

Despliegue del agente para Linux

En esta sección se mostrarán todos los procedimientos que se deben realizar para llevar a cabo la instalación del agente antifraude en Linux.

- [Características del agente](#)
- [Requisitos previos](#)
- [Permisos de seguridad](#)
- [Video con todos los pasos](#)
- [Instalación del agente](#)
- [Verificación de la instalación](#)
- [Desinstalación del agente](#)

Características del agente

Antes de iniciar cualquier proceso de instalación, actualización o desinstalación, es importante que conozca la estructura del agente para que prepare su infraestructura y permita su funcionamiento. A continuación se realizará una caracterización de sus propiedades:

Conectividad	El agente requiere comunicarse con un servidor externo. Esta comunicación sucede solamente en una vía (agente - > servidor) y lo hace por 2 puertos, uno TCP y uno UDP. Los clientes recibirán un correo indicando cuáles son estos puertos para que procedan a configurar sus Firewalls.
Seguridad en su ejecución	Los antivirus podrían impedir que el agente se ejecute, por ello será importante añadir a la lista de exclusión la carpeta donde se aloja y el MD5 y SHA-1 de su ejecutable. Además del antivirus, si su distribución es basada en Red Hat, el sistema SELinux podría bloquear el agente. Tome las medidas necesarias para que el agente no sea bloqueado de acuerdo a la distribución Linux que use.
Carpetas y archivos que se crean	/home/usuario/businessAnalytics es la ruta donde se almacena todo el agente /home/usuario/.local/share/gnome-shell/extensions/window-calls-extended es la ruta donde se almacena la extensión de GNOME que permite el acceso a los datos de las ventanas. /home/usuario/businessAnalytics/config.ini el archivo de configuración /home/usuario/businessAnalytics/agent.log es el archivo de log
Arranque	/home/usuario/.autostart/enable-gnome-window-ext.desktop solo funciona una vez y se encarga de habilitar la extensión de GNOME al reinicio del PC /home/usuario/.autostart/businessAnalytics.desktop arranca el agente
Espacio en disco duro	0.14 MB (144 Kb)
Memoria RAM que consume	Entre 8 MB y 25 MB de memoria RAM
Compatibilidad con Linux	El agente es compatible con cualquier versión de Linux que tenga la interfaz gráfica GNOME y que use el administrador de ventanas Wayland.

Conociendo estas propiedades, puede proceder con el despliegue del agente.

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

Requisitos previos

Antes de ejecutar cualquier procedimiento en un sistema operativo Linux es importante tener en cuenta los siguientes requisitos previos:

Debe contar con la capacidad de realizar acciones administrativas en el sistema operativo Linux. El procedimiento de instalación del agente **NO debe ser ejecutado con usuario root**, mas bien, el usuario normal del sistema debe tener la capacidad de ejecutar comandos administrativos con el comando **sudo**. En caso de que el usuario normal no tenga permisos para usar **sudo**, se le debe habilitar temporalmente para instalar el agente. Una vez terminado el proceso de instalación se le pueden quitar los permisos.

Si su empresa tiene instalado un agente de despliegue masivo de software en el computador Linux, como lo puede ser System Center, Microsoft Intune o incluso el Directorio Activo, puede crear un procedimiento desde dichas consolas para instalar el agente antifraude ya que nuestro agente viene con un instalador único (**install.sh**).

