifraude.



Para saber cuál es el código del producto, puede usar la herramienta **Microsoft Orca**, aunque en NOFRAUD se le estregará toda esta información a la hora de iniciar el proyecto.

Asignación de usuarios o máquinas

Existen 3 secciones en las asignaciones, una llamada **Required**, otra llamada **Available for enrolled devices** y otra **Uninstall**. Dependiendo de la operación a realizar, se agregar usuarios o máquinas a una de ellas. En este caso, se agregarán todas las máquinas a la categoría **Required** porque se requiere que esta aplicación se instale en todas las máquinas.

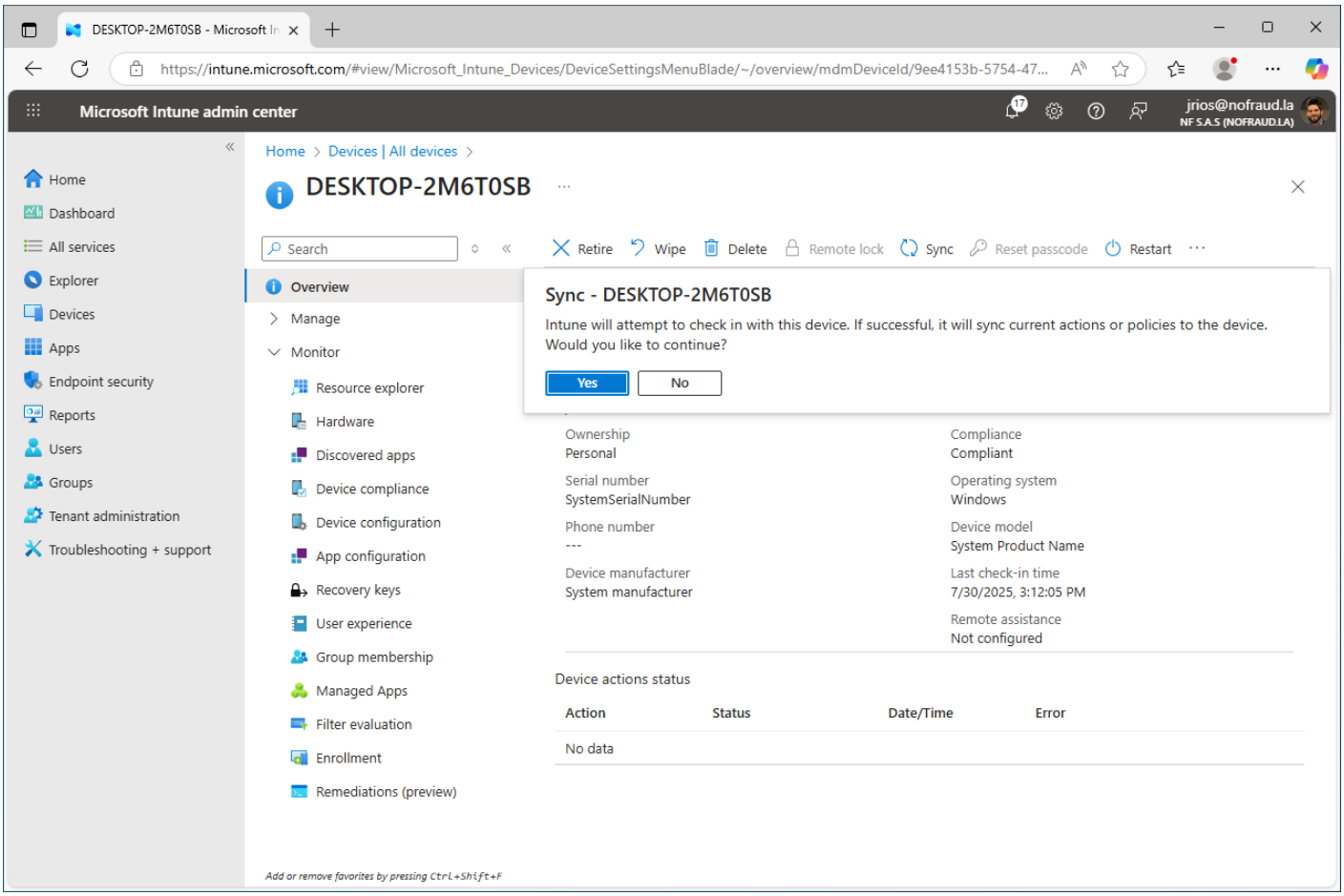


En su organización podrá suceder que no se quiera desplegar el agente antifraude a todas las máquinas, por ello, deberá crear un grupo y agregar como miembros aquellos dispositivos o usuarios que serán objeto de la metodología antifraude.

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

Sincronización de dispositivo

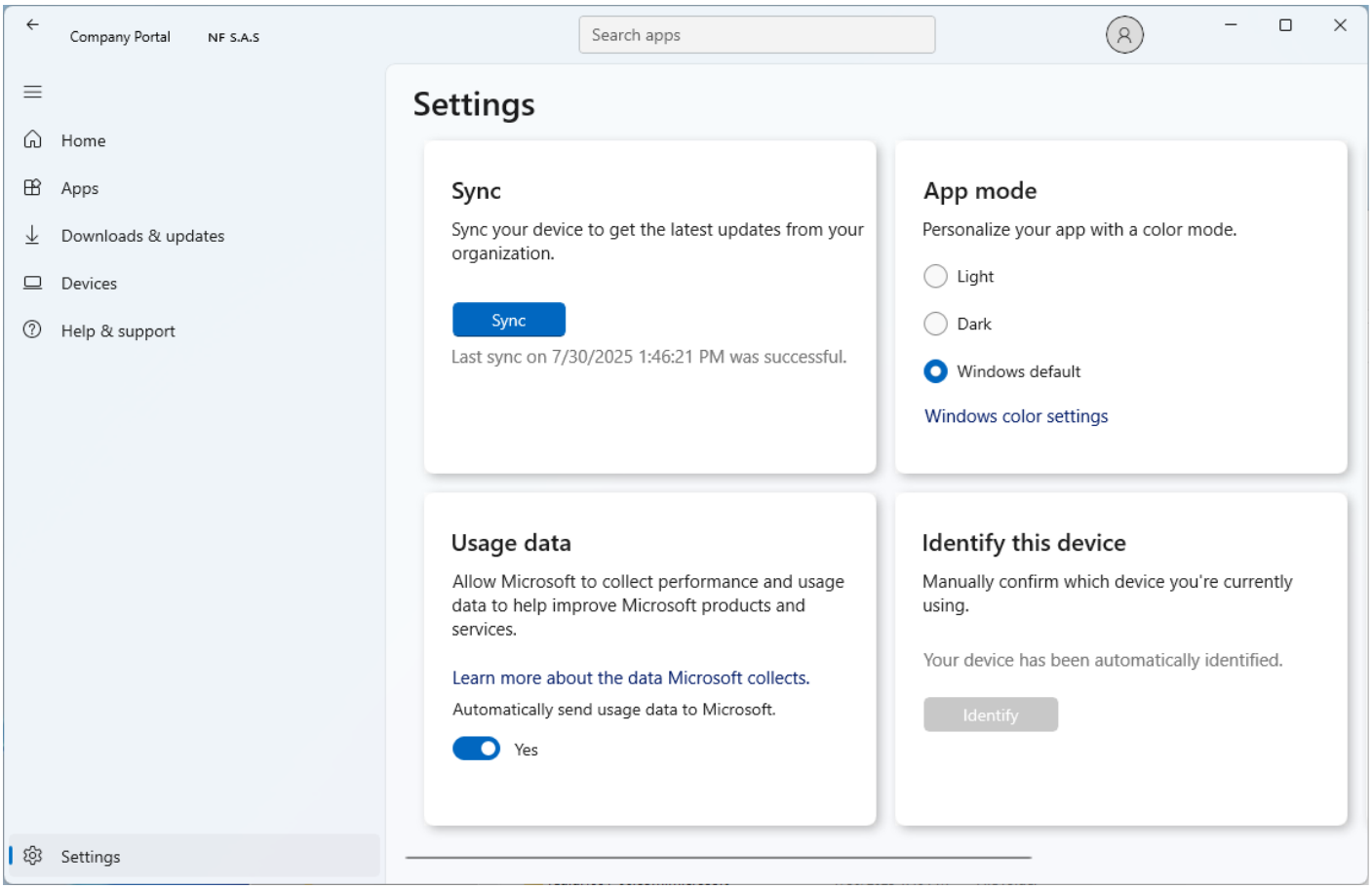
Para forzar la aplicación de la política del lado de **Microsoft Intune**, debe dar clic en **Devices**, luego en **All Devices**, seleccionar la máquina donde desea forzar la aplicación de la política y luego en el botón **Sync**.



El siguiente paso será forzar la sincronización del lado de las máquinas.

Sincronizar cliente Windows

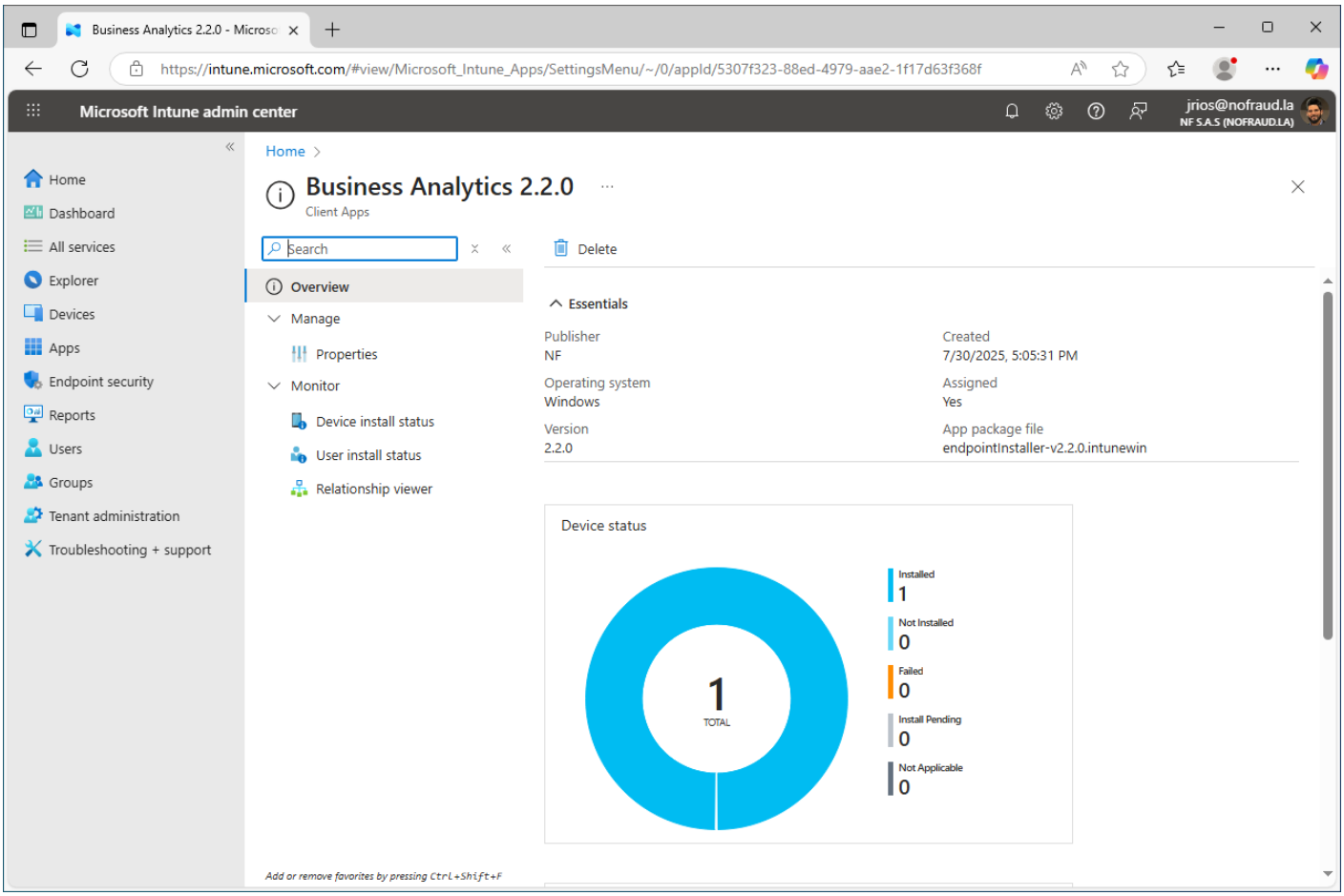
Si desea que la política se aplique de inmediato en alguna máquina cliente Windows, deberá ingresar a esa máquina por escritorio remoto y ejecutar la aplicación **Company Portal**.



Una vez que esté en la aplicación, de clic en **Settings** y luego en el botón **Sync**. Esto forzará la aplicación de la política e instalará el agente antifraude de manera inmediata en esta máquina.

Monitoreo de la instalación

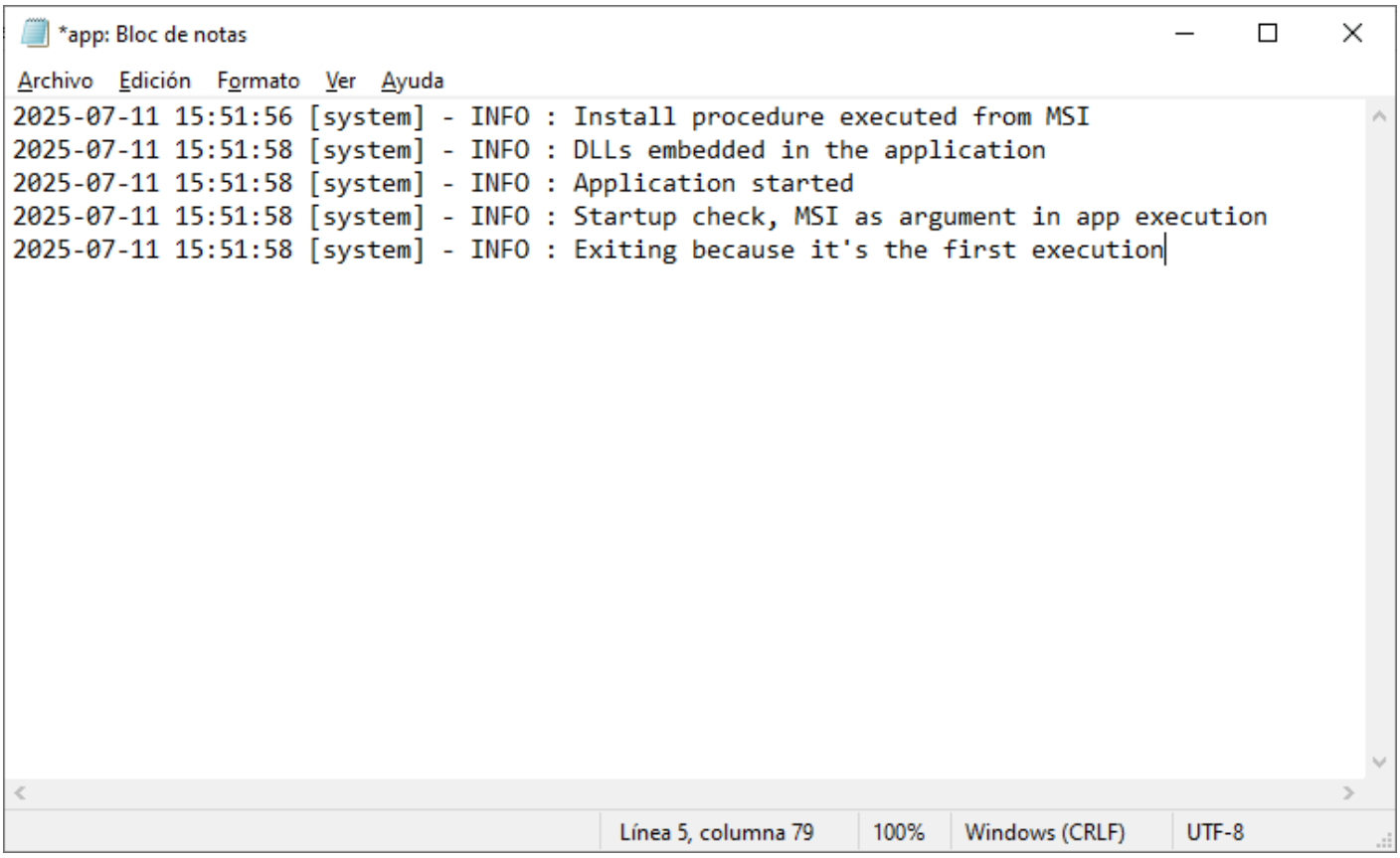
Para monitorear el estado de la instalación, de clic en en **Apps**, **All Apps** y seleccione **Business Analytics**. Allí aparecerá un gráfico de torta indicando un resumen de las operaciones.



