3.12 Pi alert. ¿Intrusos en tu red?

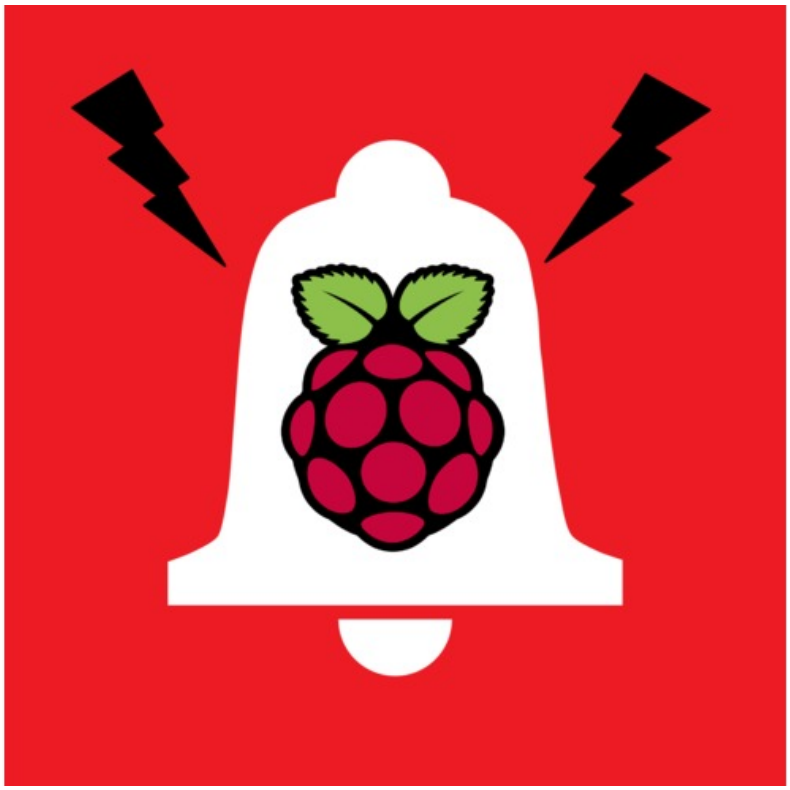


Imagen obtenida de https://devpost.com/software/pialert

> Este proyecto lleva mas de 2 años sin ser actualizado

Esta herramienta sirve para...

detectar nuevos equipos conectados en nuestra red de modo que si aparece algún equipo nuevo del cuál no estamos al tanto detectaremos una conexión no permitida.

Copyright 2026

Web de proyecto y otros enlaces de interés

Repositorio de código original: https://github.com/pucherot/Pi.Alert

Imagen que utilizaremos: https://registry.hub.docker.com/r/jokobsk/pi.alert

Despliegue

Como en ocasiones anteriores vamos a hacer con docker-compose para ello accedemos al terminal y escribimos

```
cd $HOME
mkdir pialert
cd pialert
nano docker-compose.yml
```

y dentro del fichero escribiremos el siguiente contenido

```
version: "3"
services:
  pialert:
    image: jokobsk/pi.alert
    ports:
      - "20211:20211/tcp"
    environment:
      - TZ=Europe/Madrid
    restart: unless-stopped
    volumes:
      - ./pialert_db:/home/pi/pialert/db
      - ./config/pialert.conf:/home/pi/pialert/config/pialert.conf
```