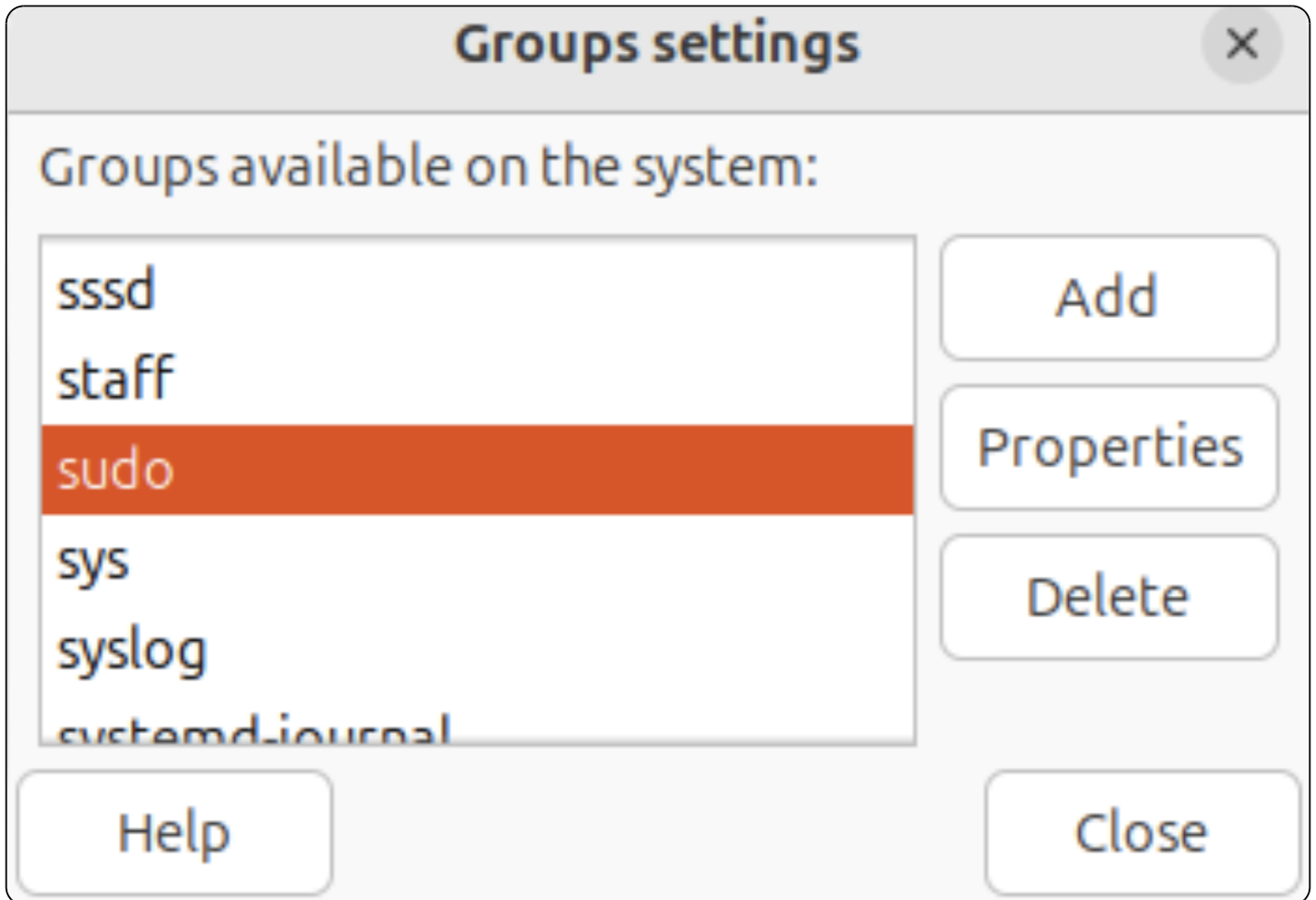
Este agente tiene un sólo componente externo del cual depende su funcionamiento y es una extensión de GNOME. La interfaz gráfica de usuario en Linux requiere de la instalación de una extensión (disponible en la página de extensiones de GNOME) para permitir el acceso a los datos de una ventana. Nuestro agente necesita este acceso para extraer los datos semánticos. Todo el proceso de instalación de esta extensión es automático, el administrador no necesita instalar nada manualmente y todo lo gestiona el instalador **install.sh**.