Este gráfico no se actualiza de manera inmediata, puede tardar un rato en aparecer que la aplicación ya fue desplegada con éxito.

Verificación de la instalación

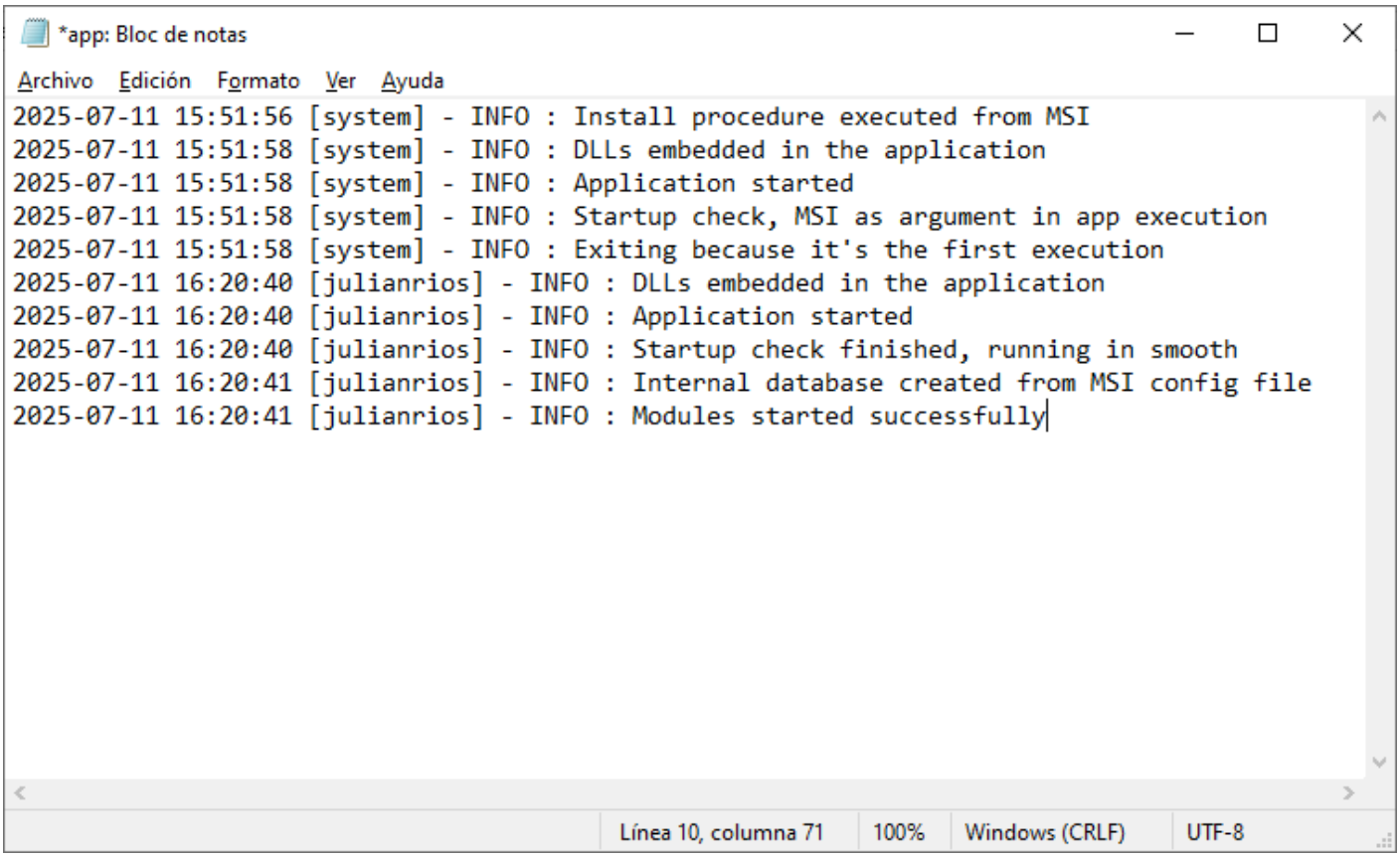
Para verificar la instalación se puede esperar a que en **Microsoft Intune** se muestre el nivel de cumplimiento por aplicación. Sin embargo si queremos verificar directamente en el PC, se debe abrir el archivo de log ubicado en **C:\ProgramData\Software\app.log** con el **blog de notas**.



En este log se puede ver que el usuario que instaló la aplicación es **system** y que además por se la primera ejecución no se inicia el agente. Esto es debido a que el agente está programado para que funcione con privilegios de usuario normal, no con privilegios de administrador ni system por seguridad.

Reinicio del PC

Para que el agente de The Fraud Explorer empiece a funcionar, se debe reiniciar el PC. Una vez reiniciado el PC se puede volver a a abrir el archivo C:\ProgramData\Software\app.log donde se verá información sobre su primera ejecución.

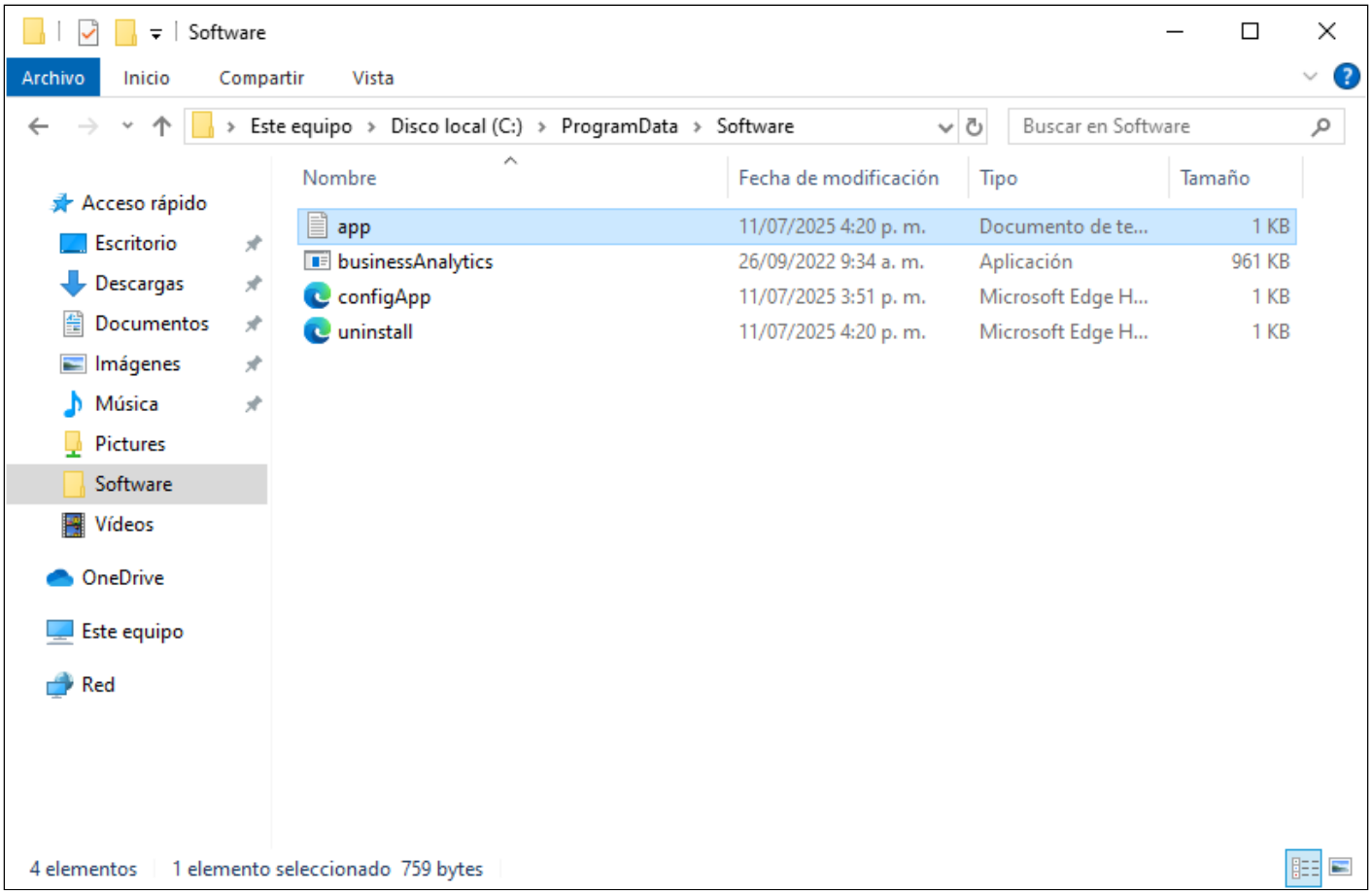


Como se observa, ya la ejecución se hace con un usuario normal sin privilegios elevados y de esa manera el agente de The Fraud Explorer lo detecta y procede a arrancar diciendo **Modules started successfully**.

El agente de The Fraud Explorer está configurado internamente para no permitir que se arranque con usuario administrador ni system.

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**.

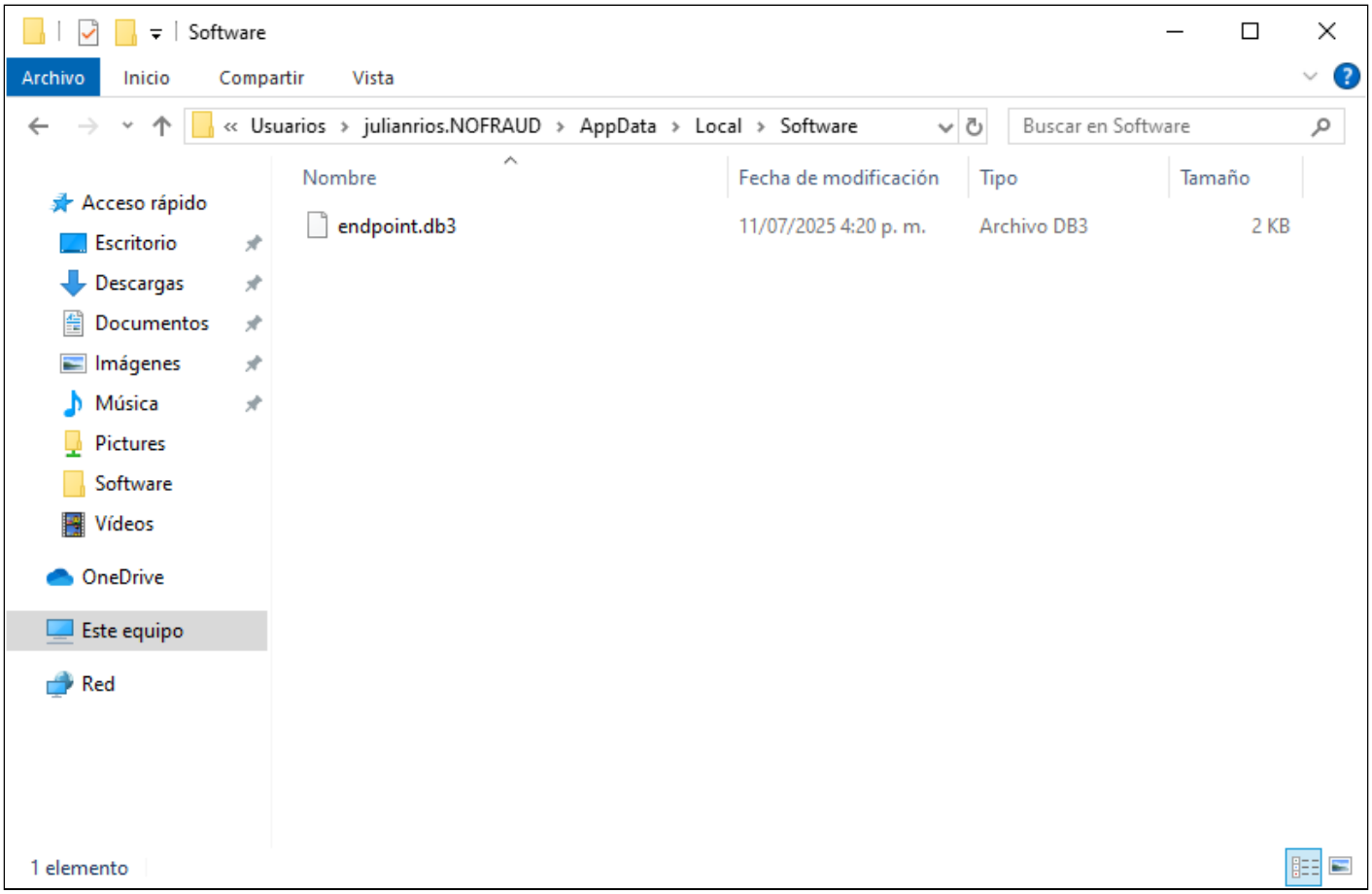


En caso de tener que agregar excepciones en el antivirus, el contenido de esta carpeta debería incluirse en las reglas de excepción o para la regla de ejecución el binario **businessAnalytics.exe** .

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.

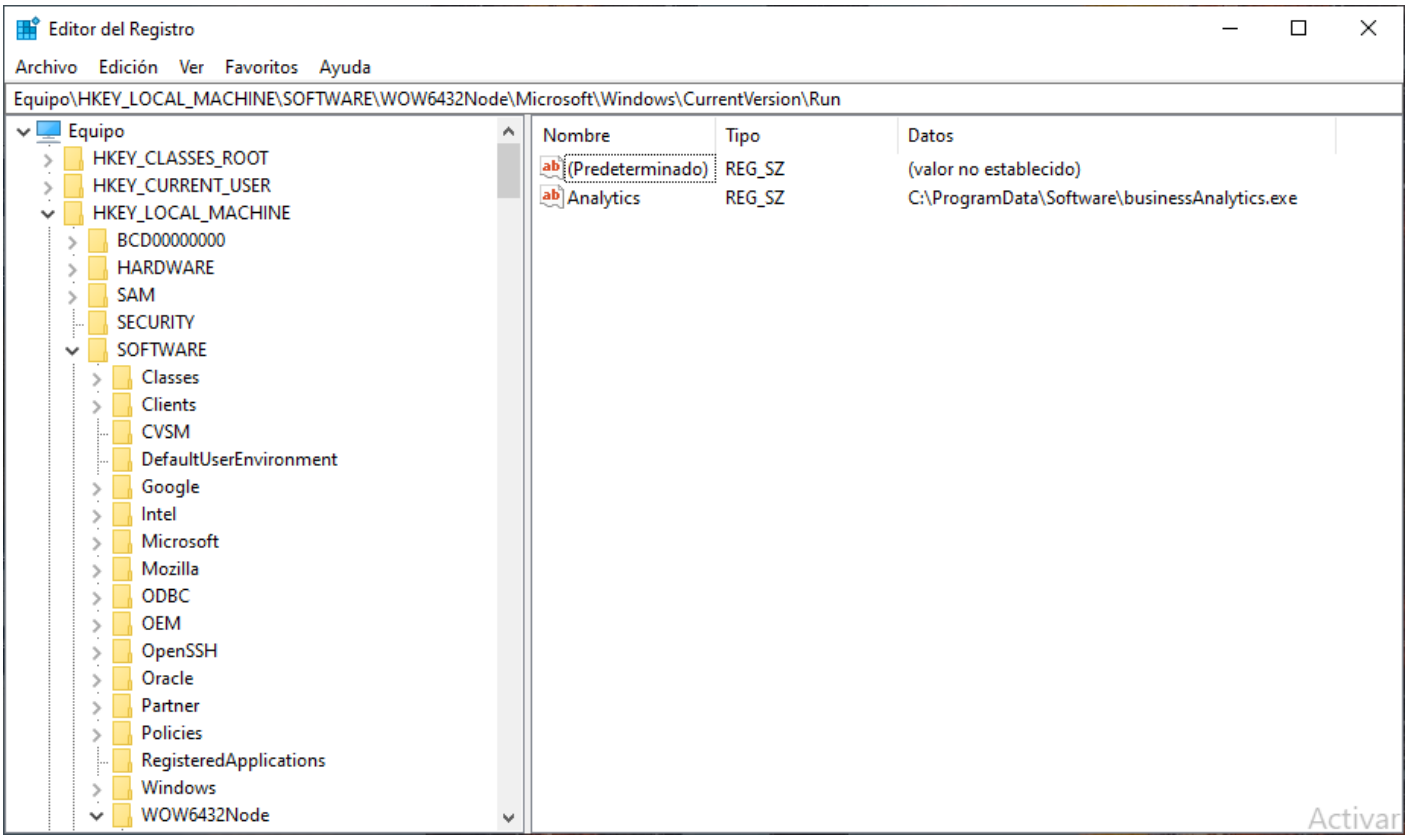


En este archivo se almacena configuración como la dirección del servidor, las llaves de cifrado para la comunicación con la consola central y otra información relevante para su funcionamiento.

