

# PINKERTON



[ MANUAL PARA USUARIOS DE GNU/LINUX ]

# Presentación

*Pinkerton* es un software desarrollado y facilitado por *Hispacec Sistemas* para realizar un análisis sobre la seguridad del sistema informático con absoluta confidencialidad, transparencia, y sin interferir en el rendimiento del equipo, permitiendo al usuario continuar utilizándolo con normalidad.

La información obtenida del análisis realizado se compone de datos sobre software malicioso (malware, virus, software-espía, troyanos, gusanos...) encontrado en el equipo, así como de las medidas de seguridad activas en el momento del escaneo.

Es importante remarcar que *Pinkerton* no es un software antivirus ni, en ningún caso, sustituye a estos. Es decir, no realiza funciones de eliminación de malware.

La información obtenida a través de *Pinkerton* es totalmente confidencial y en ningún momento la información es enlazada con ninguna persona, respetando totalmente el anonimato de la persona que utiliza *Pinkerton*.

*Pinkerton* es utilizado para un estudio sobre la seguridad en Internet. La información recopilada no es transferida ni facilitada fuera de este estudio.

**Importante: Este manual está realizado pensando en distribuciones Ubuntu y similares. Si usted utiliza una distribución diferente el método de instalación de los requisitos de *Pinkerton* puede variar.**

## Requisitos

Para el correcto funcionamiento de *Pinkerton*, el equipo debe de disponer de los siguientes programas instalados.

### Python3

Es el motor utilizado por *Pinkerton*, y por tanto necesario para su ejecución. Si python no se encuentra en el sistema, deberá de instalarlo. Para ello debe ejecutar el comando siguiente:

```
sudo apt-get install python3
```



```

terry@ubuntu: ~
terry@ubuntu:~$ sudo apt-get install python3
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  app-install-data appmenu-qt appmenu-qt5 apport-symptoms appstream aptdaemon-data
  avahi-utils bamfdaemon blt command-not-found-data compiz-core compiz-plugins-default dc
  diffstat distro-info-data gconf-service gconf-service-backend gconf2-common gedit-common
  gettext gir1.2-accounts-1.0 gir1.2-appindicator3-0.1 gir1.2-atspi-2.0
  gir1.2-dbusmenu-glib-0.4 gir1.2-dee-1.0 gir1.2-gdata-0.0 gir1.2-gmenu-3.0
  gir1.2-gnomekeyring-1.0 gir1.2-goa-1.0 gir1.2-gst-plugins-base-1.0 gir1.2-gstreamer-1.0
  gir1.2-gtksource-3.0 gir1.2-gudev-1.0 gir1.2-javascriptcoregtk-3.0
  gir1.2-javascriptcoregtk-4.0 gir1.2-json-1.0 gir1.2-notify-0.7 gir1.2-packagekitglib-1.0
  gir1.2-rb-3.0 gir1.2-secret-1 gir1.2-signon-1.0 gir1.2-totem-1.0
  gir1.2-totem-plparser-1.0 gir1.2-udisks-2.0 gir1.2-unity-5.0 gir1.2-vte-2.91
  gir1.2-webkit-3.0 gir1.2-webkit2-4.0 gir1.2-wnck-3.0 gnome-software-common
  gnome-terminal-data guile-2.0-libs hardening-includes hud indicator-appmenu
  indicator-bluetooth indicator-messages indicator-printers intel-gpu-tools
  intltool-debian ippusbxd jayatana libandroid-properties1 libapparmor-perl libappstream3
  libapt-pkg-perl libarchive-zip-perl libart-2.0-2 libasprintf-dev libautodie-perl

