

MANUAL DE USO

En este apartado se mostrará, además del proceso de instalación del dispositivo, una explicación para el correcto uso del sistema y una guía por las distintas funcionalidades que se ofrecen al usuario.

1. Instalación *Cibercanario*

La instalación del Cibercanario es un proceso simple, en pocos pasos estará totalmente configurado y funcionando.

Antes de introducir la microSD en el dispositivo, será necesario conectarlo al ordenador (que deberá tener un lector de tarjetas SD) con un adaptador microSD. Tras eso habrá que acceder al contenido de la tarjeta microSD con el *Explorador de archivos* (o cualquier gestor de este tipo).

Buscar el archivo *network_config* y abrirlo con un editor de texto. Este archivo nos permite conectarle la red WIFI antes de ejecutarlo con la Raspberry.

```
# This file contains a netplan-compatible configuration which cloud-init
# will apply on first-boot. Please refer to the cloud-init documentation and
# the netplan reference for full details:
#
# https://cloudinit.readthedocs.io/
# https://netplan.io/reference
#
# Some additional examples are commented out below

version: 2
ethernets:
  eth0:
    dhcp4: true
    optional: true
wifis:
  wlan0:
    dhcp4: true
    optional: true
    access-points:
      My_WIFI:
        password: "papopepo"
```

FIGURA B.1: CONFIGURACIÓN WIFI

Habr  que indicar como se indica en la **Figura B.1**, el nombre de la red y la contrase a de esta. No ser  necesario modificar ning n elemento del resto del documento.

Tras esto, guardar el archivo, desconectar del ordenador, conectar al dispositivo e iniciarla. Lo primero que solicitar  al iniciarlo ser  un usuario y contrase a que son los siguientes:

- Nombre de usuario: **ubuntu**
- Contrase a: **ubuntu**

Se solicitar  modificar la contrase a (la cual se pedir  introducir junto al nombre de usuario cada vez que se encienda el *Cibercanario*) y tras hacerlo, el sistema se iniciar  y la aplicaci n empezar  a funcionar.

2. Detecci n de amenazas

Una vez que el *Cibercanario* es iniciado y se muestra la pantalla inicial (**Figura B.2**), comenzar  autom ticamente a detectar cualquier amenaza que pueda aparecer.

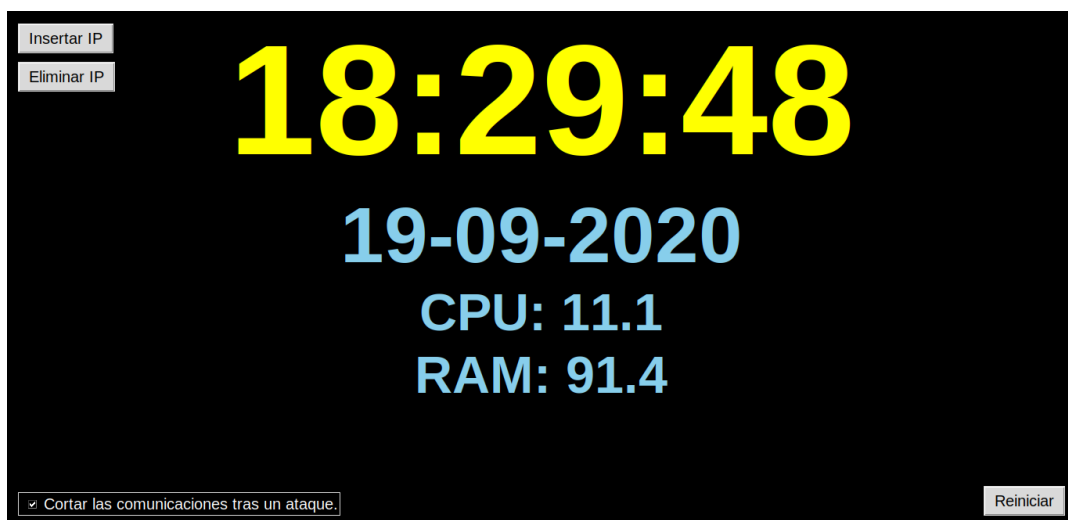


FIGURA B.2: PANTALLA INICIAL CIBERCANARIO

Cuando la amenaza aparezca, se mostrará una pantalla en la que se advierte de la misma, junto con la hora a la que se ha detectado y un listado en el que se detalla brevemente que se ha detectado. Si se ha indicado que se corten las comunicaciones tras detectar un ataque (ver apartado 4 de este manual), el dispositivo no detectará más amenazas hasta que no se reinicie (ver apartado 5 de este manual).