Este agente es compatible con todas las versiones de Linux que usen GNOME y el administrador de ventanas Wayland. Entre las cuales se encuentran Ubuntu Linux desde la versión 24 y Fedora Linux desde la versión 39. Estas distribuciones (Ubuntu y Fedora) son las distribuciones de Linux más usadas en ambiente de escritorio en el mundo, tanto de forma corporativa como de forma personal.

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

Permisos de seguridad

Antes de iniciar la instalación, el usuario debe pertenecer al grupo **sudo**. Esto permitirá luego ejecutar el instalador desde el entorno del usuario.



Puede usar las herramientas de GNOME para modificar los grupos a los cuales pertenece un usuario pero también puede escribir el siguiente comando como root para lograrlo:

```
# usermod -aG sudo usuario
```

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/C6Z_aRijlZE?si=L9fS7J3vIT8Xqjh0

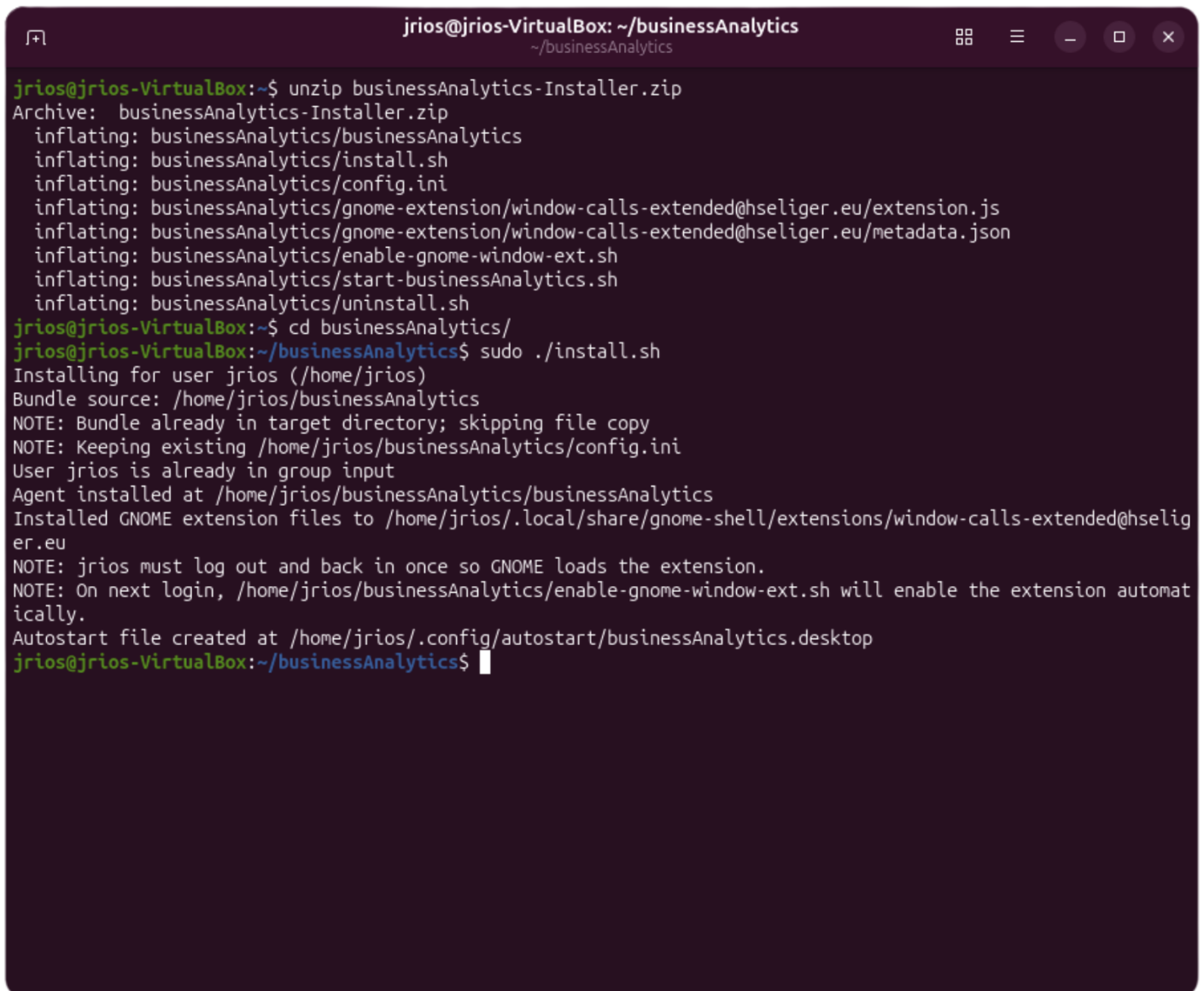
El video contiene todos los pasos de la guía ejecutados de forma práctica y cada uno de los pasos está separado por capítulos.