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**.

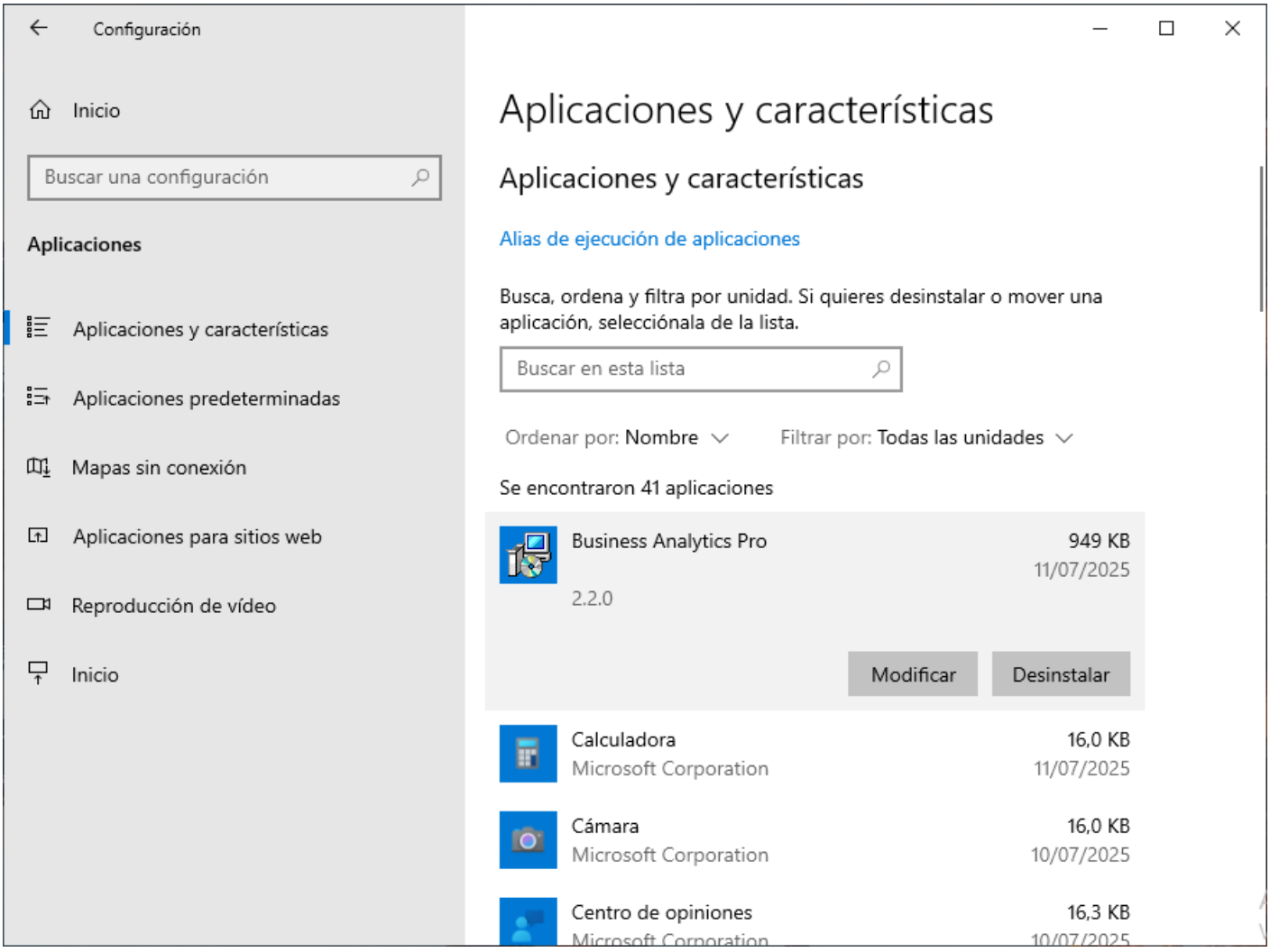


Esta entrada garantiza que el agente inicie cada vez que el dispositivo sea reiniciado. El agente de The Fraud Explorer no crea ninguna otra entrada en el registro de Windows aparte de esta.

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**.



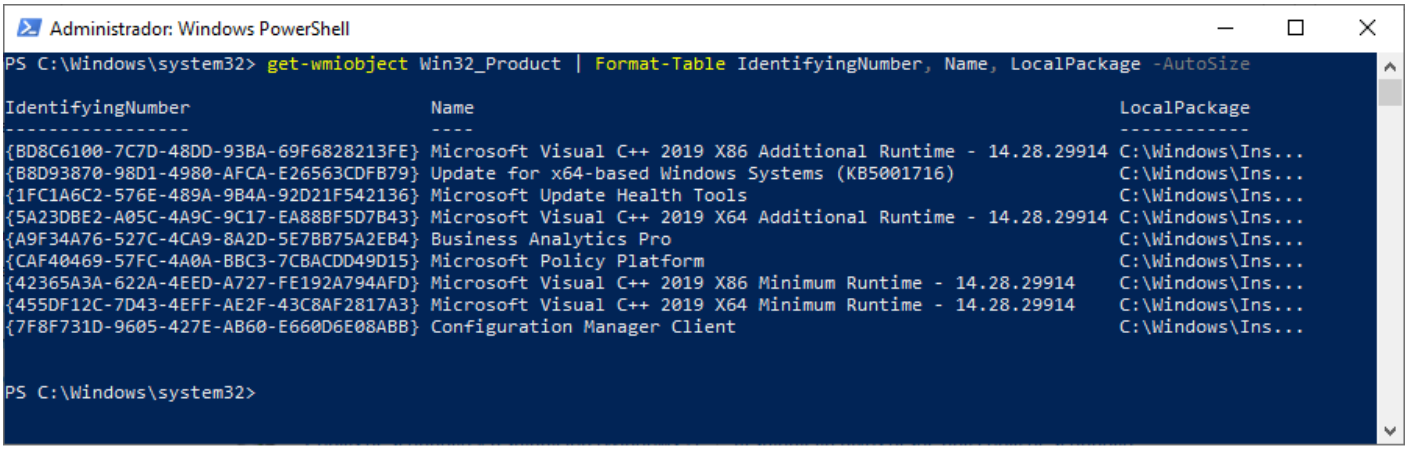
Junto con el nombre de la aplicación aparece también la versión del agente. Cuando se realiza una actualización, no se crean entradas nuevas sino que se re-emplaza la actual con la nueva versión.

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

ProductID con PowerShell

Se puede verificar la instalación del agente de The Fraud Explorer a bajo nivel con **PowerShell**. Para ello debe ejecutar el siguiente comando en modo administrador:

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

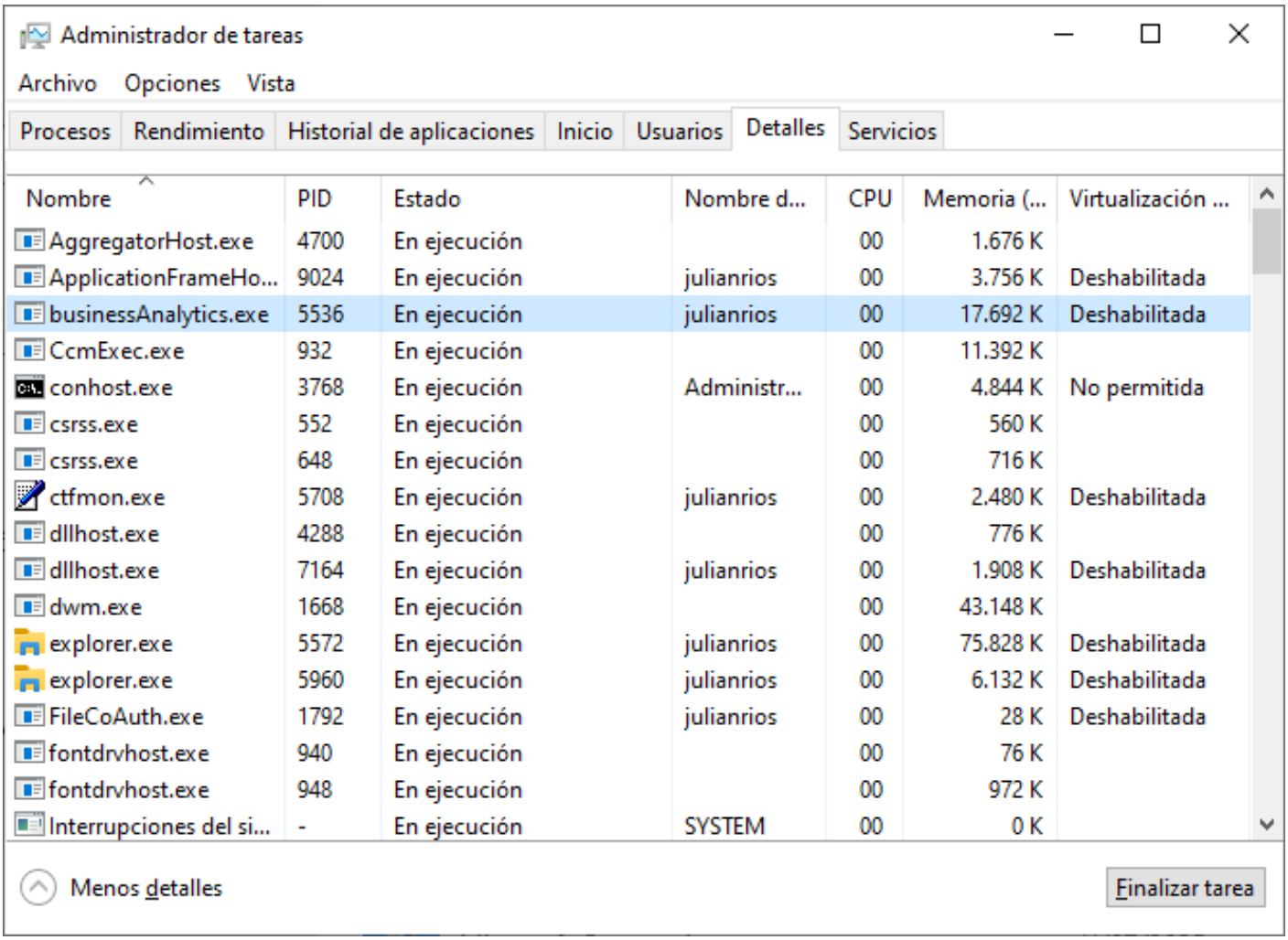


El comando mostrará información relevante como el nombre del producto, el ID del producto y la ubicación del archivo MSI dentro del caché de archivos de instalación de Windows.

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

Monitoreo del agente

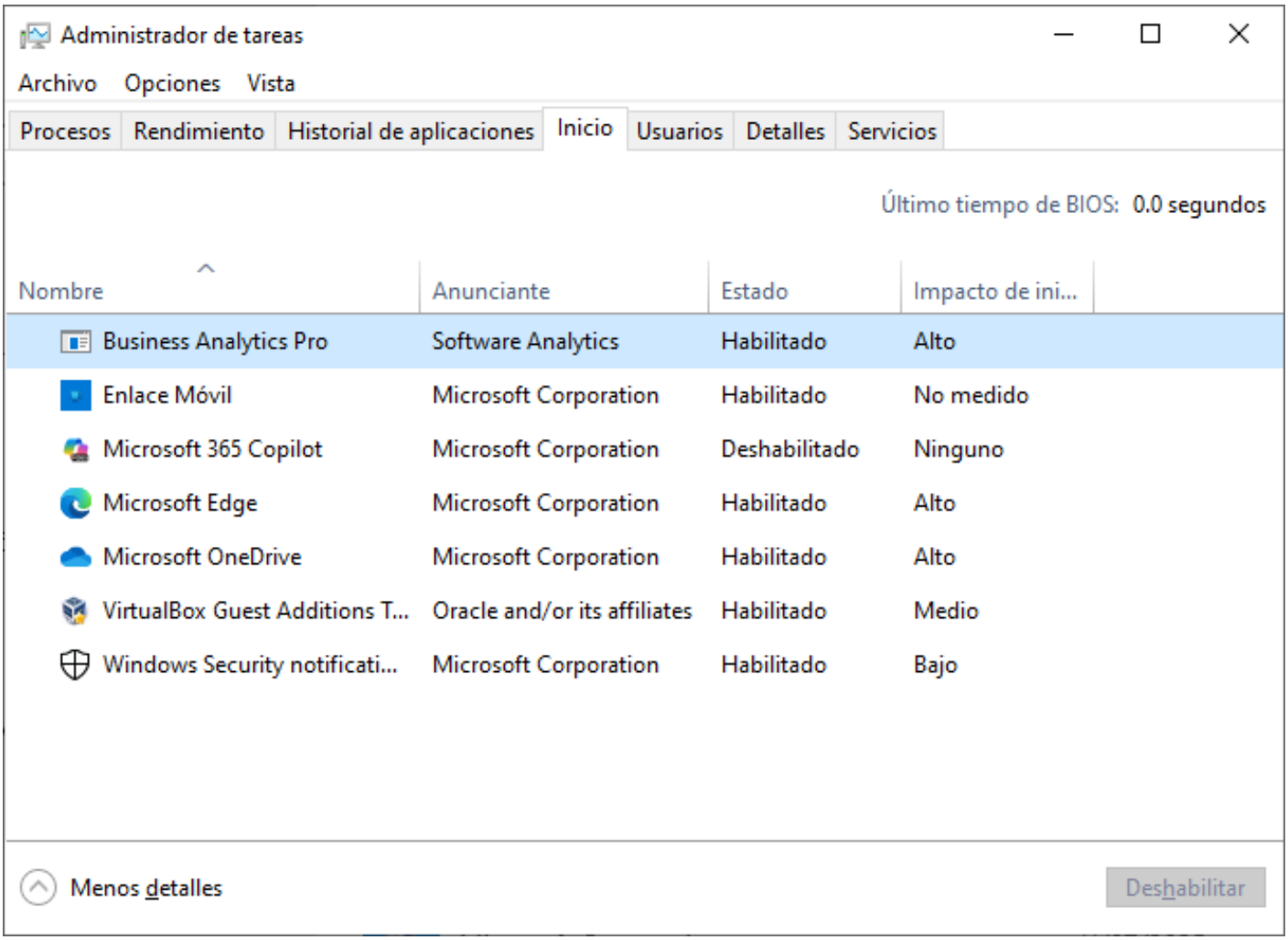
En el PC del usuario, se puede abrir el **Administrador de tareas** y en la pestaña **Detalles** buscar el ejecutable **businessAnalytics.exe**.



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.

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**.



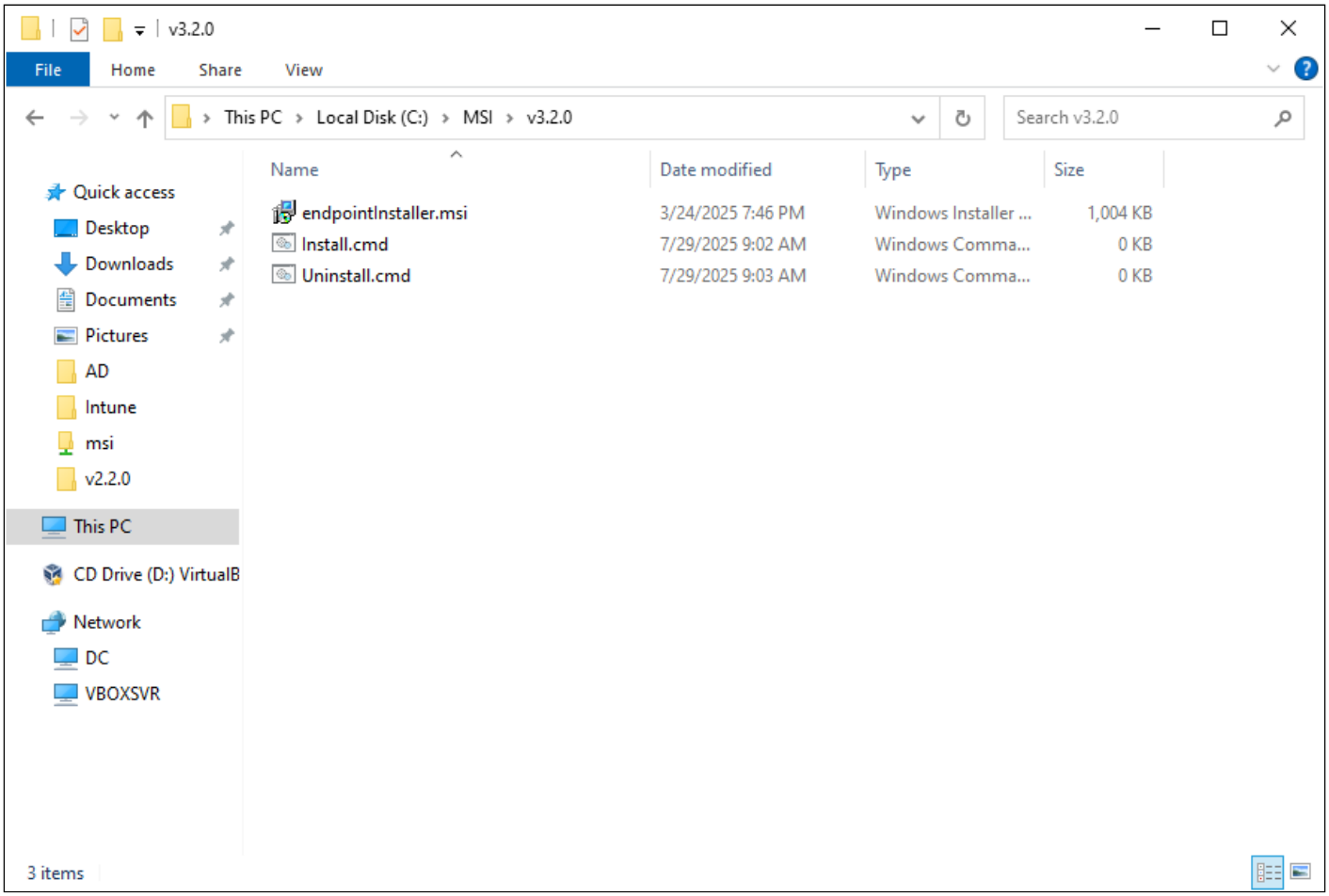
En esta ventana se muestran todas las aplicaciones que arrancan cuando el usuario inicia sesión con su cuenta en Windows. El agente de The Fraud Explorer no arranca como servicio y no interfiere en el proceso de arranque de sistema operativo.