3. Insertar nueva IP

Para insertar una nueva IP a la *lista blanca* (listado de IPs que el *Cibercanario* no detectará como amenazas), se deberá, estando en la pantalla inicial, clicar en el botón de *Insertar IP*.

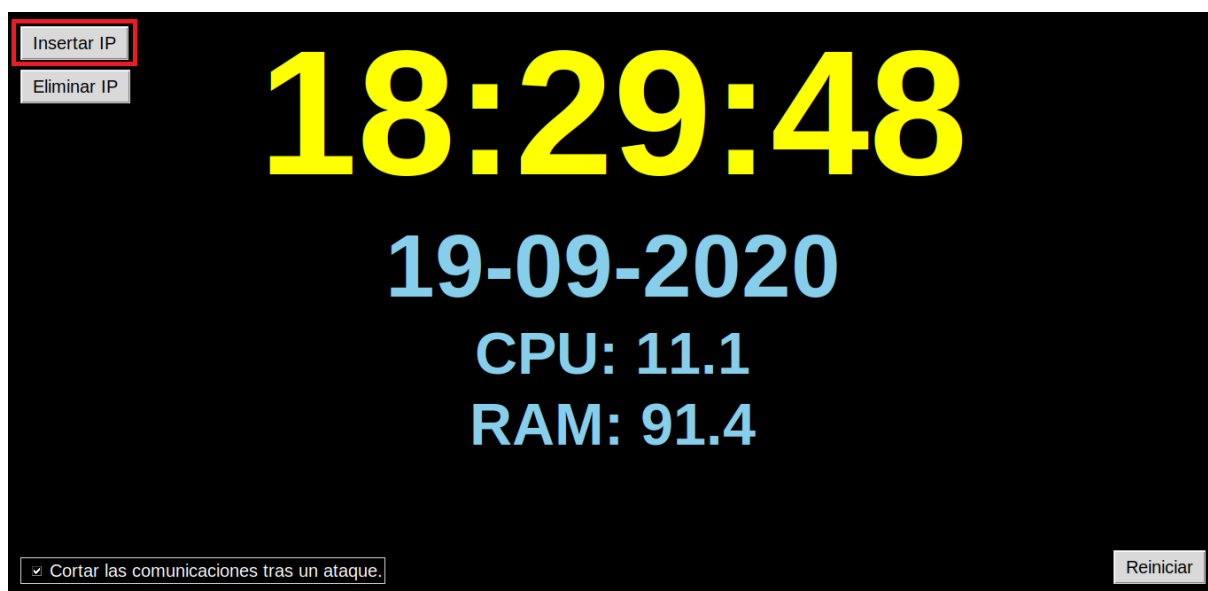
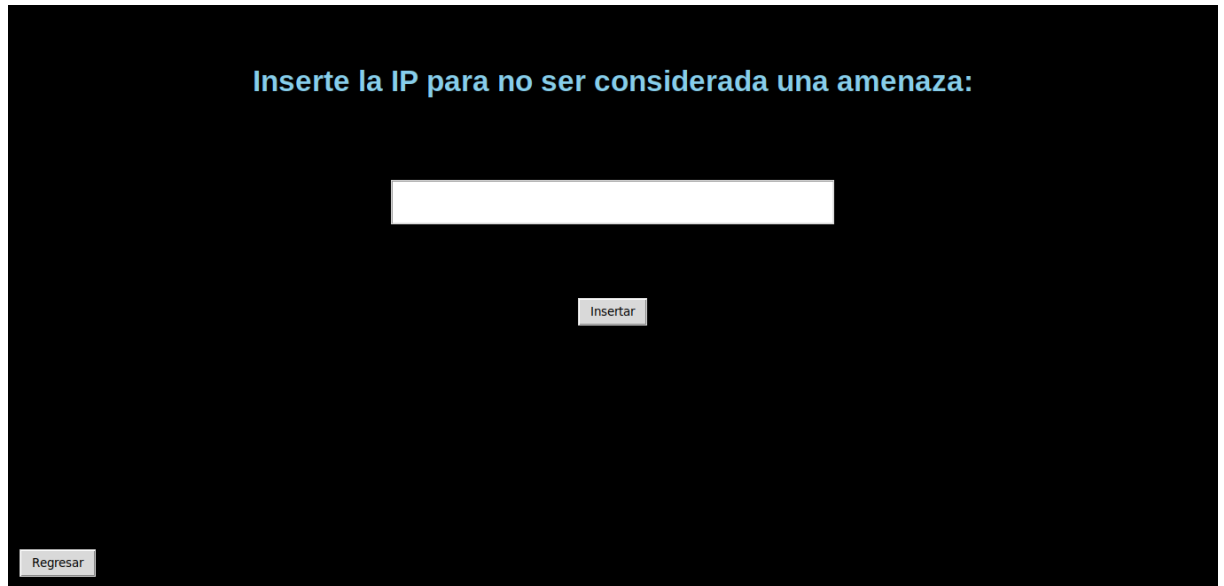