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

Instalación del agente

Descargue el instalador del agente **businessAnalytics-Installer.zip** al equipo Linux. Lo puede colocar en la carpeta **Home** del usuario (/home/usuario) temporalmente. Una vez allí, ejecute estos comandos:

```
$ sudo apt install unzip
$ unzip businessAnalytics-Installer.zip
$ sudo ./install.sh
```



```
jrios@jrios-VirtualBox: ~/businessAnalytics
~/businessAnalytics
jrios@jrios-VirtualBox:~$ unzip businessAnalytics-Installer.zip
Archive:  businessAnalytics-Installer.zip
  inflating: businessAnalytics/businessAnalytics
  inflating: businessAnalytics/install.sh
  inflating: businessAnalytics/config.ini
  inflating: businessAnalytics/gnome-extension/window-calls-extended@hseliger.eu/extension.js
  inflating: businessAnalytics/gnome-extension/window-calls-extended@hseliger.eu/metadata.json
  inflating: businessAnalytics/enable-gnome-window-ext.sh
  inflating: businessAnalytics/start-businessAnalytics.sh
  inflating: businessAnalytics/uninstall.sh
jrios@jrios-VirtualBox:~$ cd businessAnalytics/
jrios@jrios-VirtualBox:~/businessAnalytics$ sudo ./install.sh
Installing for user jrios (/home/jrios)
Bundle source: /home/jrios/businessAnalytics
NOTE: Bundle already in target directory; skipping file copy
NOTE: Keeping existing /home/jrios/businessAnalytics/config.ini
User jrios is already in group input
Agent installed at /home/jrios/businessAnalytics/businessAnalytics
Installed GNOME extension files to /home/jrios/.local/share/gnome-shell/extensions/window-calls-extended@hseliger.eu
NOTE: jrios must log out and back in once so GNOME loads the extension.
NOTE: On next login, /home/jrios/businessAnalytics/enable-gnome-window-ext.sh will enable the extension automatically.
Autostart file created at /home/jrios/.config/autostart/businessAnalytics.desktop
jrios@jrios-VirtualBox:~/businessAnalytics$
```