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.

Carpeta para actualizar el agente

Se debe crear la carpeta del nuevo agente con la nueva versión. Para este caso se llamará **v3.2.0** y en ella se colocará el archivo MSI del agente **endpointInstaller.msi** y se deberán crear dos archivos en blanco, uno llamado **Install.cmd** y el otro **Uninstall.cmd**.

Esta carpeta se crea así para cumplir con las normas del tipo de paquete **IntuneWin**, que se necesita crear para hacer nuestro agente antifraude compatible con **Microsoft Intune**.

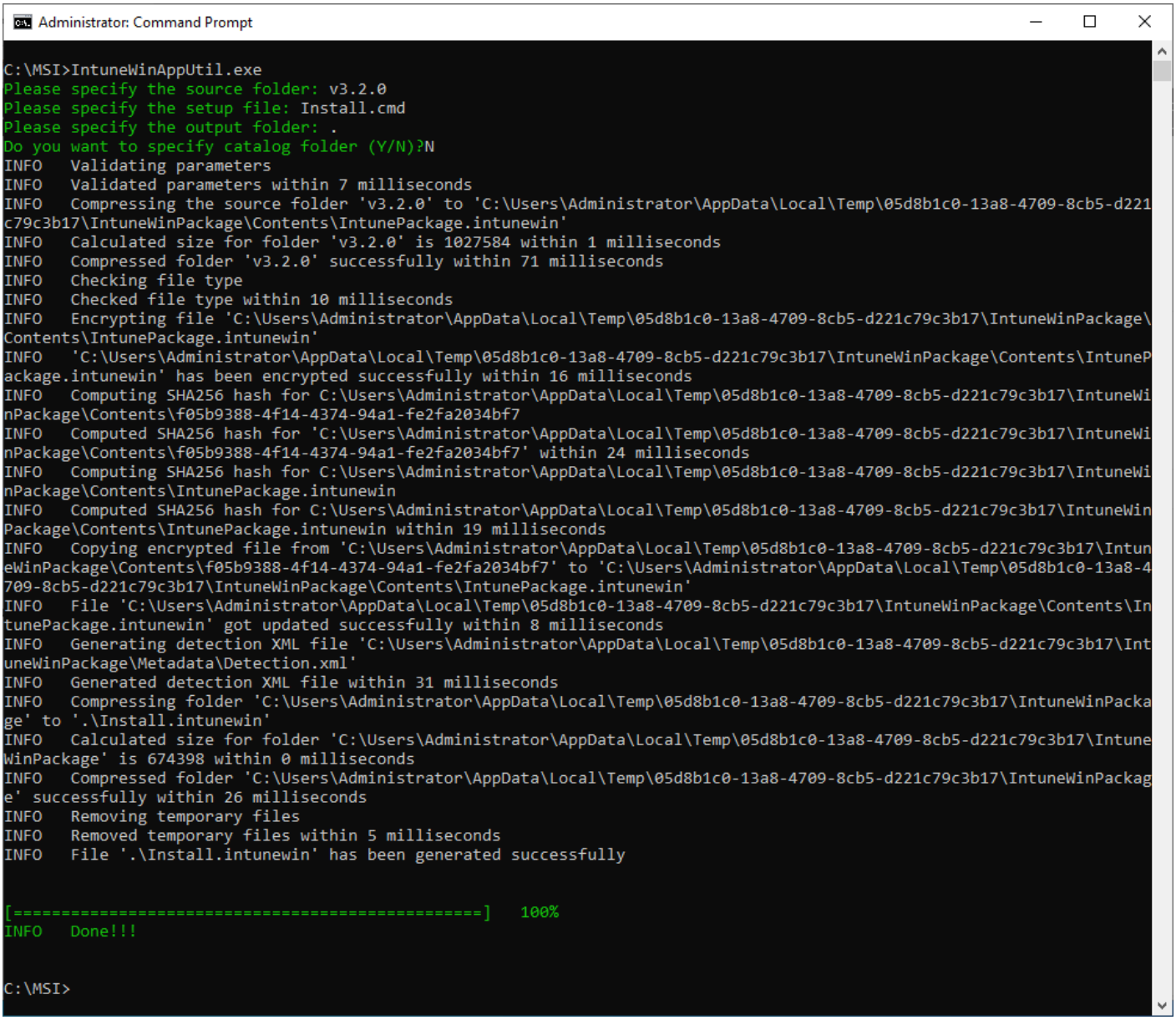


Una vez creada esta estructura, se podrá proceder a crear el paquete como se indica a continuación.

Paquete de actualización

Se debe abrir una consola MS-DOS y navegar hasta la carpeta C:\MSI donde se encuentra la estructura de carpetas compatibles con los paquetes de Microsoft Intune. Una vez allí se ejecuta el comando:

```
IntuneWinAppUtil.exe
```

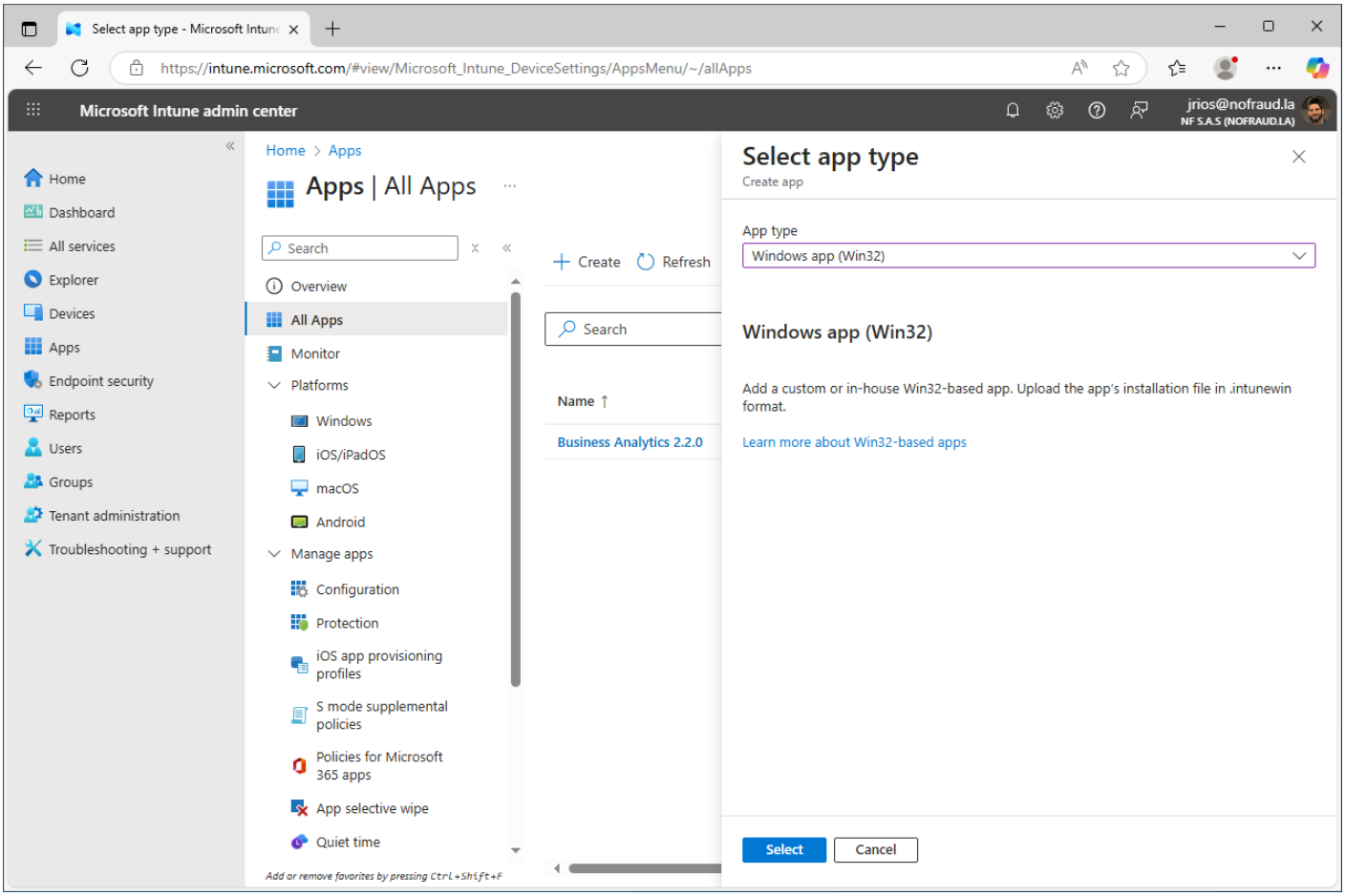


Cuando pregunte por la carpeta origen, escriba **v3.2.0**, cuando pregunte por el archivo de configuración escriba **Install.cmd**, cuando pregunte por la carpeta de destino escriba **un punto** y al final escriba **N** cuando se le pregunte por el catálogo. Este proceso creará un archivo llamado **Install.intunewin** que deberá ser renombrado a **endpointInstaller-v3.2.0.intunewin** para mejor recordación.

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

Aplicación para la actualización

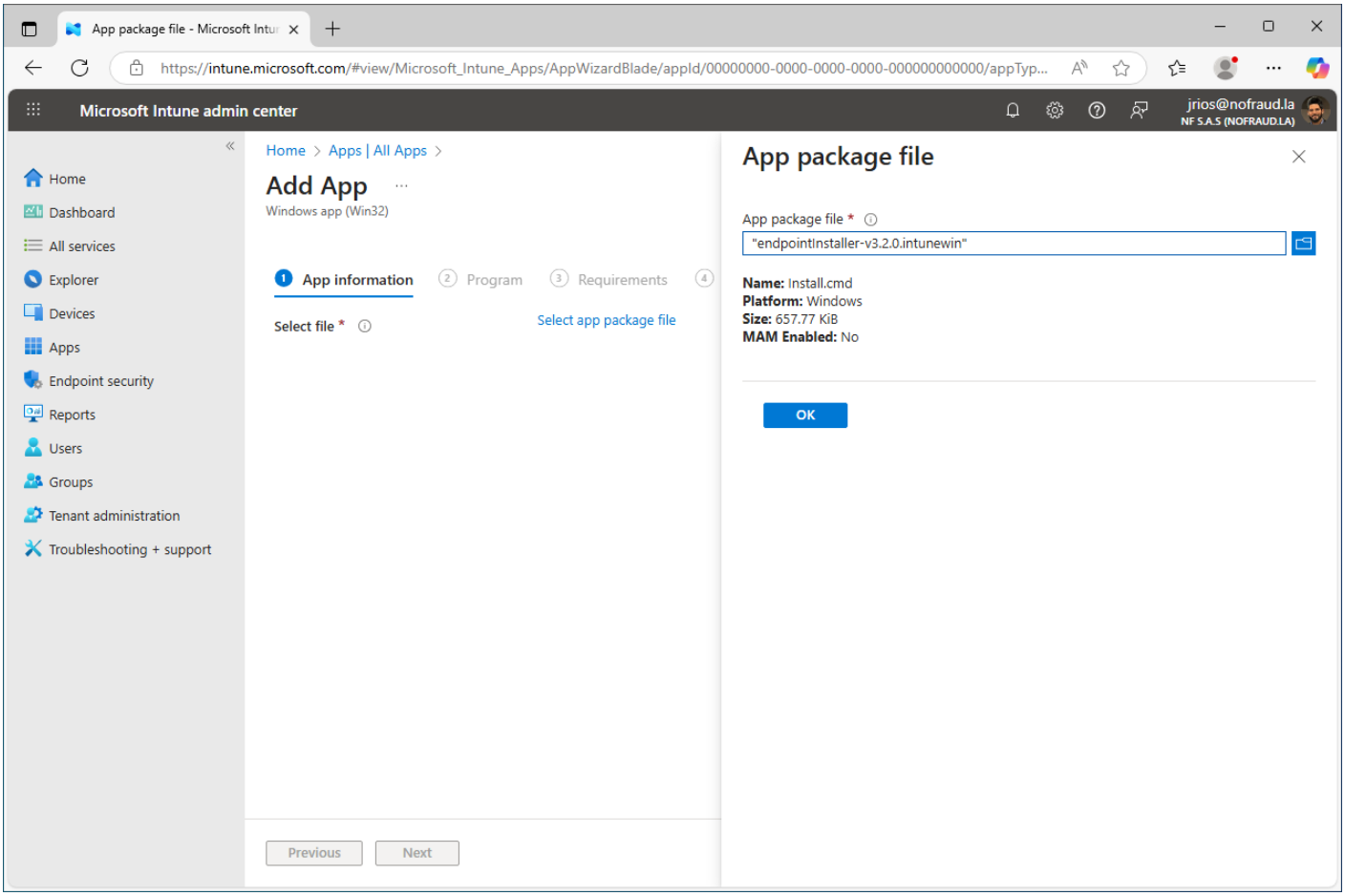
En la plataforma de **Microsoft Intune**, dar clic en **Apps**, **All Apps** y luego en el botón **Create**.



Allí seleccione que la aplicación es de tipo **Windows app (Win32)** y de clic en **Select**.

Seleccionar paquete de actualización

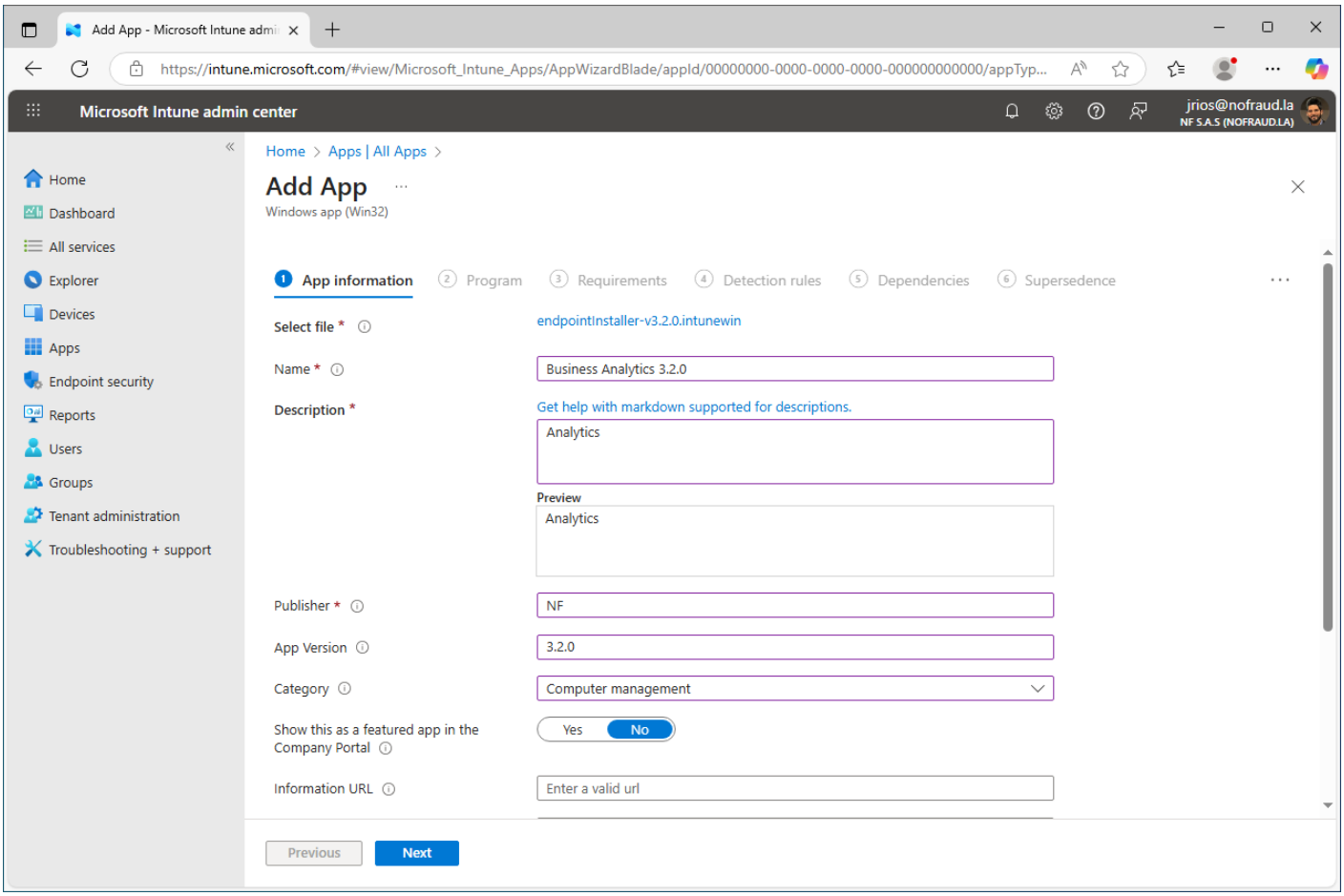
Seleccione el archivo que acabó de crear llamado **endpointInstaller-v3.2.0.intunewin**.