FIGURA B.3: BOTÓN PARA INSERTAR NUEVA IP

Tras esto aparecerá una pantalla (**Figura B.3**) en la que el usuario puede introducir una determinada IP en el cuadro de texto que aparece. Debe tenerse en cuenta que el cuadro de texto no deberá estar vacío, que la IP no debe estar ya incluida en la *lista blanca* y que la IP introducida deberá mantener la estructura de este tipo de direcciones: XXX.XXX.XXX.XXX (p.e. 192.168.1.72). Si estas tres condiciones se cumplen, al clicar en el botón que se encuentra justo

debajo del cuadro de texto (*Insertar*) se guardará la IP, en caso contrario aparecerá un mensaje de error.

En caso de no querer hacer ninguna operación, se puede regresar a la pantalla inicial (**Figura B.2**) clicando en el botón de *Regresar* que se encuentra en la esquina inferior izquierda.



The screenshot shows a web interface with a black background. At the top, the text "Inserte la IP para no ser considerada una amenaza:" is displayed in a light blue font. Below this text is a white rectangular input field. Underneath the input field is a small, light gray button labeled "Insertar". In the bottom left corner, there is another small, light gray button labeled "Regresar".

FIGURA B.4: INSERTAR NUEVA IP

4. Borrar IP existente

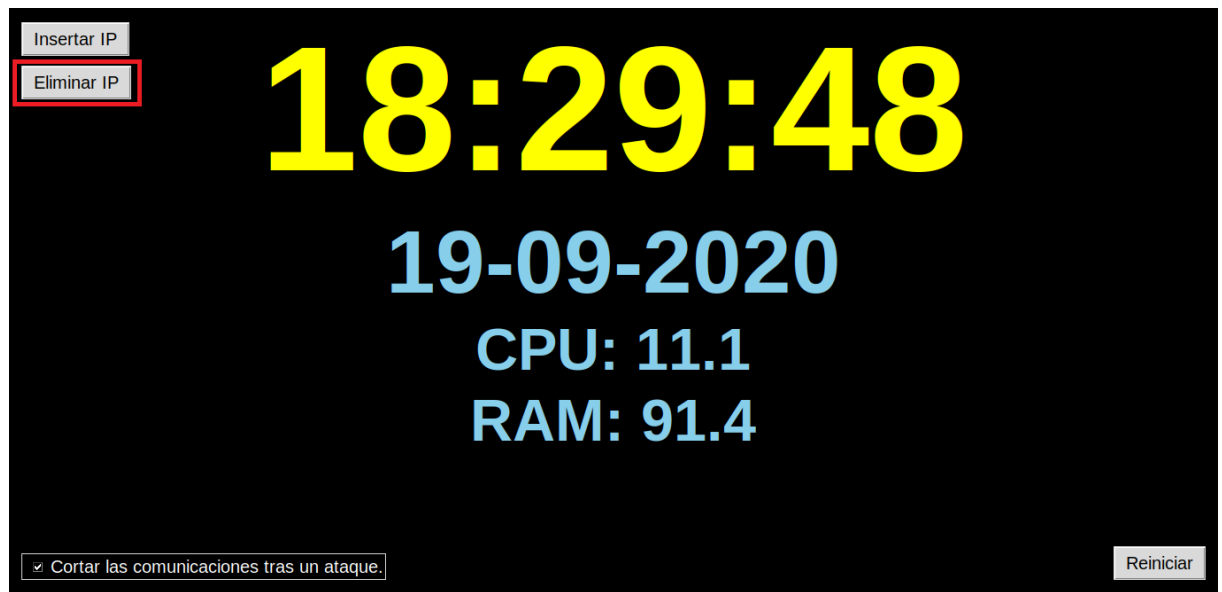


FIGURA B.5: BOTÓN BORRAR IP EXISTENTE

Para borrar una nueva IP ya existente de la *lista blanca*, se deberá, estando en la pantalla inicial, clicar en el botón de Eliminar IP.