```

Imagen1: Instalación del motor *Python3*

Y aceptar su instalación para terminar el proceso.

```

terry@ubuntu: ~
qtdeclarative5-accounts-plugin qtdeclarative5-qtquick2-plugin
qtdeclarative5-ubuntu-ui-toolkit-plugin qtdeclarative5-unity-action-plugin
rhythmbox-data session-shortcuts signon-keyring-extension snapd-login-service
suru-icon-theme syslinux syslinux-common syslinux-legacy tiutils tcl tk tk8.6-blt2.5
ubuntu-mobile-icons ubuntu-ui-toolkit-theme unity-gtk-module-common unity-gtk2-module
unity-gtk3-module unity-lens-applications unity-lens-files unity-lens-music
unity-lens-video unity-schemas unity-scope-video-remote unity-scopes-master-default
unity-scopes-runner unity-services unity-webapps-qml unity-webapps-service
webapp-container webbrowser-app xbrlapi
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  dh-python python3-minimal python3.5 python3.5-minimal
Suggested packages:
  python3-doc python3-tk python3-venv python3.5-venv python3.5-doc binfmt-support
The following NEW packages will be installed:
  dh-python python3 python3-minimal python3.5 python3.5-minimal
0 upgraded, 5 newly installed, 0 to remove and 147 not upgraded.
Need to get 1,868 kB of archives.
After this operation, 9,915 kB of additional disk space will be used.
Do you want to continue? [Y/n]

```

Imagen 2: Aceptar la instalación de *python3*

## Librería gráfica tk

La librería gráfica *Tk* es utilizada por *Pinkerton* para mostrar su interfaz. Si la librería gráfica de *python3 Tk* no se encuentra en el sistema, es necesario instalarla. Para ello debe ejecutar el comando siguiente:

```
sudo apt-get install python3-tk
```

```

terry@ubuntu: ~
terry@ubuntu:~$ sudo apt-get install python3-tk
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  app-install-data appmenu-qt appmenu-qt5 apport-symptoms appstream aptdaemon-data
  avahi-utils bamfdaemon command-not-found-data compiz-core compiz-plugins-default dc
  diffstat distro-info-data gconf-service gconf-service-backend gconf2-common gedit-common
  gettext gir1.2-accounts-1.0 gir1.2-appindicator3-0.1 gir1.2-atspi-2.0
  gir1.2-dbusmenu-glib-0.4 gir1.2-dee-1.0 gir1.2-gdata-0.0 gir1.2-gmenu-3.0
  gir1.2-gnomekeyring-1.0 gir1.2-goa-1.0 gir1.2-gst-plugins-base-1.0 gir1.2-gstreamer-1.0
  gir1.2-gtksource-3.0 gir1.2-gudev-1.0 gir1.2-javascriptcoregtk-3.0
  gir1.2-javascriptcoregtk-4.0 gir1.2-json-1.0 gir1.2-notify-0.7 gir1.2-packagekitglib-1.0
  gir1.2-rb-3.0 gir1.2-secret-1 gir1.2-signon-1.0 gir1.2-totem-1.0 gir1.2-totem-plparser-1.0
  gir1.2-udisks-2.0 gir1.2-unity-5.0 gir1.2-vte-2.91 gir1.2-webkit-3.0 gir1.2-webkit2-4.0

```



Debe aceptar su instalación para terminar el proceso, introduciendo “Y” (sin comillas).

## PIP para python3

Se debe instalar pip para python3 para permitir la instalación de módulos en Python. Se hace a través de este comando:

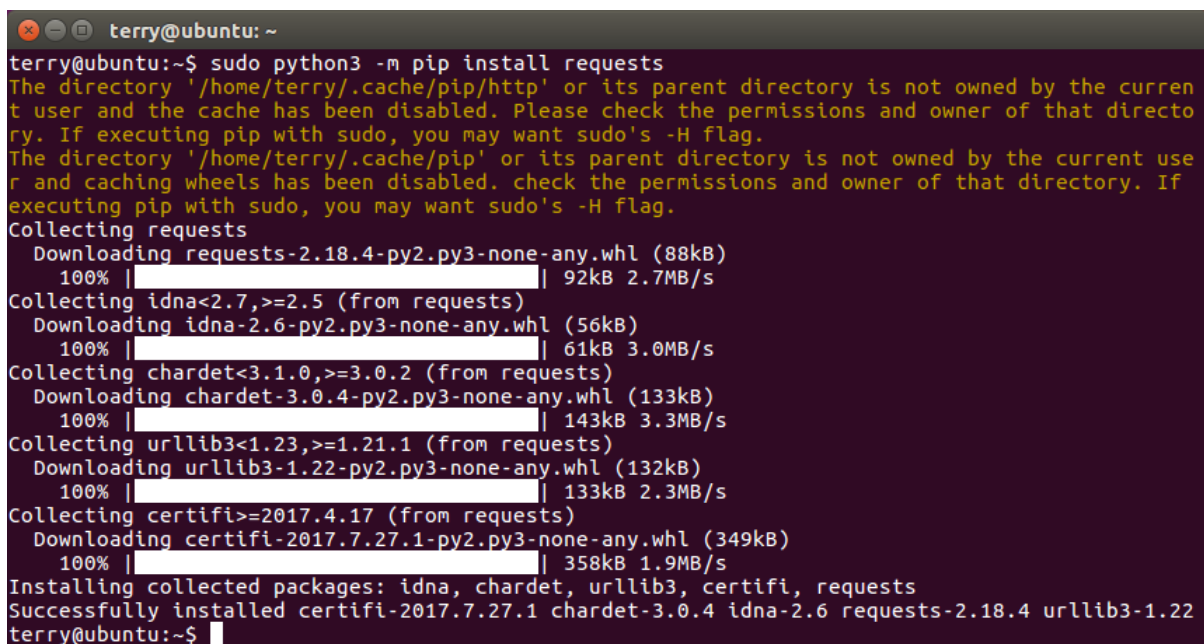
```
sudo apt-get install python3-pip
```

Debe aceptar su instalación para terminar el proceso, introduciendo “Y” (sin comillas).

## Requests

Es el módulo utilizado por *Pinkerton* para la comunicación de red. Si *requests* no se encuentra en el sistema, debe instalarlo. Para ello debe de ejecutar el comando siguiente:

```
sudo python3 -m pip install requests
```



```
terry@ubuntu: ~  
terry@ubuntu:~$ sudo python3 -m pip install requests  
The directory '/home/terry/.cache/pip/http' or its parent directory is not owned by the current user and the cache has been disabled. Please check the permissions and owner of that directory. If executing pip with sudo, you may want sudo's -H flag.  
The directory '/home/terry/.cache/pip' or its parent directory is not owned by the current user and caching wheels has been disabled. check the permissions and owner of that directory. If executing pip with sudo, you may want sudo's -H flag.  
Collecting requests  
  Downloading requests-2.18.4-py2.py3-none-any.whl (88kB)  
    100% |#####| 92kB 2.7MB/s  
Collecting idna<2.7,>=2.5 (from requests)  
  Downloading idna-2.6-py2.py3-none-any.whl (56kB)  
    100% |#####| 61kB 3.0MB/s  
Collecting chardet<3.1.0,>=3.0.2 (from requests)  
  Downloading chardet-3.0.4-py2.py3-none-any.whl (133kB)  
    100% |#####| 143kB 3.3MB/s  
Collecting urllib3<1.23,>=1.21.1 (from requests)  
  Downloading urllib3-1.22-py2.py3-none-any.whl (132kB)  
    100% |#####| 133kB 2.3MB/s  
Collecting certifi>=2017.4.17 (from requests)  
  Downloading certifi-2017.7.27.1-py2.py3-none-any.whl (349kB)  
    100% |#####| 358kB 1.9MB/s  
Installing collected packages: idna, chardet, urllib3, certifi, requests  
Successfully installed certifi-2017.7.27.1 chardet-3.0.4 idna-2.6 requests-2.18.4 urllib3-1.22  
terry@ubuntu:~$
```

Imagen 4: Instalación del módulo *requests*

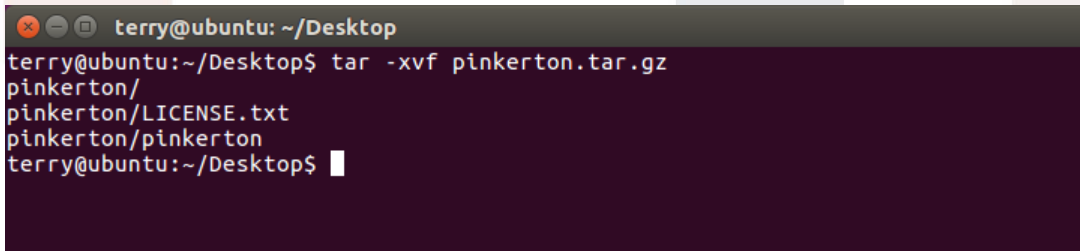
## Instalación

El link para descargar *Pinkerton* se facilita al final de la encuesta. Si por algún motivo no es posible acceder al mismo, se puede descargar alternativamente desde la web de la comunidad de internautas: <http://www.comunidad.gfk.es> o a través desde el sitio web de Hispasec: <https://www.hispasec.com/resources/pinkerton.tar.gz>