De clic en **OK** para continuar con el proceso.

Información de actualización

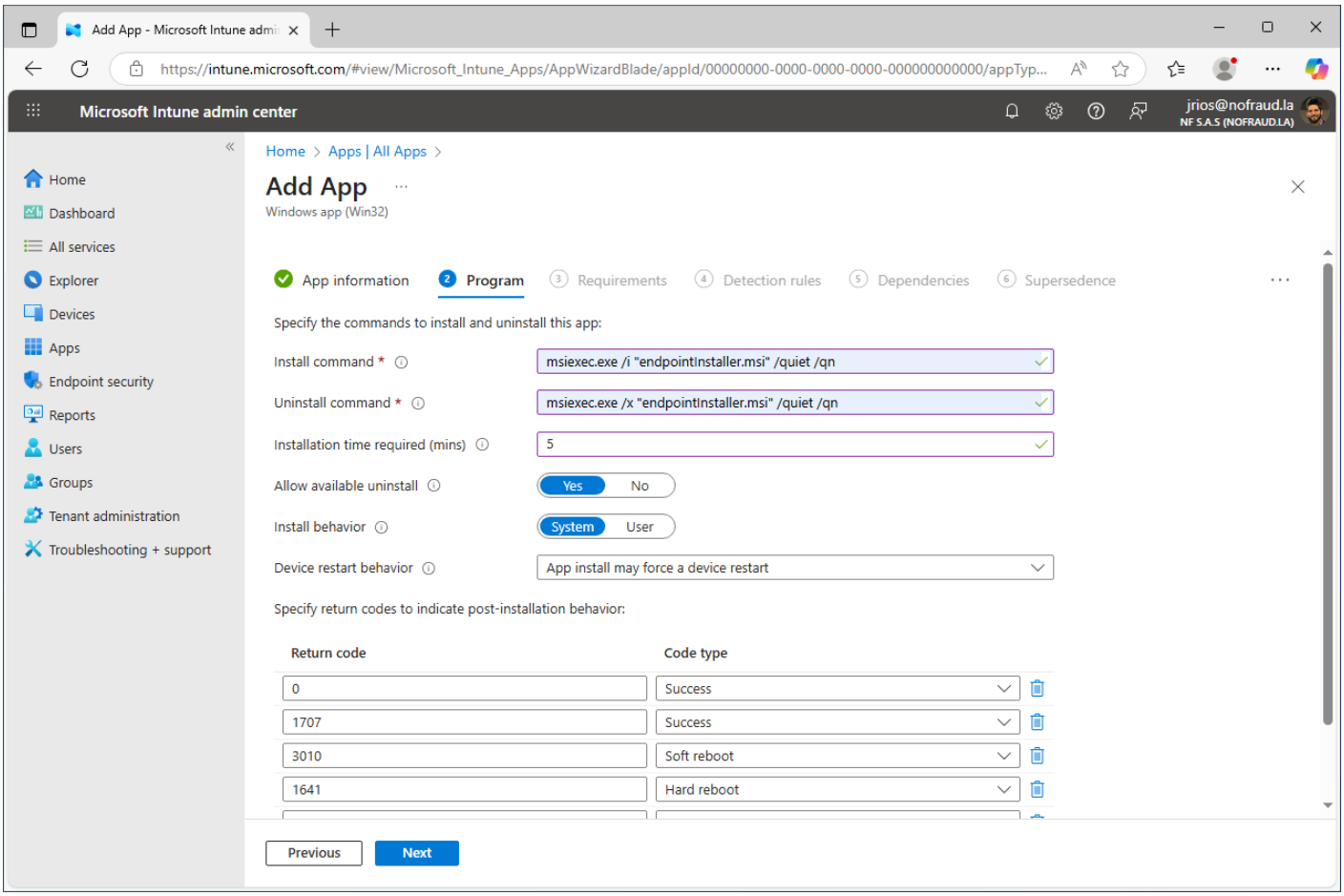
Escriba el nombre **Business Analytics 3.2.0** en el campo de nombre para diferenciar esta aplicación de la anterior.



Asegúrese de que la opción de mostrar esta aplicación en el portal de compañía este deshabilitada.

Comandos de actualización

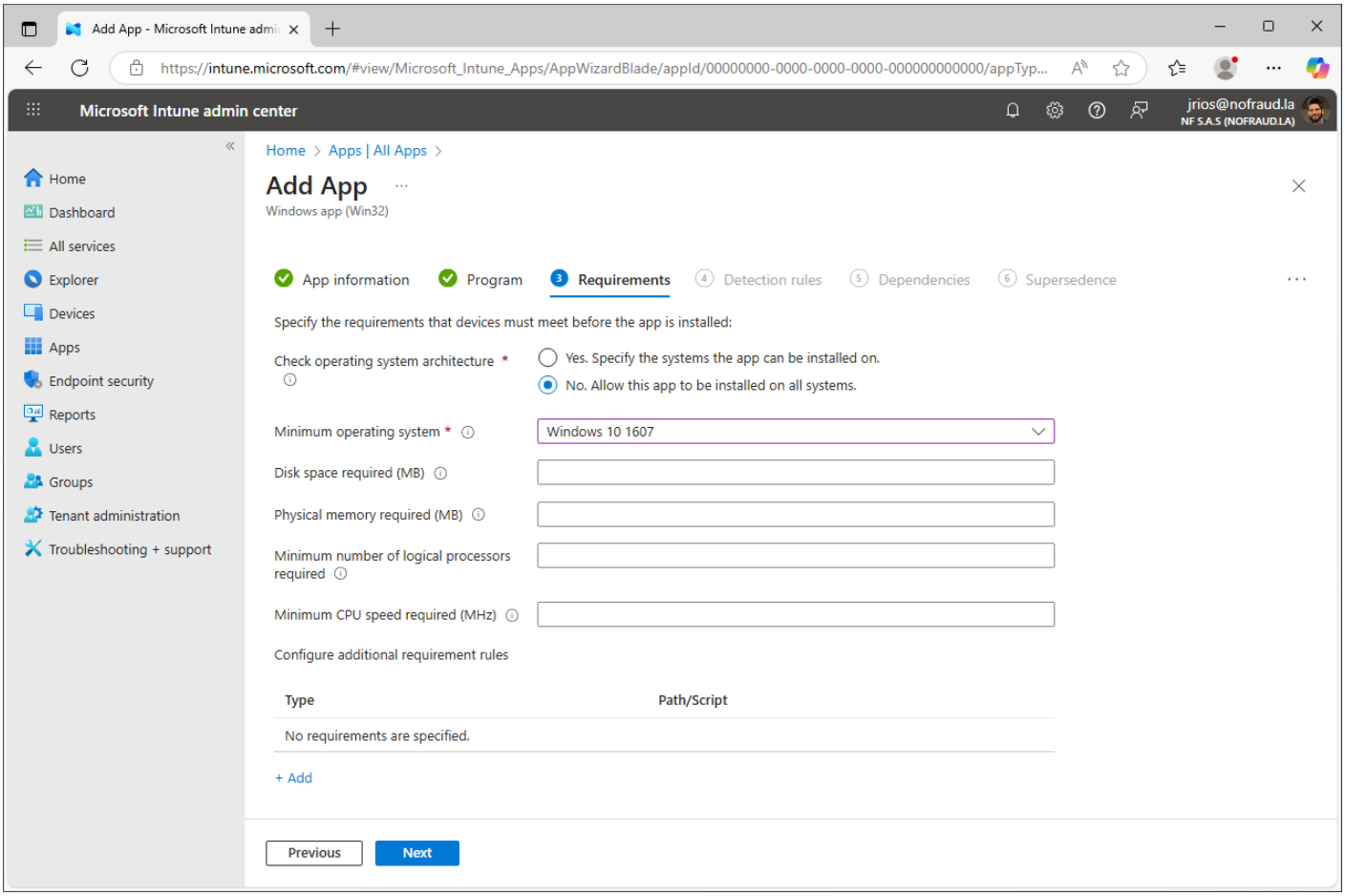
Asegúrese de escribir los comandos de instalación y desinstalación como se muestra en la imagen abajo.



Asegúrese también de que la opción de **Install Behavior** esté marcada como **System**.

Requerimientos de actualización

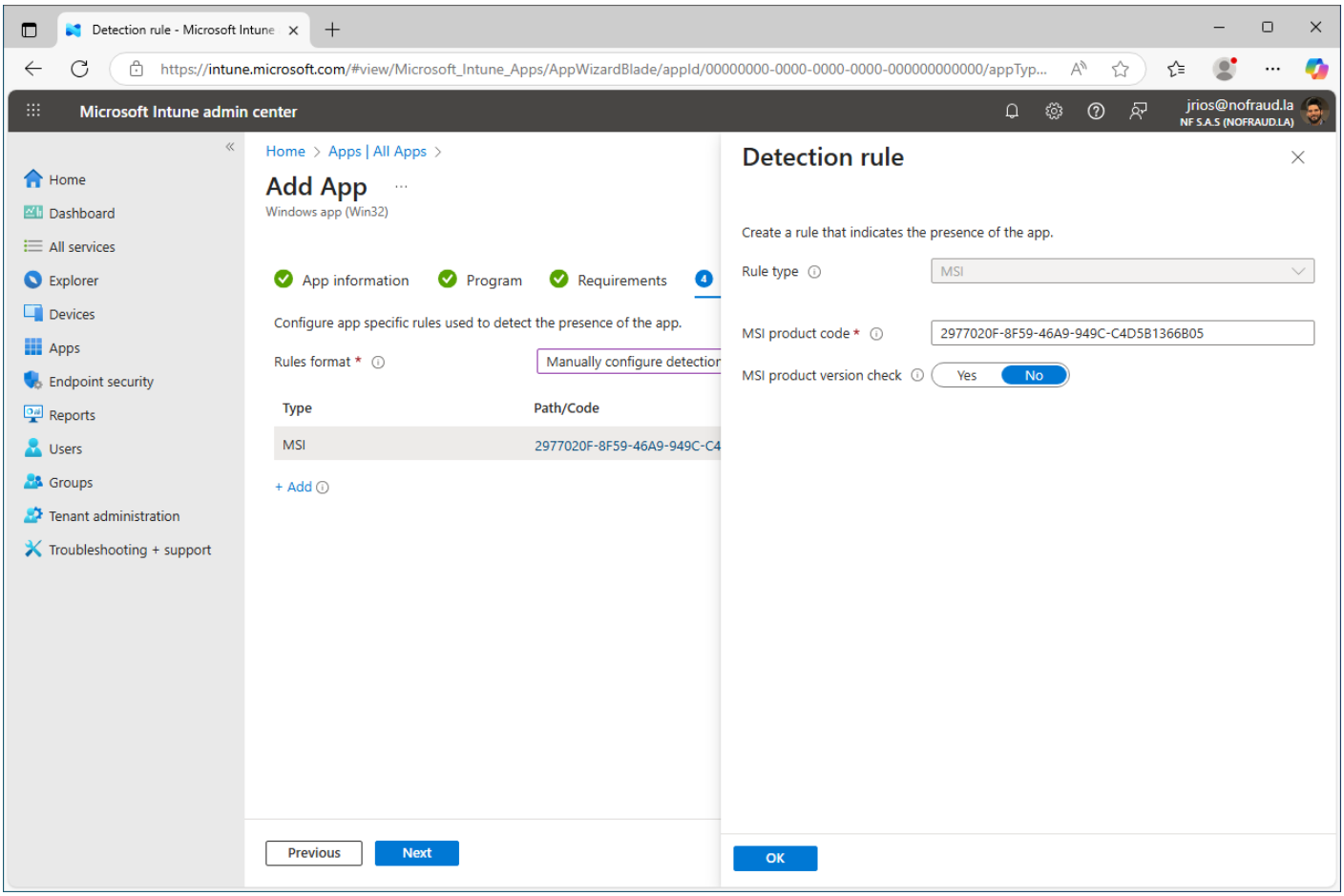
Microsoft Intune exige seleccionar como requerimiento una versión de Windows mínima, para este caso se selecciona Windows 10 1607.



El resto de opciones se deja en blanco y se da clic en el botón **Next**.

Reglas de detección

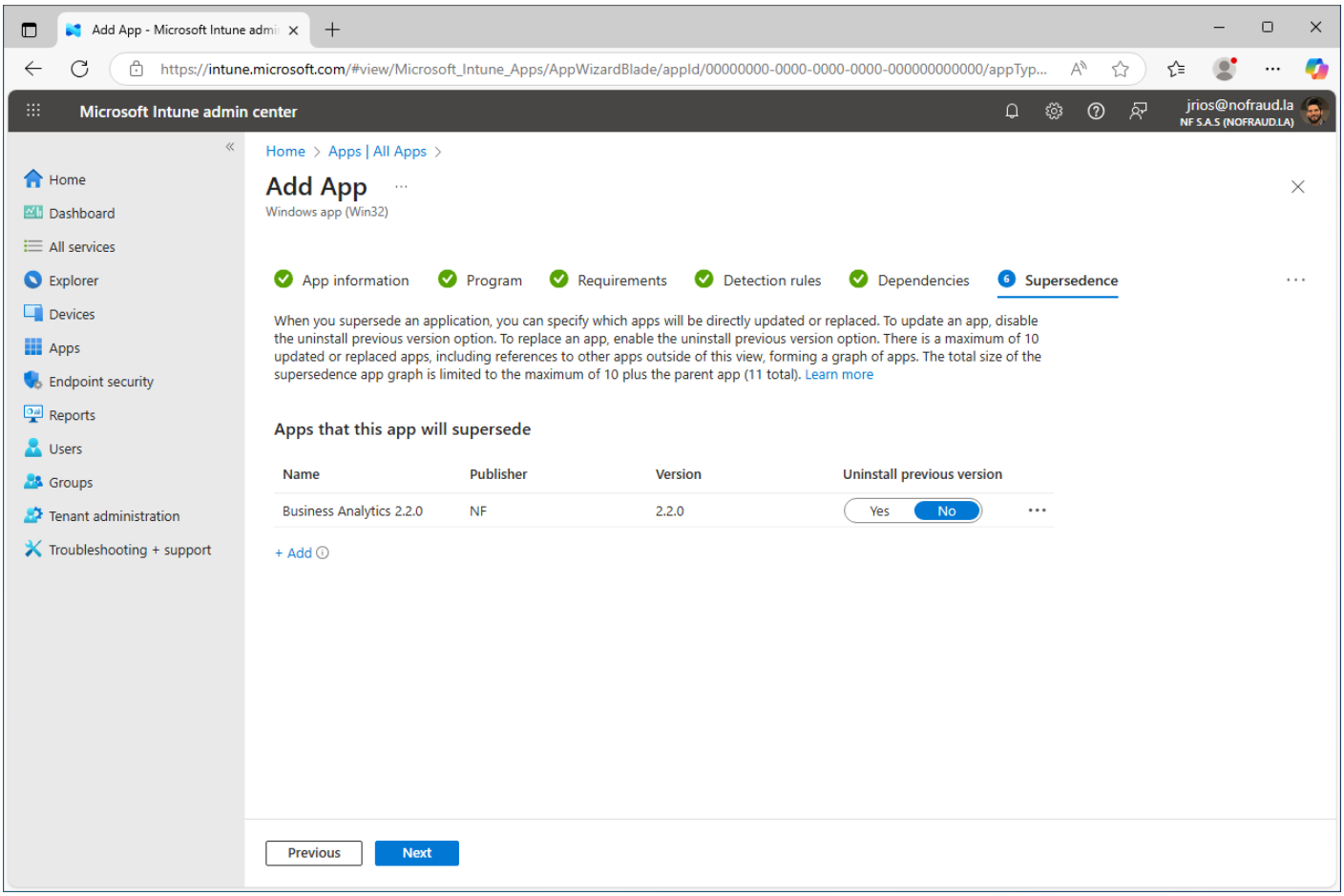
Microsoft Intune necesita que se le especifique cuál será la regla de detección mediante la cual se averiguará si la aplicación queda instalada o no. En este caso se especifica que la regla es a través del **código del producto** del MSI.