Tras esto aparecerá una pantalla (**Figura B.6**) en la que el usuario puede señalar de la lista que se le muestra una IP. Debe tenerse en cuenta que se deberá realizar una selección antes de clicar en el botón *Eliminar*. En caso contrario se mostrará un mensaje de error. Si se encuentra seleccionada, al clicar en dicho botón que se encuentra justo debajo de la lista se eliminará la IP.

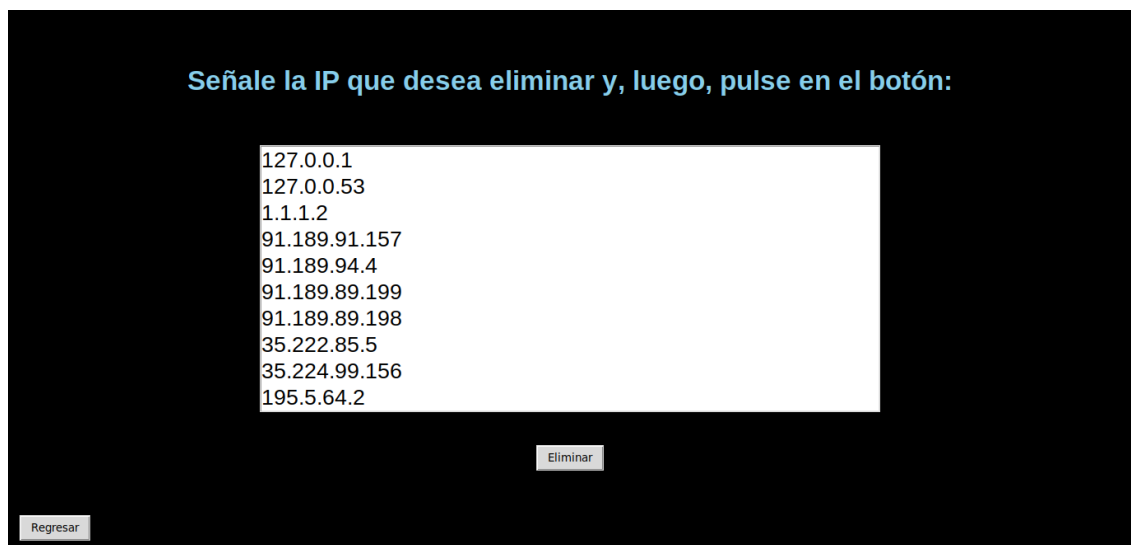


FIGURA B.6: BOTÓN BORRAR IP EXISTENTE

En caso de no querer hacer ninguna operación, se puede regresar a la pantalla inicial (**Figura A.2**) clicando en el botón de *Regresar* que se encuentra en la esquina inferior izquierda.

5. Cortar comunicaciones tras detectar una amenaza

Si se desea que, tras detectar un ataque, el *Cibercanario* cierre las comunicaciones se deberá señalar el recuadro que aparece en página inicial (**Figura B.7**). En caso contrario, se deberá dejar sin señalar (por defecto estará seleccionado).