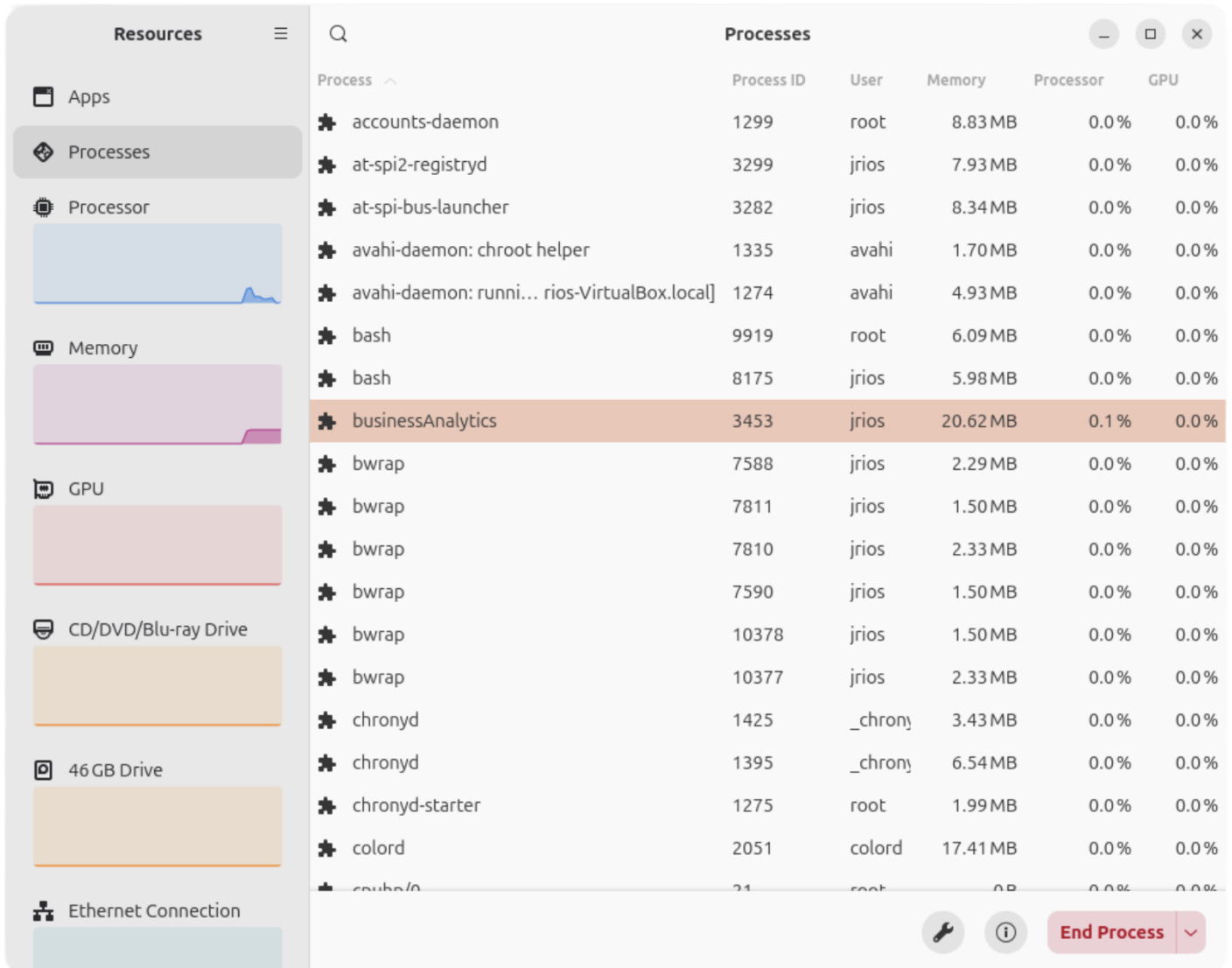
El instalador agregará el usuario al grupo input (para poder leer eventos de entrada), instalará la extensión de GNOME para acceder a los datos de las ventanas y creará las entradas necesarias para que el agente arranque siempre al iniciar la sesión en GNOME (autostart).

El agente empezará a funcionar en el **próximo reinicio**.

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

Verificación de la instalación

Para verificar la instalación se puede ejecutar la aplicación **Resources** accesible desde el menú principal de GNOME.