Este código del producto es proporcionado por NOFRAUD al momento de iniciar el proyecto, sin embargo, también puede usar la aplicación **Microsoft Orca** para abrir el MSI y ver el código del producto.

Supersedencia

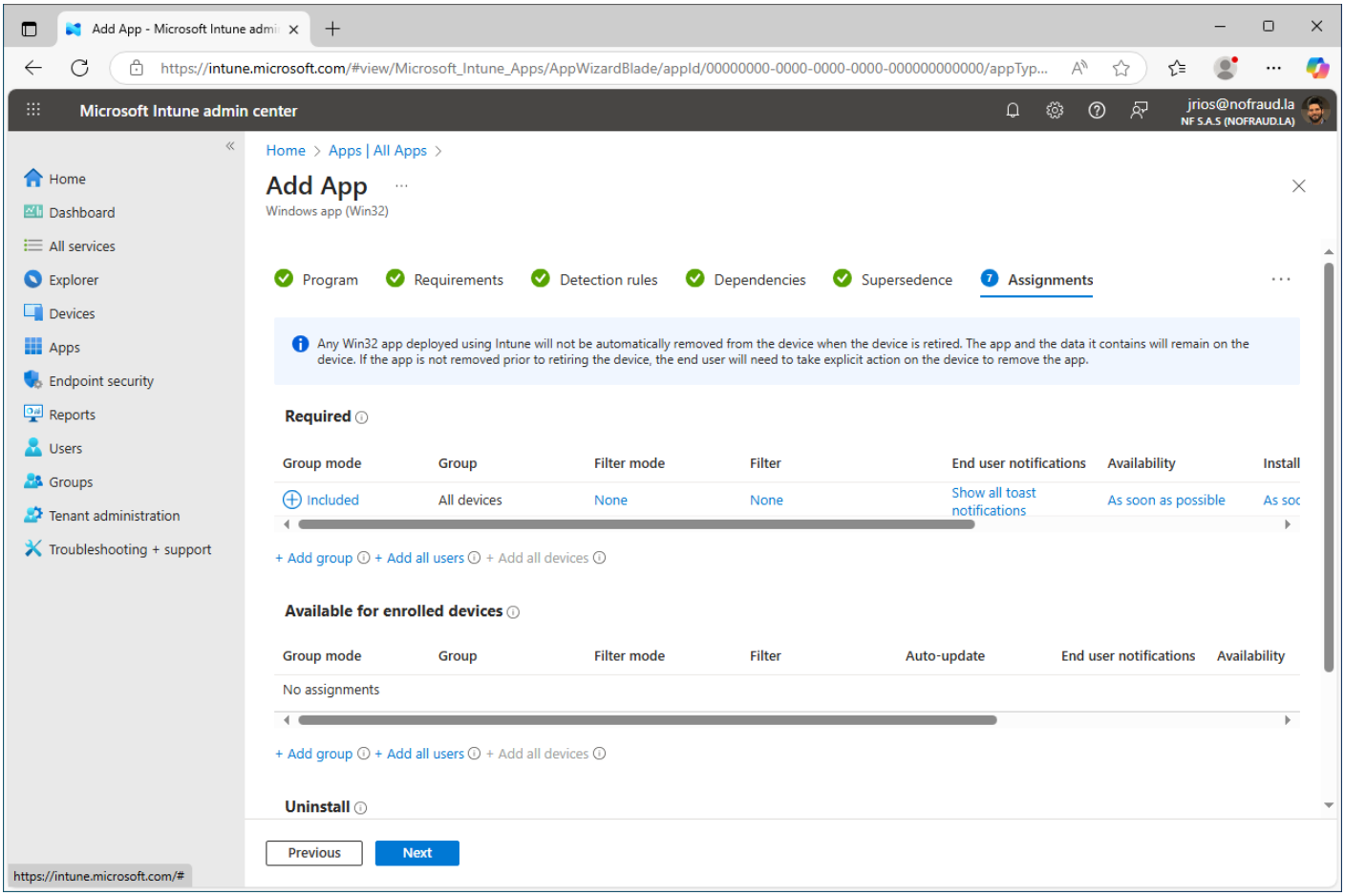
Esta es la parte donde se le especifica a **Microsoft Intune** que la aplicación que se está creando es la versión más actual de otra que ya existe. Se debe dar clic en **añadir** y seleccionar **Business Analytics 2.2.0** (la versión anterior).



Debe asegurarse de que no se desinstale la versión anterior. Esto no significa que quedarán dos versiones instaladas, esto lo que significa es que el proceso de actualización se llevará a cabo por el MSI y no por **Microsoft intune**.

Asignaciones para actualización

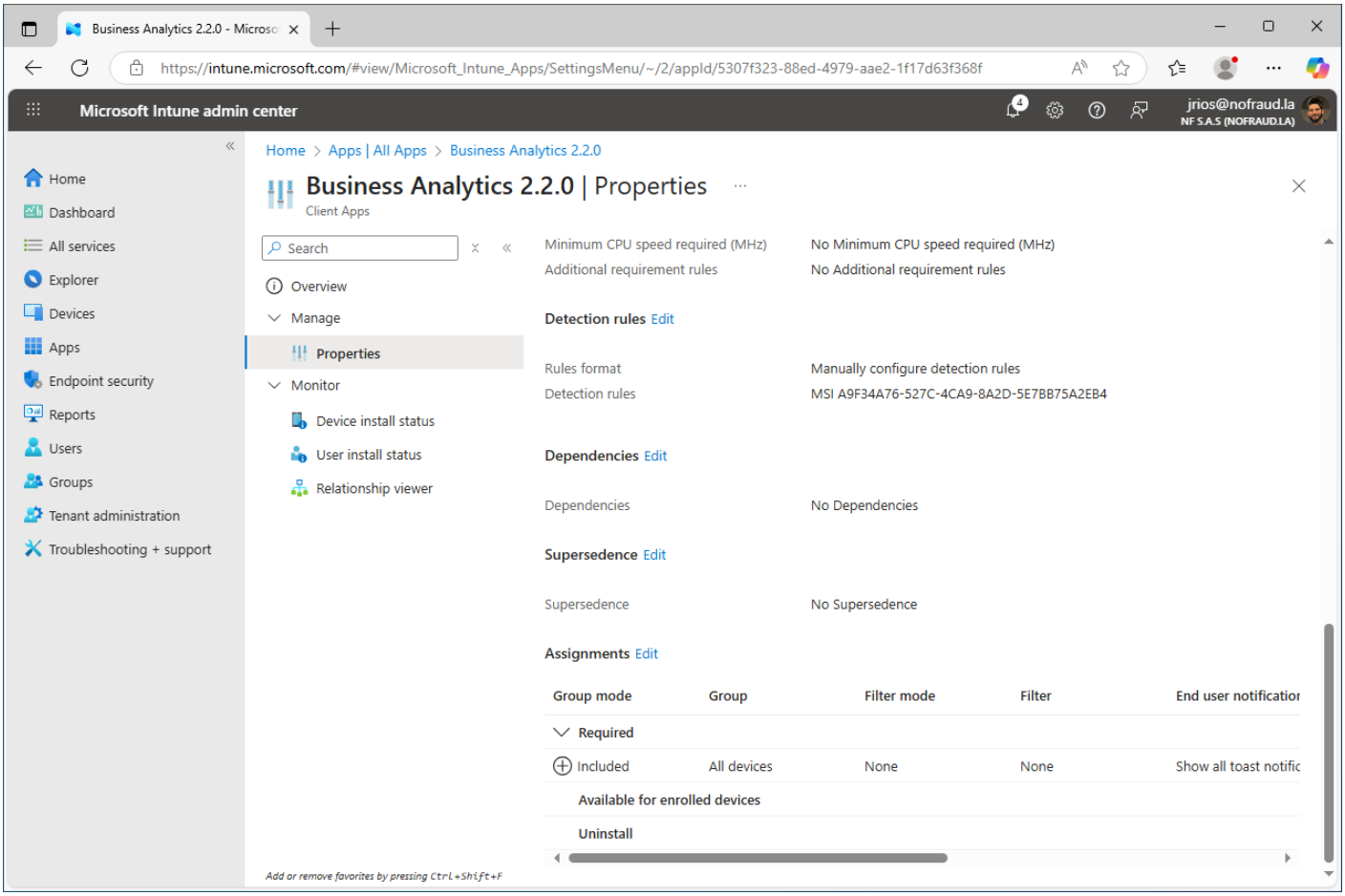
En la pantalla de asignaciones, seleccione en la categoría **Required** el grupo de usuarios o dispositivos al cual desea realizarle la actualización del agente.



En este caso, se seleccionó **Add all devices**, pero en su ambiente lo más seguro es que el agente no se haya instalado en todos los dispositivos, por lo cual deberá elegir el grupo que creó al momento de instalar por primera vez el agente. Con esto ya estaría creada la aplicación para la actualización.

Eliminar asignaciones antiguas

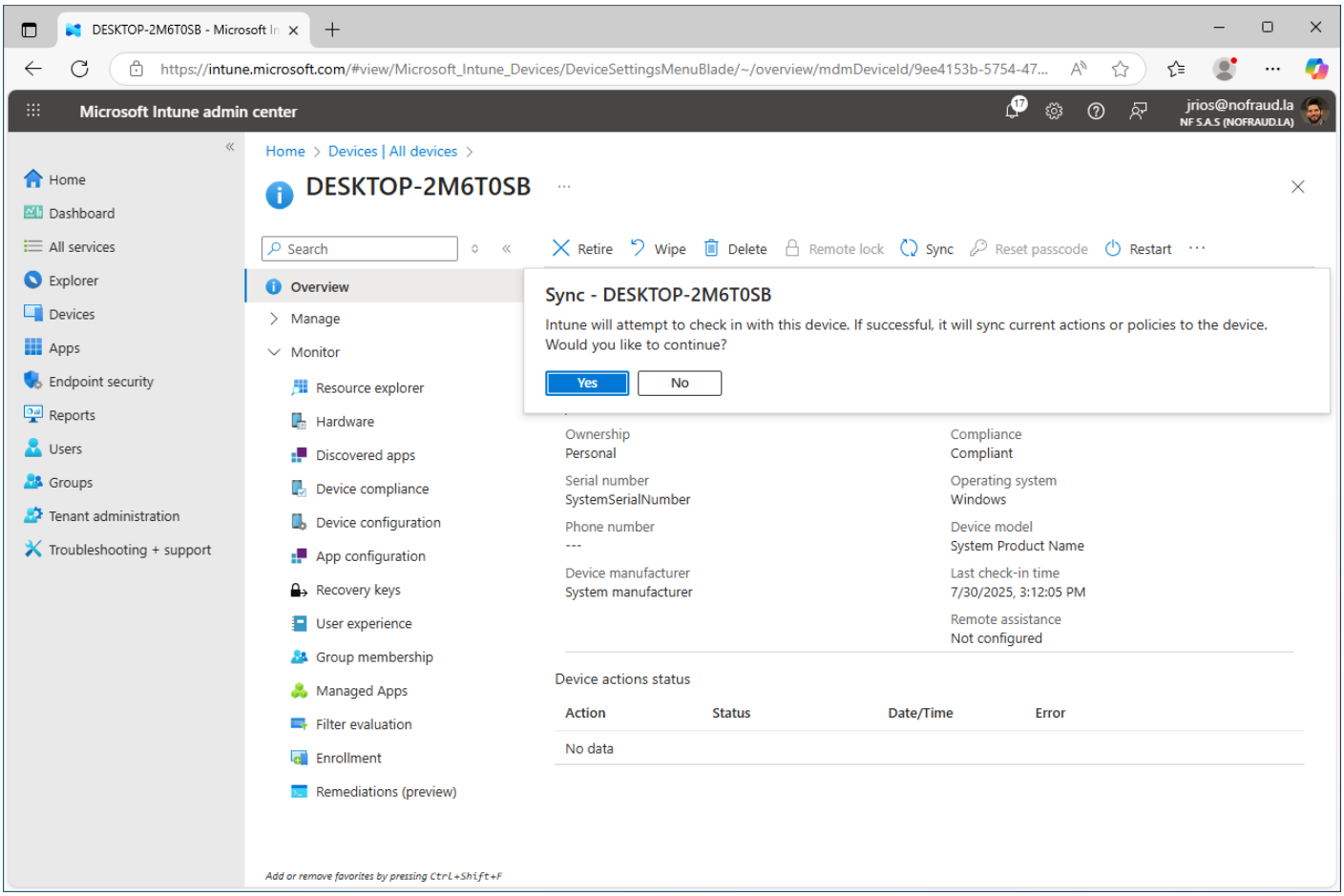
Entre a la aplicación de la versión anterior del agente, de clic en **Properties** y luego en **Assignments Edit**.



Asegúrese de eliminar la asignación de esta aplicación para que no interfiera en futuras acciones de desinstalación.

Sincronización de dispositivo

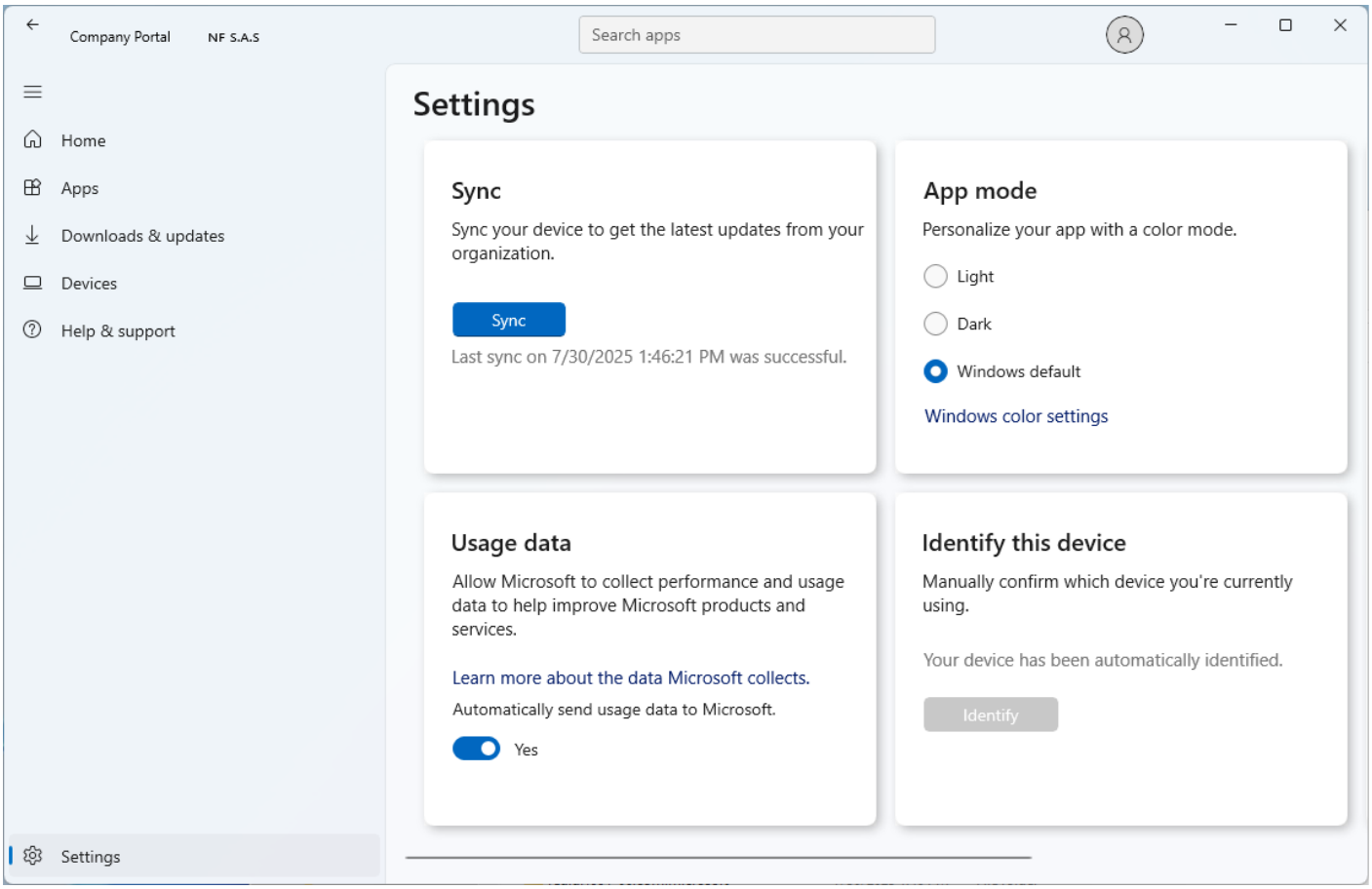
Para forzar la aplicación de la política del lado de **Microsoft Intune**, debe dar clic en **Devices**, luego en **All Devices**, seleccionar la máquina donde desea forzar la aplicación de la política y luego en el botón **Sync**.