Una vez obtenido, es necesario extraer el contenido del paquete ejecutando desde el terminal el comando siguiente:

```
"tar -xvf pinkerton.tar.gz"
```

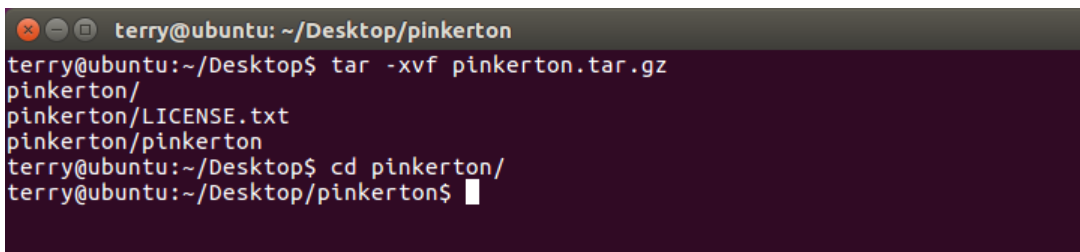


```
terry@ubuntu: ~/Desktop
terry@ubuntu:~/Desktop$ tar -xvf pinkerton.tar.gz
pinkerton/
pinkerton/LICENSE.txt
pinkerton/pinkerton
terry@ubuntu:~/Desktop$
```

Imagen 5: Extracción de *Pinkerton*

Cuando este proceso acabe, se habrá creado una carpeta que contiene el software *Pinkerton* y el archivo de licencia (se recomienda su lectura). Por tanto hay que cambiar el directorio de trabajo con el comando siguiente:

```
"cd pinkerton"
```



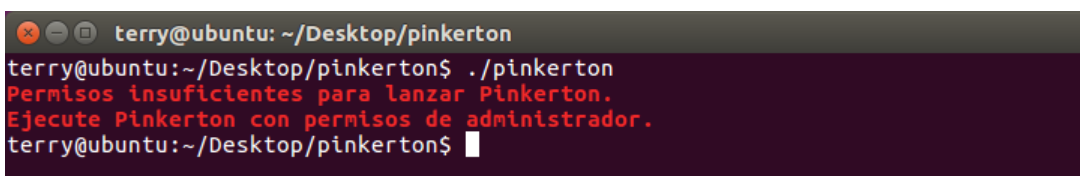
```
terry@ubuntu: ~/Desktop/pinkerton
terry@ubuntu:~/Desktop$ tar -xvf pinkerton.tar.gz
pinkerton/
pinkerton/LICENSE.txt
pinkerton/pinkerton
terry@ubuntu:~/Desktop$ cd pinkerton/
terry@ubuntu:~/Desktop/pinkerton$
```

Imagen 6: cambio de directorio al directorio de *Pinkerton*

Como paso previo a la ejecución del mismo con el comando siguiente:

```
"sudo ./pinkerton"
```

En caso de no ejecutarse con sudo (privilegios de Administrador o root), *Pinkerton* mostrará un aviso informando de este hecho.



```
terry@ubuntu: ~/Desktop/pinkerton
terry@ubuntu:~/Desktop/pinkerton$ ./pinkerton
Permisos insuficientes para lanzar Pinkerton.
Ejecute Pinkerton con permisos de administrador.
terry@ubuntu:~/Desktop/pinkerton$
```

Imagen 7: Ejecución de *Pinkerton* sin privilegios de Administrador (root)

Al ejecutarse, se instalan los archivos necesarios en el directorio **'/root/pinkerton'**. A partir de ese momento se podrá ejecutar el comando *"pinkerton"* desde cualquier directorio (siempre que se tenga privilegios de Administrador o root). Si se ejecuta todo correctamente, se mostrará la interfaz de *Pinkerton*.