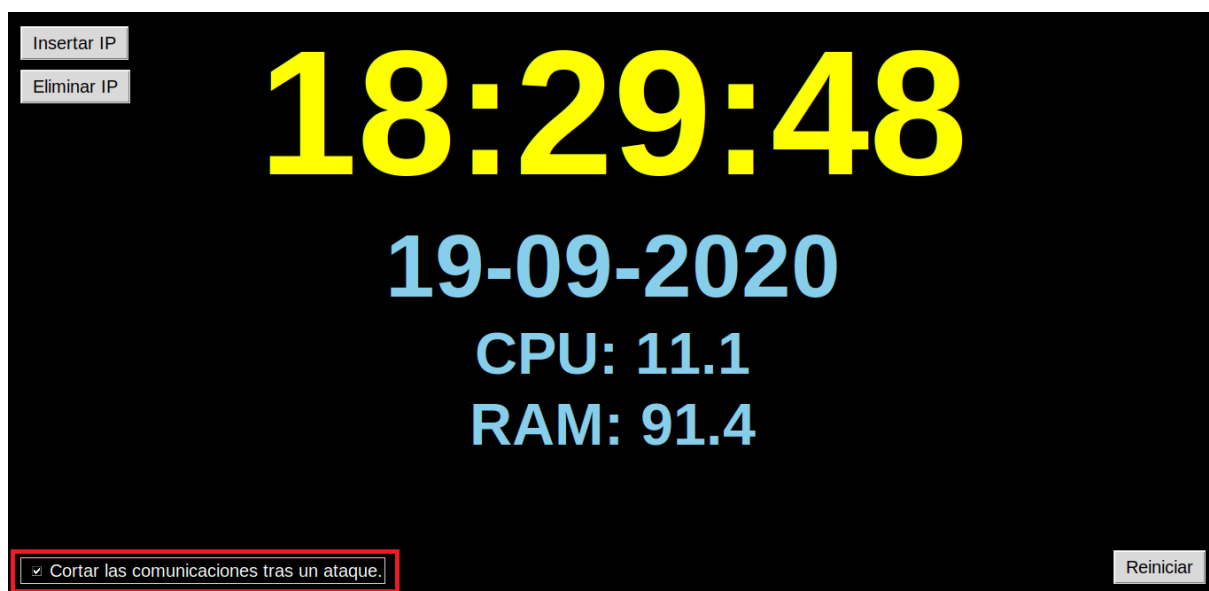


FIGURA B.7: BOTÓN BORRAR IP EXISTENTE

6. Reiniciar el *Cibercanario*

Si se desea que el *Cibercanario* se reinicie y vuelva a abrir las comunicaciones (si se han cerrado), deberá clicar en el botón de *Reiniciar* en la pantalla inicial.

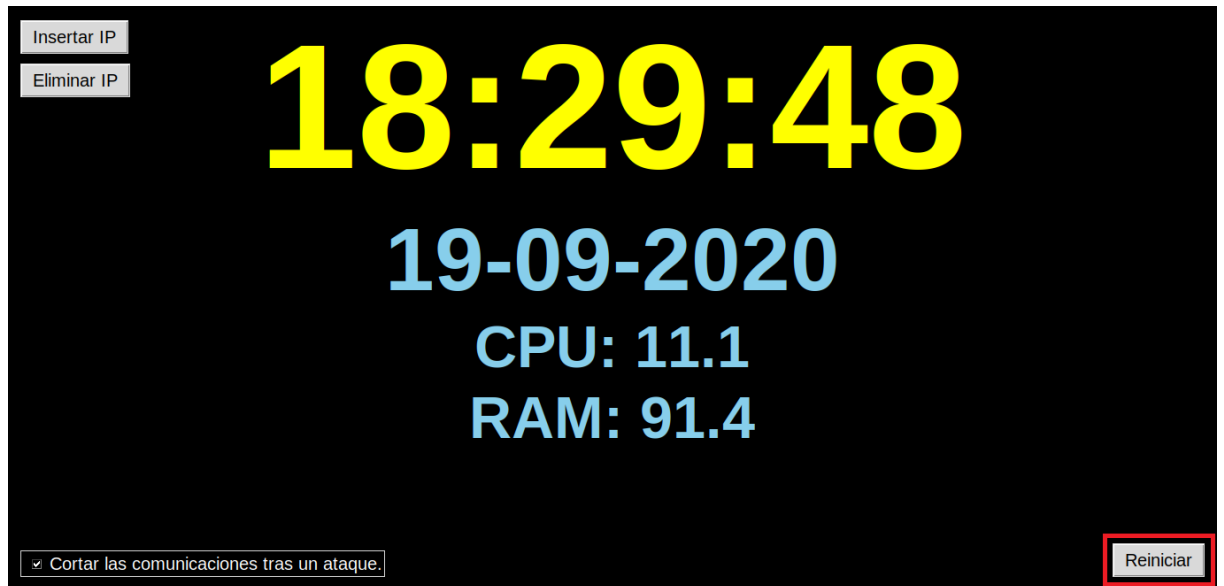


FIGURA B.8: BOTÓN REINICIAR *CIBERCANARIO*