El siguiente paso será forzar la sincronización del lado de las máquinas.

Sincronizar cliente Windows

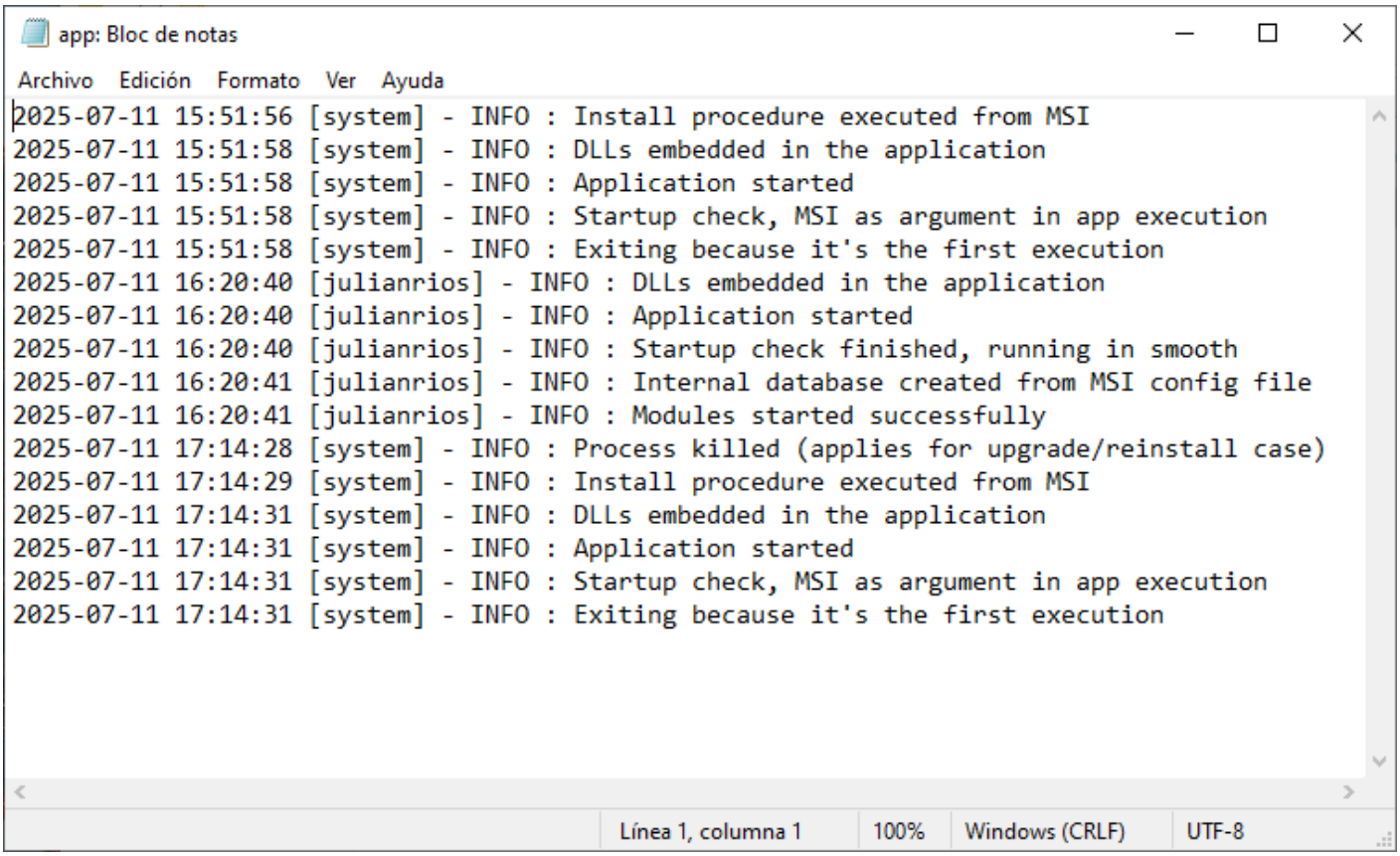
Si desea que la política se aplique de inmediato en alguna máquina cliente Windows, deberá ingresar a esa máquina por escritorio remoto y ejecutar la aplicación **Company Portal**.



Una vez que esté en la aplicación, de clic en **Settings** y luego en el botón **Sync**. Esto forzará la aplicación de la política y actualizará el agente antifraude de manera inmediata en esta máquina.

Verificación de la actualización

En el PC del usuario donde se llevó a cabo la actualización, se puede abrir el archivo **C:\ProgramData\Software\app.log** para verificar que la actualización se haya llevado a cabo con éxito.

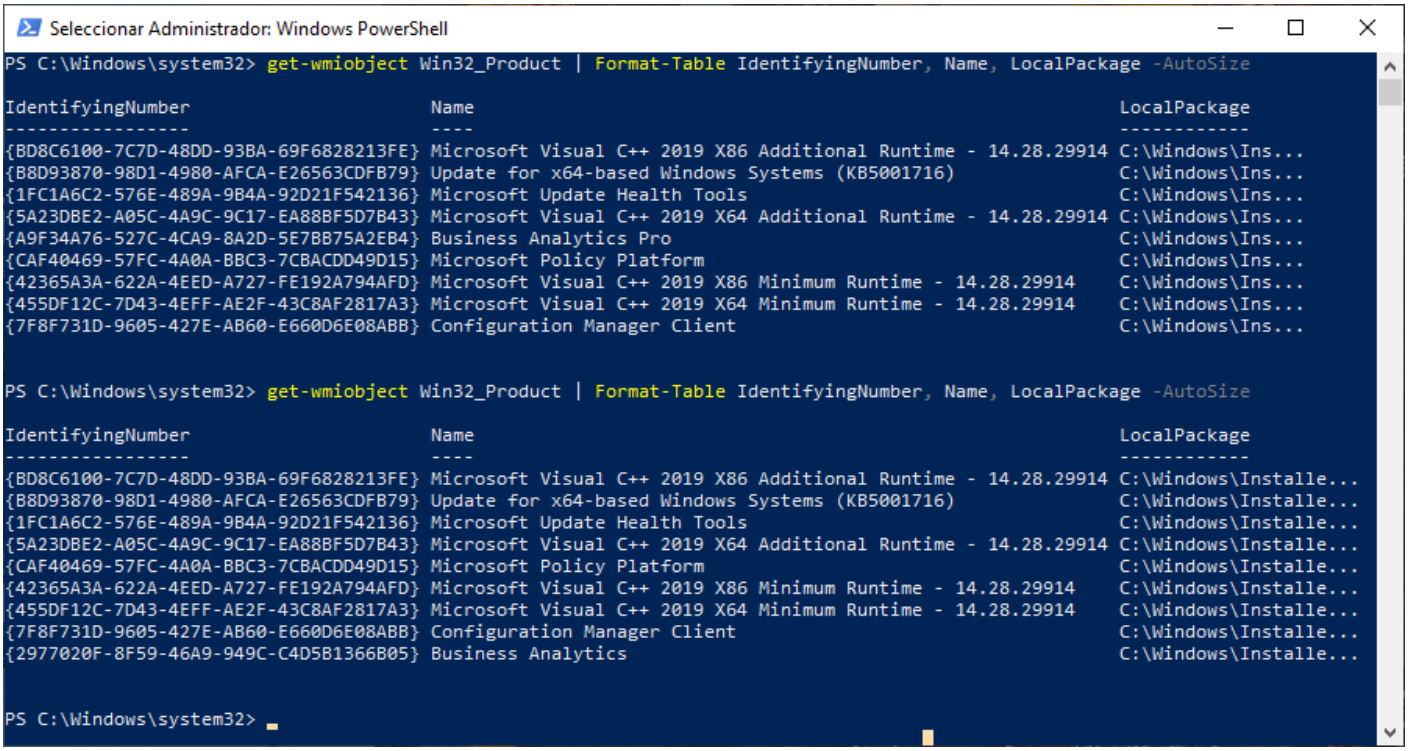


Deberá aparecer el mensaje **Process killed (applies for upgrade/reinstall case)** y se mostrará la usuario **system** como el ejecutor de esa actividad.

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:

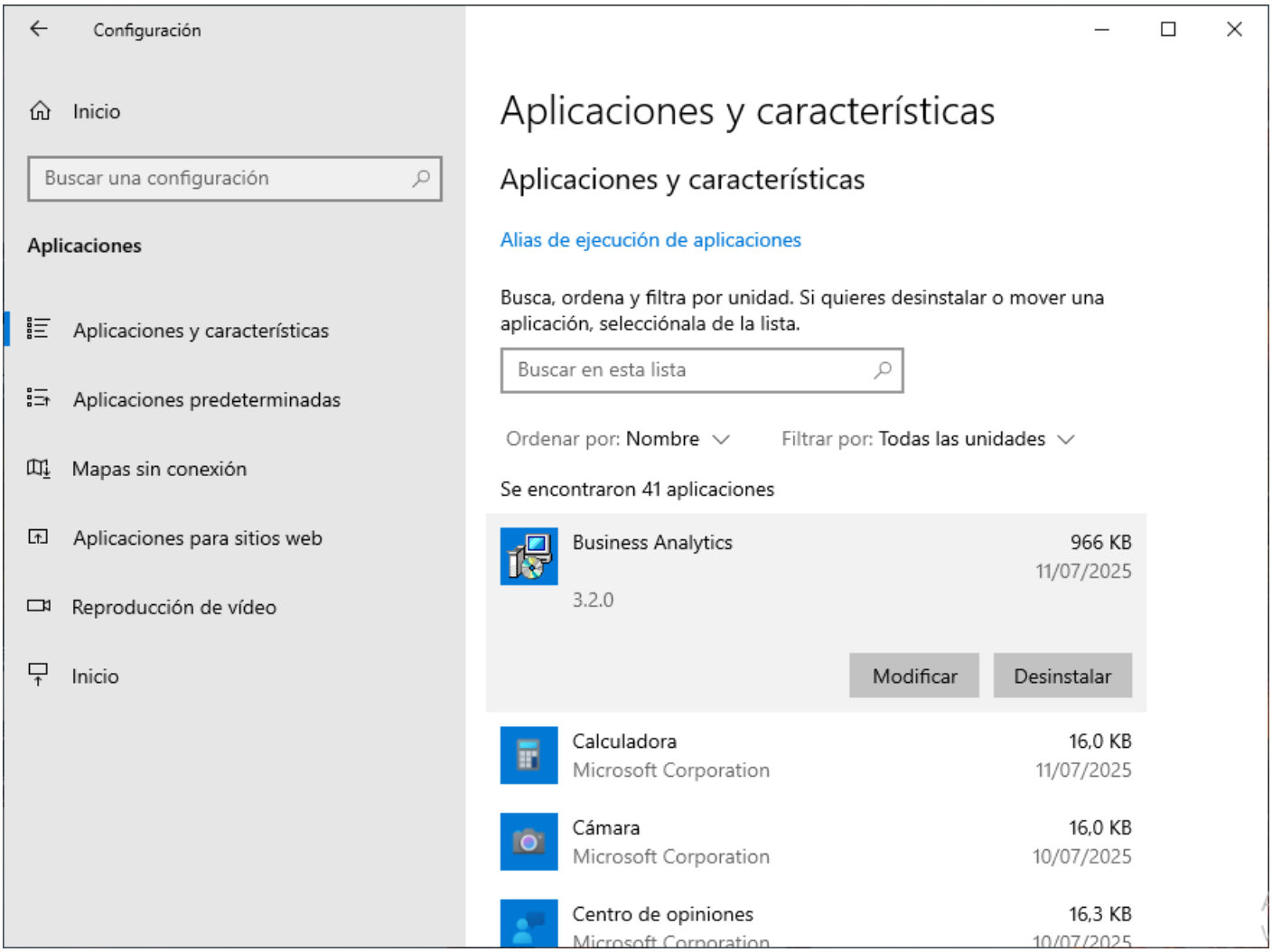
```
get-wmiobject Win32_Product | Format-Table IdentifyingNumber, Name, LocalPackage -AutoSize
```



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

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.

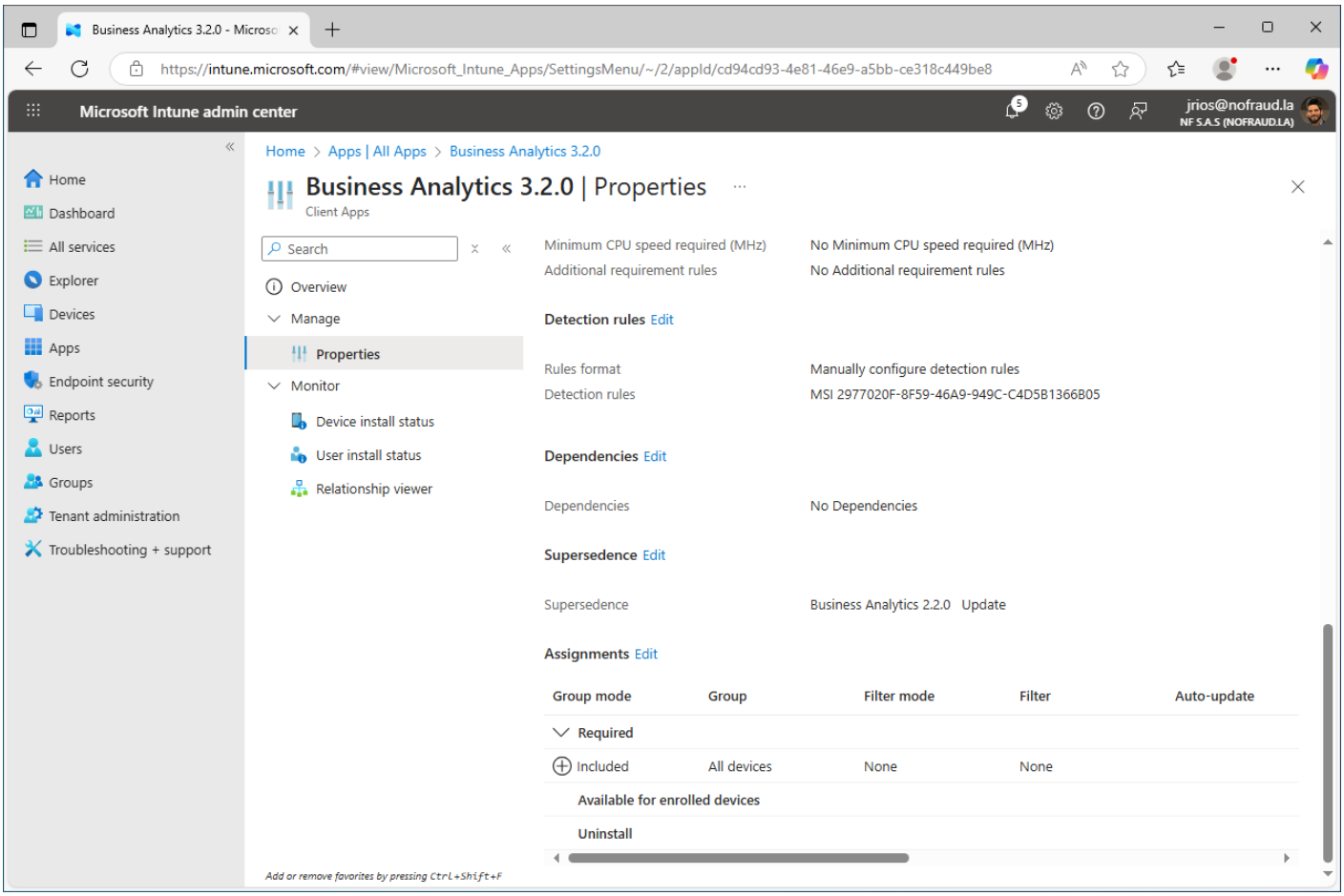


Se podrá ver adicionalmente que la versión cambió y se muestra la versión del nuevo agente.