Process	Process ID	User	Memory	Processor	GPU
accounts-daemon	1299	root	8.83 MB	0.0%	0.0%
at-spi2-registryd	3299	jrios	7.93 MB	0.0%	0.0%
at-spi-bus-launcher	3282	jrios	8.34 MB	0.0%	0.0%
avahi-daemon: chroot helper	1335	avahi	1.70 MB	0.0%	0.0%
avahi-daemon: runni... rios-VirtualBox.local]	1274	avahi	4.93 MB	0.0%	0.0%
bash	9919	root	6.09 MB	0.0%	0.0%
bash	8175	jrios	5.98 MB	0.0%	0.0%
businessAnalytics	3453	jrios	20.62 MB	0.1%	0.0%
bwrap	7588	jrios	2.29 MB	0.0%	0.0%
bwrap	7811	jrios	1.50 MB	0.0%	0.0%
bwrap	7810	jrios	2.33 MB	0.0%	0.0%
bwrap	7590	jrios	1.50 MB	0.0%	0.0%
bwrap	10378	jrios	1.50 MB	0.0%	0.0%
bwrap	10377	jrios	2.33 MB	0.0%	0.0%
chronyd	1425	_chrony	3.43 MB	0.0%	0.0%
chronyd	1395	_chrony	6.54 MB	0.0%	0.0%
chronyd-starter	1275	root	1.99 MB	0.0%	0.0%
colord	2051	colord	17.41 MB	0.0%	0.0%
gnome/0	21	root	0.0 MB	0.0%	0.0%

En esta aplicación puede navegar en la pestaña **Processes** y buscar el programa **businessAnalytics**. Si el programa se encuentra, significa que se está ejecutando correctamente.

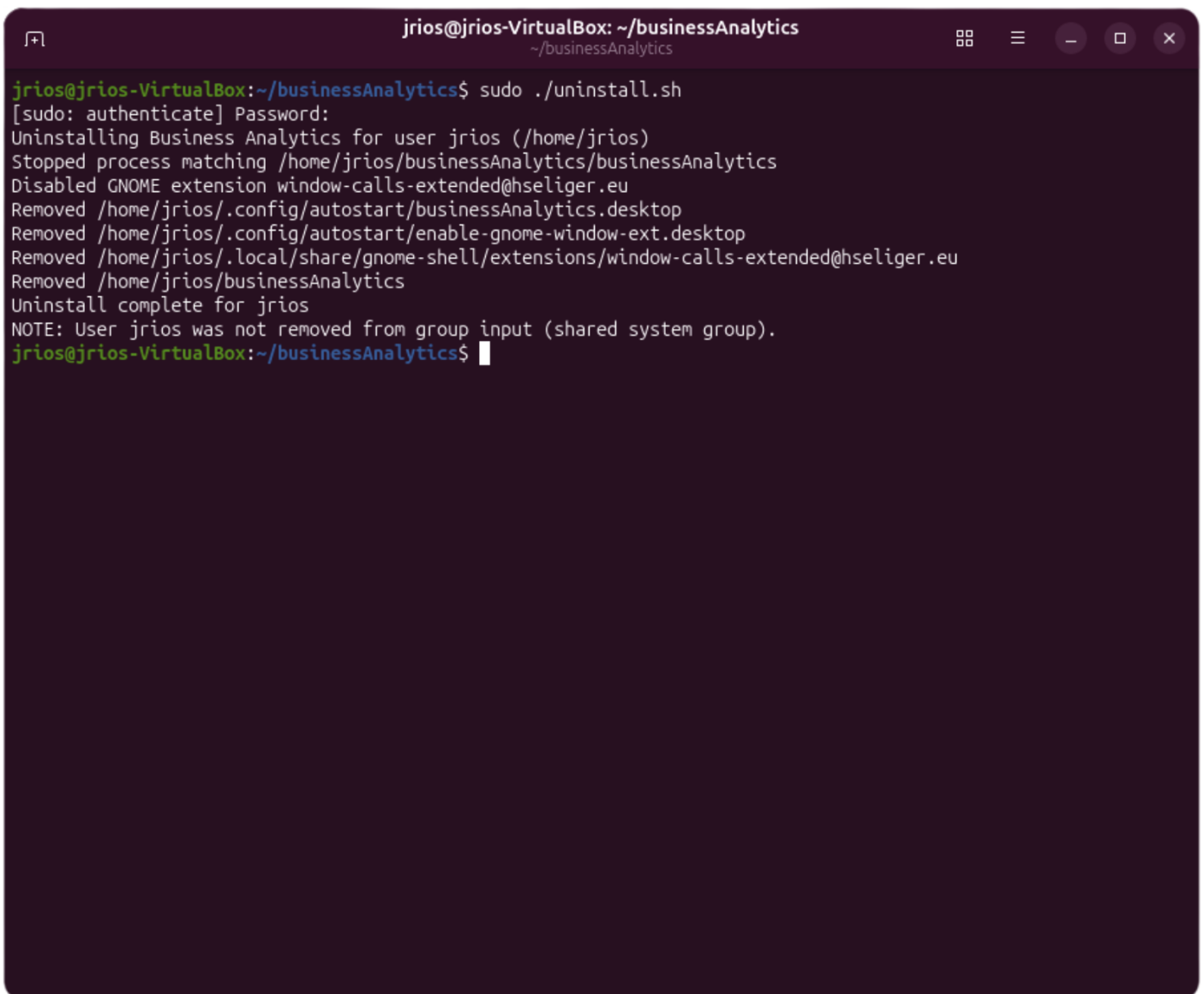
The Fraud Explorer es un software que junto con **FraudGPT** detecta el fraude y la corrupción en las organizaciones. Este software está siendo desarrollado por [NOFRAUD.la](https://www.nofraud.la). Este contenido es privado y únicamente está disponible para clientes de NOFRAUD. Está prohibida su publicación en fuentes abiertas o disponibles al público.