Imagen8: Interfaz de *Pinkerton*

## Utilización

El único trabajo que el usuario deberá de hacer es introducir el código de la encuesta (código de 8 letras que se le debe haber facilitado) mediante el recuadro de inserción de texto, y validar el mismo con el botón 'VALIDAR'.

En caso de introducir un código erróneo, el fondo del recuadro de texto se pondrá de color rojo. En caso de ser correcto el código introducido, el área de texto dejará de ser un campo editable y el botón 'VALIDAR' desaparecerá.

La interfaz también dispone de un botón para 'LANZAR' y 'PARAR' el escaneo de *Pinkerton*. Una vez que el análisis se ha completado, dicho botón también desaparecerá.

Mediante el botón 'AYUDA' se accede a información básica sobre *Pinkerton* e información de contacto.

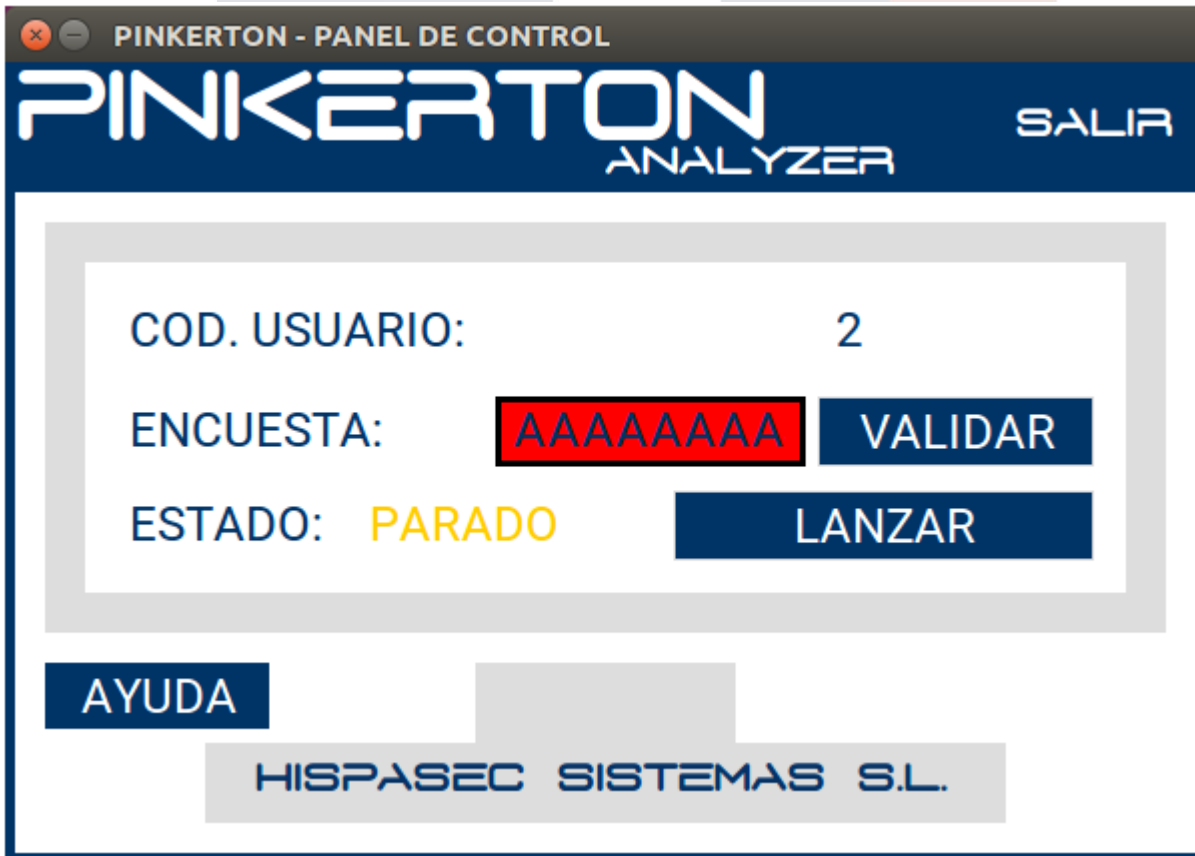


Imagen9: Código de encuesta erróneo



Imagen10: Código de encuesta validado



# Desinstalación

Para desinstalar Pinkerton, se debe ejecutar el comando siguiente:

```
"sudo pinkerton -u"
```