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

Desinstalación del agente

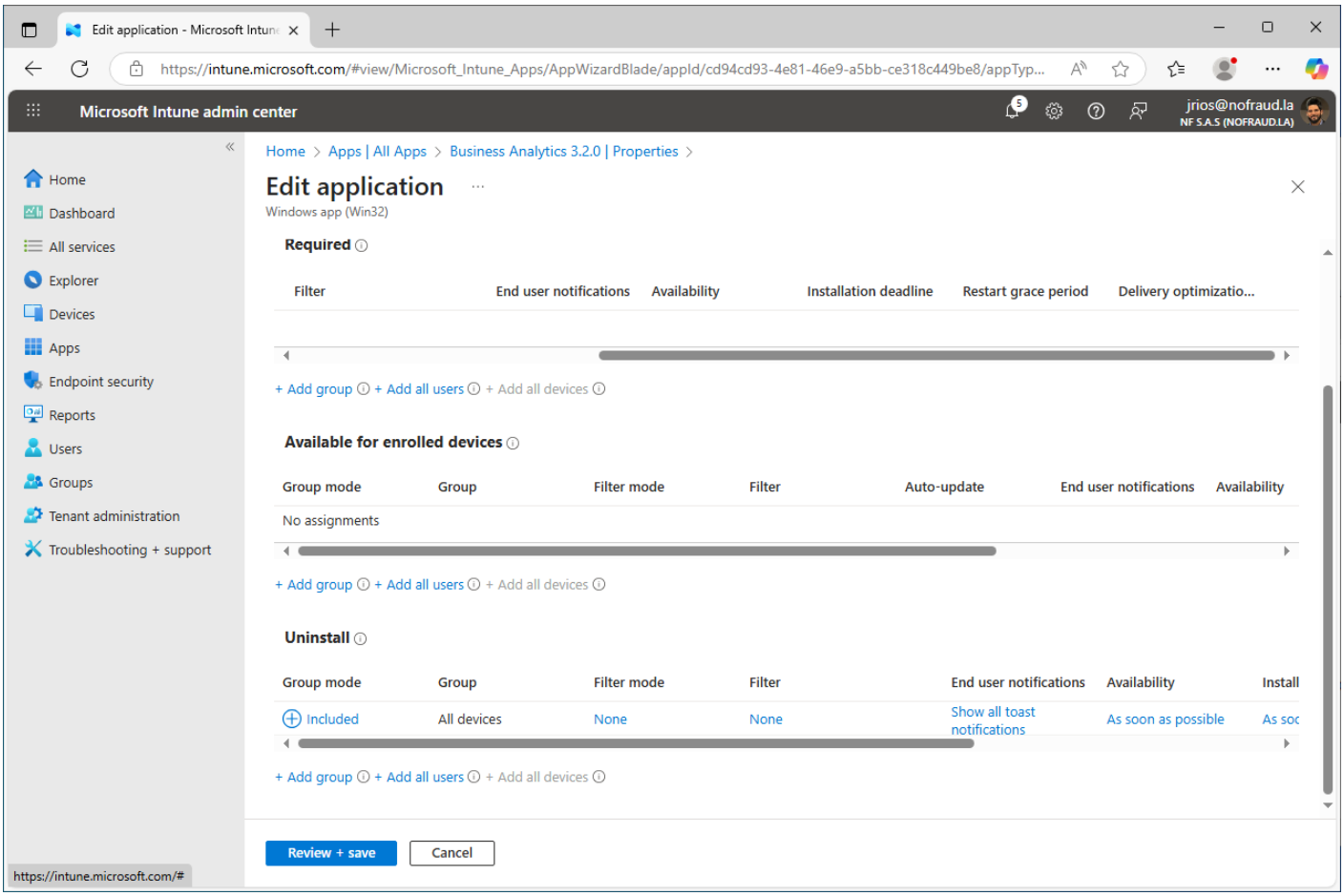
De clic en **Apps**, **All Apps** y seleccione la última versión del agente instalada. De clic en **Properties** y en **Assignments Edit**.



A continuación ponga mucha atención a la operación que se realizará sobre las asignaciones.

Asignación de desinstalación

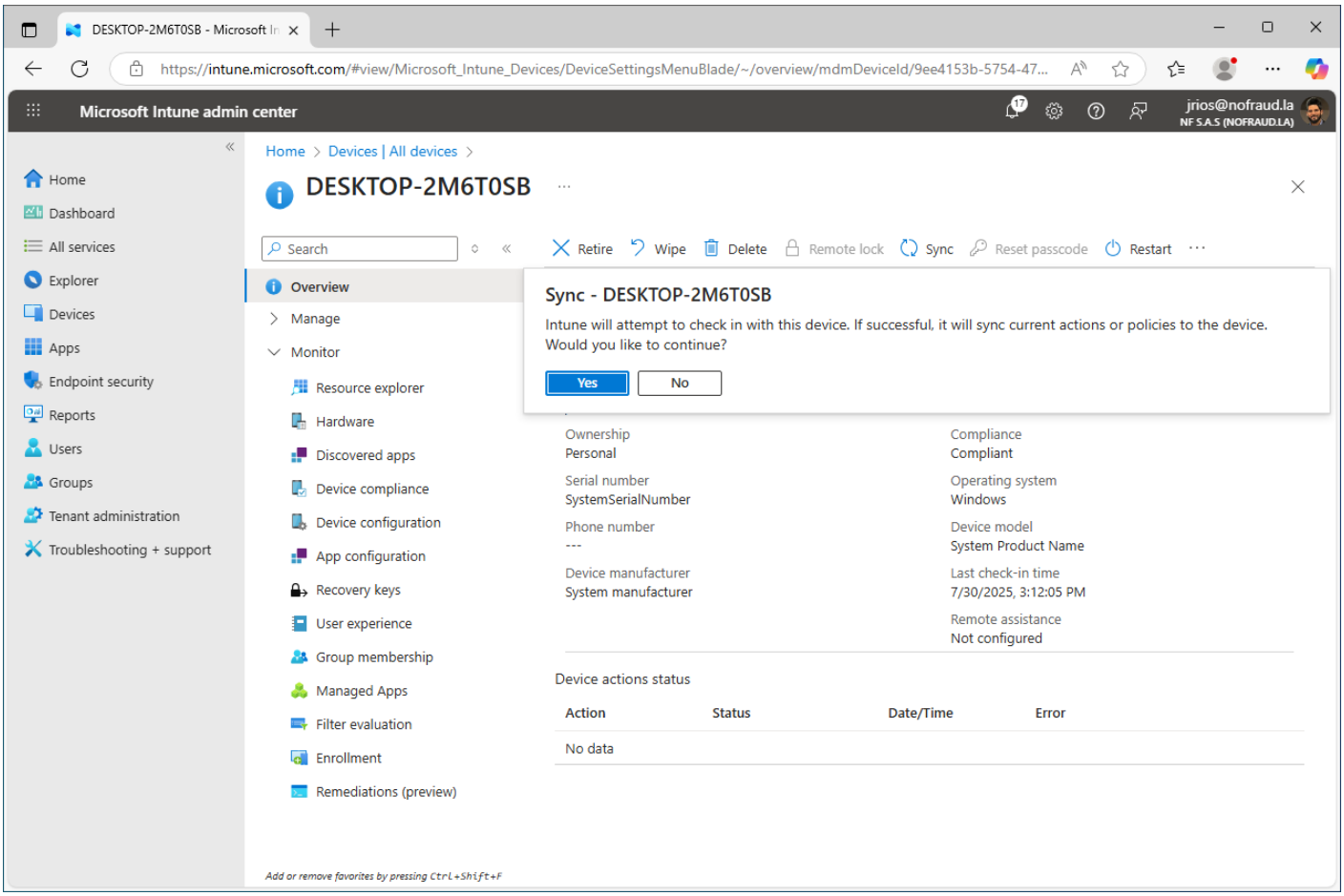
Se debe borrar de **Required** las entradas que previamente se añadieron. Luego, se deben crear en la categoría **Uninstall** las asignaciones de acuerdo al objetivo de desinstalación.



Dar clic en **Review + save** y con esto ya estaría lista la política de desinstalación del agente.

Sincronización de dispositivo

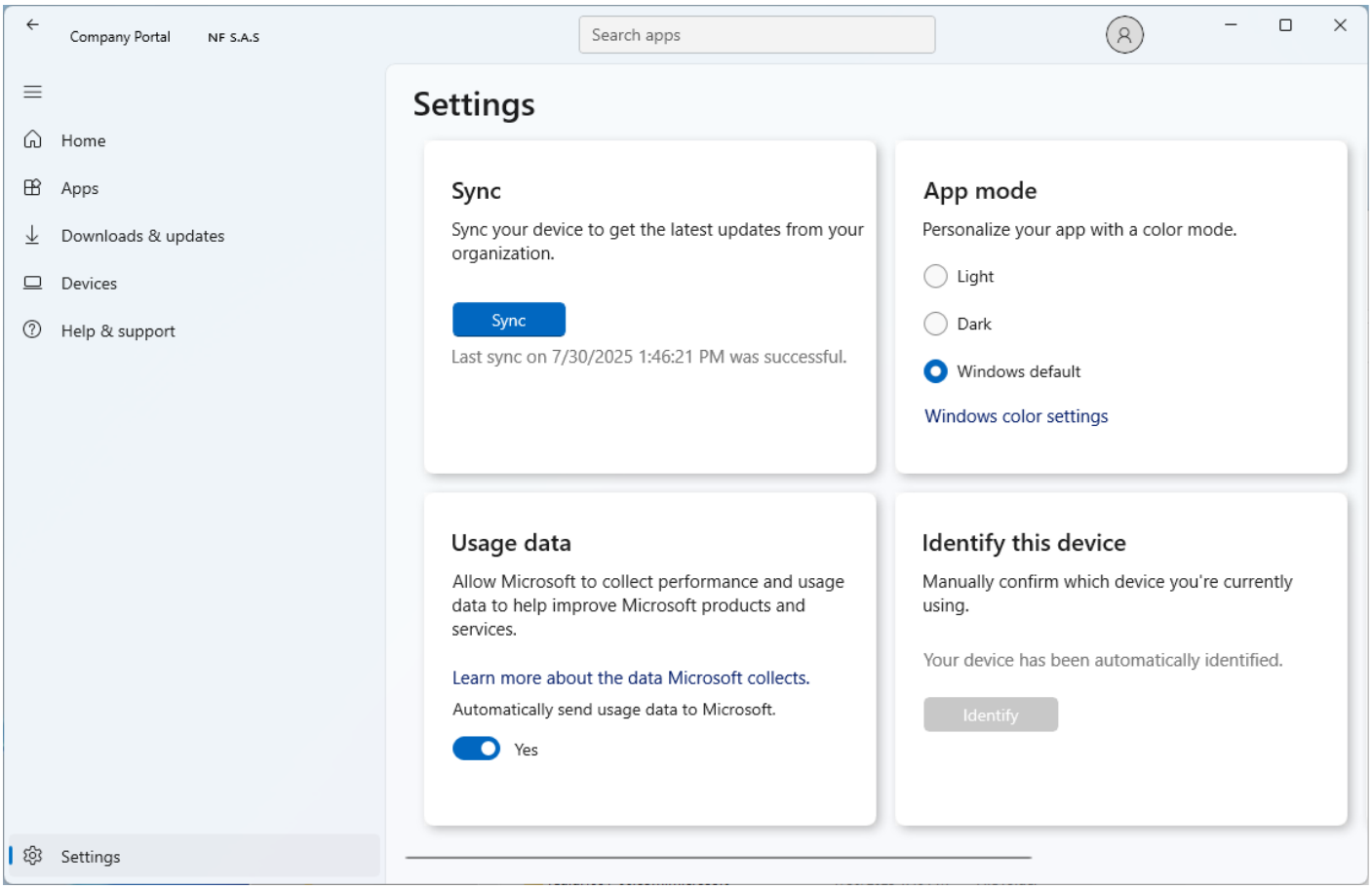
Para forzar la aplicación de la política del lado de **Microsoft Intune**, debe dar clic en **Devices**, luego en **All Devices**, seleccionar la máquina donde desea forzar la aplicación de la política y luego en el botón **Sync**.



El siguiente paso será forzar la sincronización del lado de las máquinas.

Sincronizar cliente Windows

Si desea que la política se aplique de inmediato en alguna máquina cliente Windows, deberá ingresar a esa máquina por escritorio remoto y ejecutar la aplicación **Company Portal**.

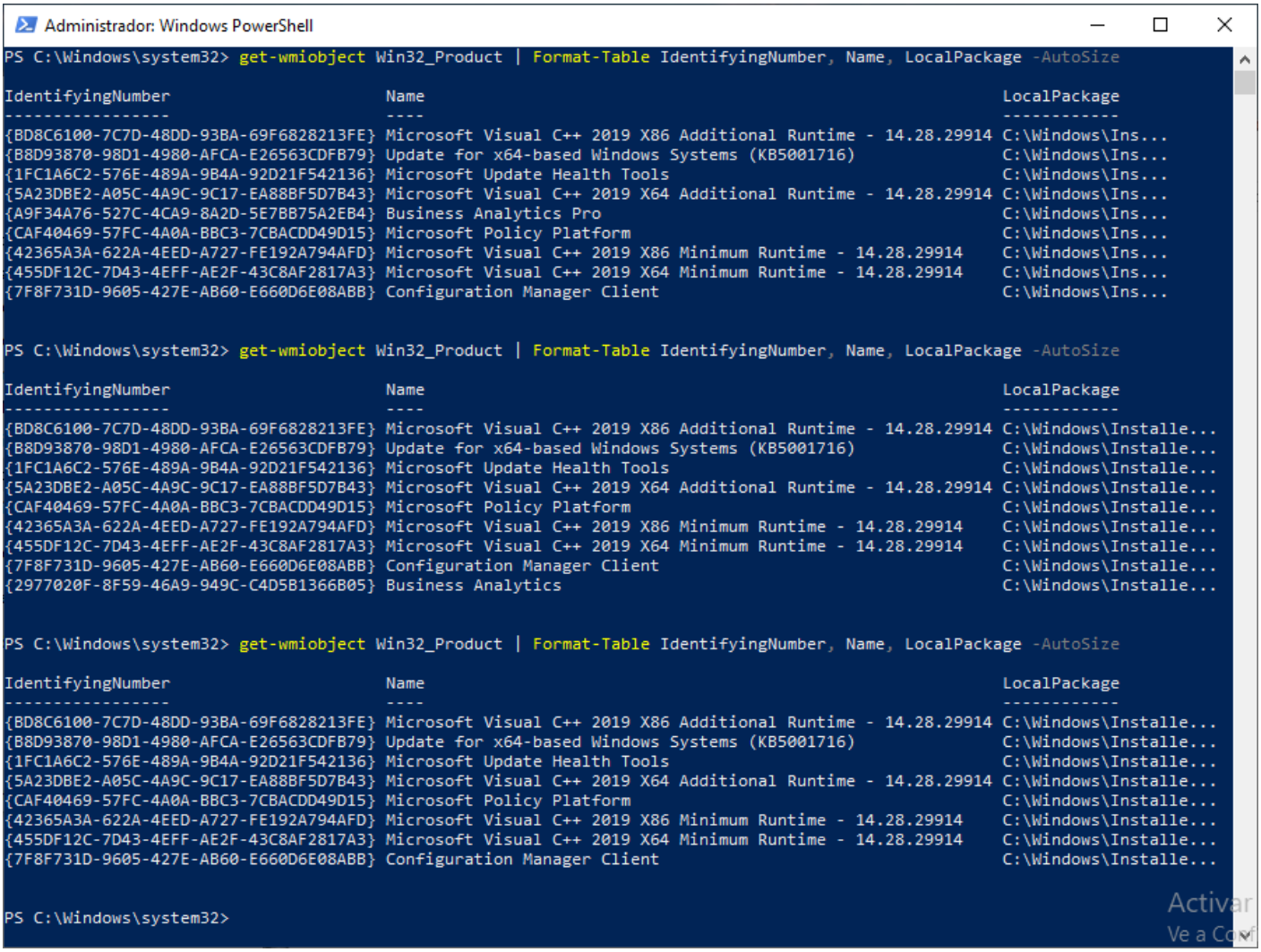


Una vez que esté en la aplicación, de clic en **Settings** y luego en el botón **Sync**. Esto forzará la aplicación de la política y desinstalará el agente antifraude de manera inmediata en esta máquina.

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 crear la acción de desinstalación en **Microsoft Intune**, ya no aparece la aplicación Business Analytics.