Desinstalación del agente

Para desinstalar el agente debe abrir la aplicación **Terminal** y ejecutar el siguiente comando:

```
$ cd ; cd businessAnalytics
$ sudo ./uninstall.sh
```

Luego se le preguntará el password para poder usar sudo y la desinstalación se ejecutará.

A screenshot of a terminal window titled "jrrios@jrrios-VirtualBox: ~/businessAnalytics". The terminal shows the execution of the command "sudo ./uninstall.sh". The output includes: "[sudo: authenticate] Password:", "Uninstalling Business Analytics for user jrrios (/home/jrrios)", "Stopped process matching /home/jrrios/businessAnalytics/businessAnalytics", "Disabled GNOME extension window-calls-extended@hseliger.eu", "Removed /home/jrrios/.config/autostart/businessAnalytics.desktop", "Removed /home/jrrios/.config/autostart/enable-gnome-window-ext.desktop", "Removed /home/jrrios/.local/share/gnome-shell/extensions/window-calls-extended@hseliger.eu", "Removed /home/jrrios/businessAnalytics", "Uninstall complete for jrrios", and "NOTE: User jrrios was not removed from group input (shared system group).". The prompt returns to "jrrios@jrrios-VirtualBox: ~/businessAnalytics\$".

```
jrrios@jrrios-VirtualBox: ~/businessAnalytics
jrrios@jrrios-VirtualBox:~/businessAnalytics$ sudo ./uninstall.sh
[sudo: authenticate] Password:
Uninstalling Business Analytics for user jrrios (/home/jrrios)
Stopped process matching /home/jrrios/businessAnalytics/businessAnalytics
Disabled GNOME extension window-calls-extended@hseliger.eu
Removed /home/jrrios/.config/autostart/businessAnalytics.desktop
Removed /home/jrrios/.config/autostart/enable-gnome-window-ext.desktop
Removed /home/jrrios/.local/share/gnome-shell/extensions/window-calls-extended@hseliger.eu
Removed /home/jrrios/businessAnalytics
Uninstall complete for jrrios
NOTE: User jrrios was not removed from group input (shared system group).
jrrios@jrrios-VirtualBox:~/businessAnalytics$
```

El agente dejará de funcionar de forma inmediata.