El cual eliminará todos los ficheros creados por *Pinkerton*. A este comando se le puede añadir el parámetro "-v" si se quiere obtener información extra del proceso de desinstalación.



```
terry@ubuntu: ~/Desktop
terry@ubuntu:~/Desktop$ sudo pinkerton -v -u
*****
<< Lanzando >>
*****
<< Pinkerton: __init__ >>
Directorio creado: /root/pinkerton/data/pinkerton.conf
<< Pinkerton: uninstall >>
Aplicación desinstalada correctamente.
*****
<< Terminado >>
*****
terry@ubuntu:~/Desktop$
```

Imagen11: Desinstalación de *Pinkerton*

## FAQ

- **¿Cuánto ocupa el software?**

El software *Pinkerton* ocupa alrededor de 300 KB de espacio en el disco duro. Aparte, el motor *python3* necesita unos 125 MB adicionales.

- **¿Cuánto tarda en instalarse?**

La duración de la instalación varía en función del ordenador y/o programas instalados, siendo el tiempo estimado de unos 5 minutos.

- **¿Dónde puedo instalar el software?**

Este software es única, y exclusivamente para ordenadores de sobremesa o portátiles con sistema operativo GNU/Linux.

- **¿Tengo que reiniciar mi ordenador después de la instalación?**

No, no es necesario.

- **¿Cuándo está en uso el software?**

El software se ejecuta automáticamente en cada inicio del sistema y comprueba si el análisis ha sido completado y, si ese es el caso, *Pinkerton* finaliza inmediatamente. En caso contrario continuará el análisis desde el punto en que fue detenido.





El análisis completo dura aproximadamente entre 30 y 60 minutos y se realiza de forma trimestral.

El usuario puede comprobar el estado del escaneo ejecutando manualmente el programa *Pinkerton*.

- **¿Cómo y quién avala este software? ¿Puedo confiar en el software?**

El programa está firmado digitalmente por *Hispacec Sistemas*, una empresa española con más de 20 años de experiencia en el sector de la seguridad informática, lo que garantiza su integridad e inocuidad.

- **¿Y si no quiero utilizarlo más?**

Puede desinstalarlo sin ningún problema, para ello mire la sección de desinstalación.

- **¿Tengo que preocuparme en el mantenimiento y uso del programa?**

Una vez instalado, la única acción necesaria será introducir el número de encuesta proporcionado por GFK, la empresa que ha realizado la misma. Solamente debe ejecutar el programa una vez dentro de cada mes natural (sin importar el día).

El programa no necesita ningún otro tipo de mantenimiento ni atención. *Pinkerton* funciona de forma transparente y sin entorpecer las tareas que el usuario realice en el equipo durante el análisis.

- **¿Qué instala el software en el ordenador?**

El software instala un analizador que se encargará de recoger la información exclusivamente necesaria sobre sistemas de seguridad y malware existente en el equipo de forma trimestral.

- **¿Qué información recoge de mi ordenador?**

*Pinkerton* recoge la información necesaria para hacer el estudio sobre la e-confianza de los hogares españoles. Entre la información típica se encuentra el navegador utilizado por defecto, tipo de cuenta de usuario (con o sin privilegios), uso de firewall, software antivirus, etc.





# Hispa**sec**]

C/ Severo Ochoa 10,  
29590 Málaga  
España  
Telf: (+34) 952 020 494

Información General: [pinkerton@hispacec.com](mailto:pinkerton@hispacec.com)

Salvo que se indique lo contrario, esta información es CONFIDENCIAL y contiene datos de carácter personal que han de ser tratados conforme a la legislación vigente en materia de protección de datos. Si usted no es destinatario original de esta información, le comunicamos que no está autorizado a revisar, reenviar, distribuir, copiar o imprimir la información en él contenida y le rogamos que proceda a borrarla de sus sistemas.