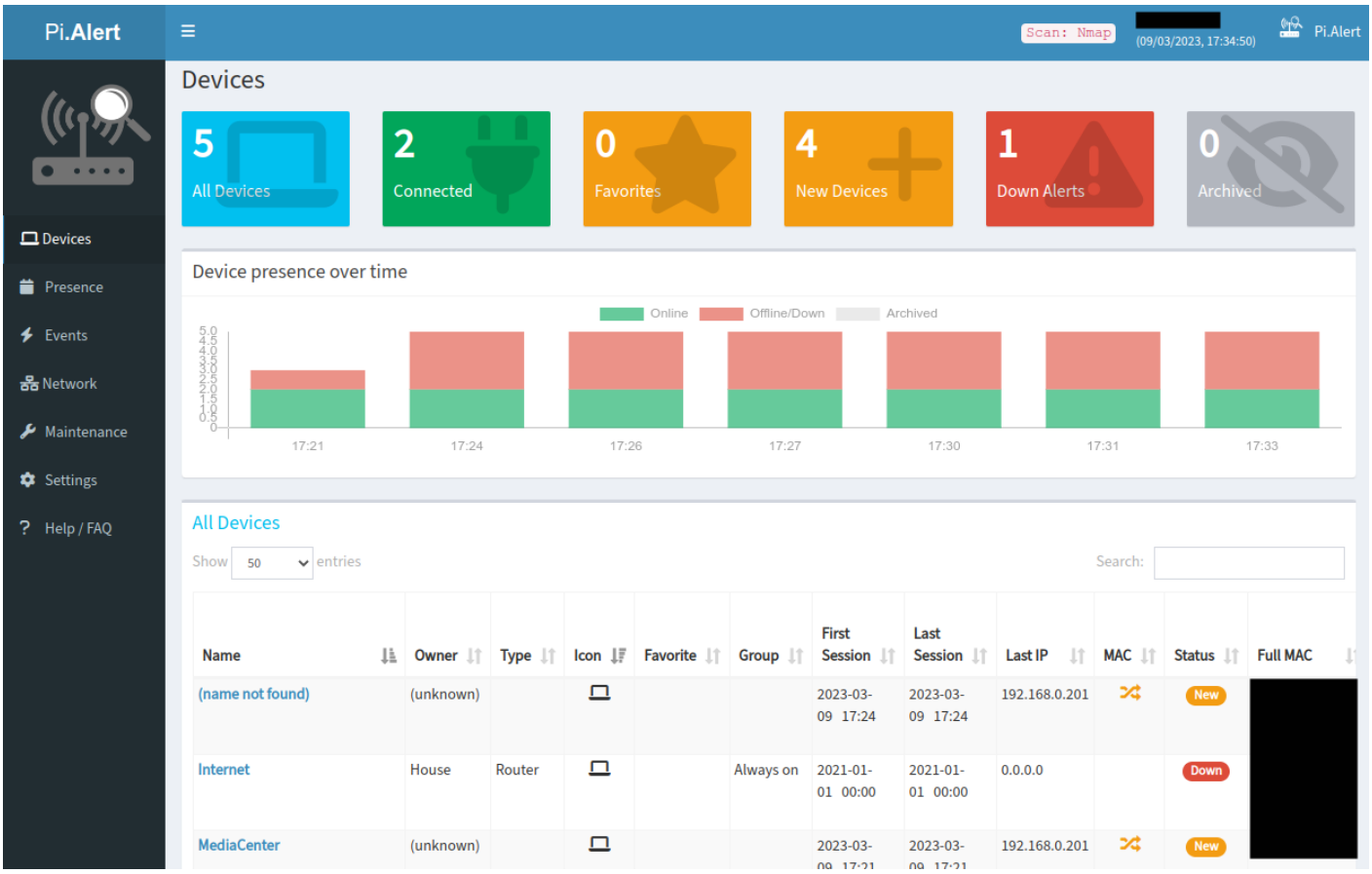
Copyright 2026

como en ocasiones anteriores, para guardar los cambios pulsaremos control + x y cuando nos pregunte aceptaremos. Una vez volvamos a estar en el terminal, escribiremos `docker compose up -d` para lanzar los servicios ubicados dentro del fichero docker-compose. Veremos algo similar a:

```
pi@mediacenter:/etc/docker $ cd $HOME
mkdir pialert
cd pialert
nano docker-compose.yml
pi@mediacenter:~/pialert $ docker-compose up -d
Pulling pialert (jokobsk/pi.alert:latest)...
latest: Pulling from jokobsk/pi.alert
934ce60d1040: Pull complete
d7da1afcf2bf: Pull complete
58d607f924cb: Pull complete
c9b26a498401: Pull complete
cecde2be4312: Pull complete
Digest: sha256:9a2472cd37540a5f2be1f3c5bf1a14912e80063adab80d1530efc7d76216bcf9
Status: Downloaded newer image for jokobsk/pi.alert:latest
Creating pialert ... done
pi@mediacenter:~/pialert $ ls -la
total 24
drwxr-xr-x  5 pi   pi   4096 mar  9 16:50 .
drwxr-xr-x 28 pi   pi   4096 mar  9 16:43 ..
drwxr-xr-x  2 root root 4096 mar  9 16:50 config
drwxr-xr-x  2 root root 4096 mar  9 16:50 db
-rw-r--r--  1 pi   pi    415 mar  9 16:43 docker-compose.yml
drwxr-xr-x  2 root root 4096 mar  9 16:50 logs
```

Elaboración propia

Si accedéis en vuestro navegador a la IP de la raspberry y al puerto que hemos establecido (20211). En mi caso sería http://192.168.0.201:20211 deberíais ver algo como:



Elaboración propia

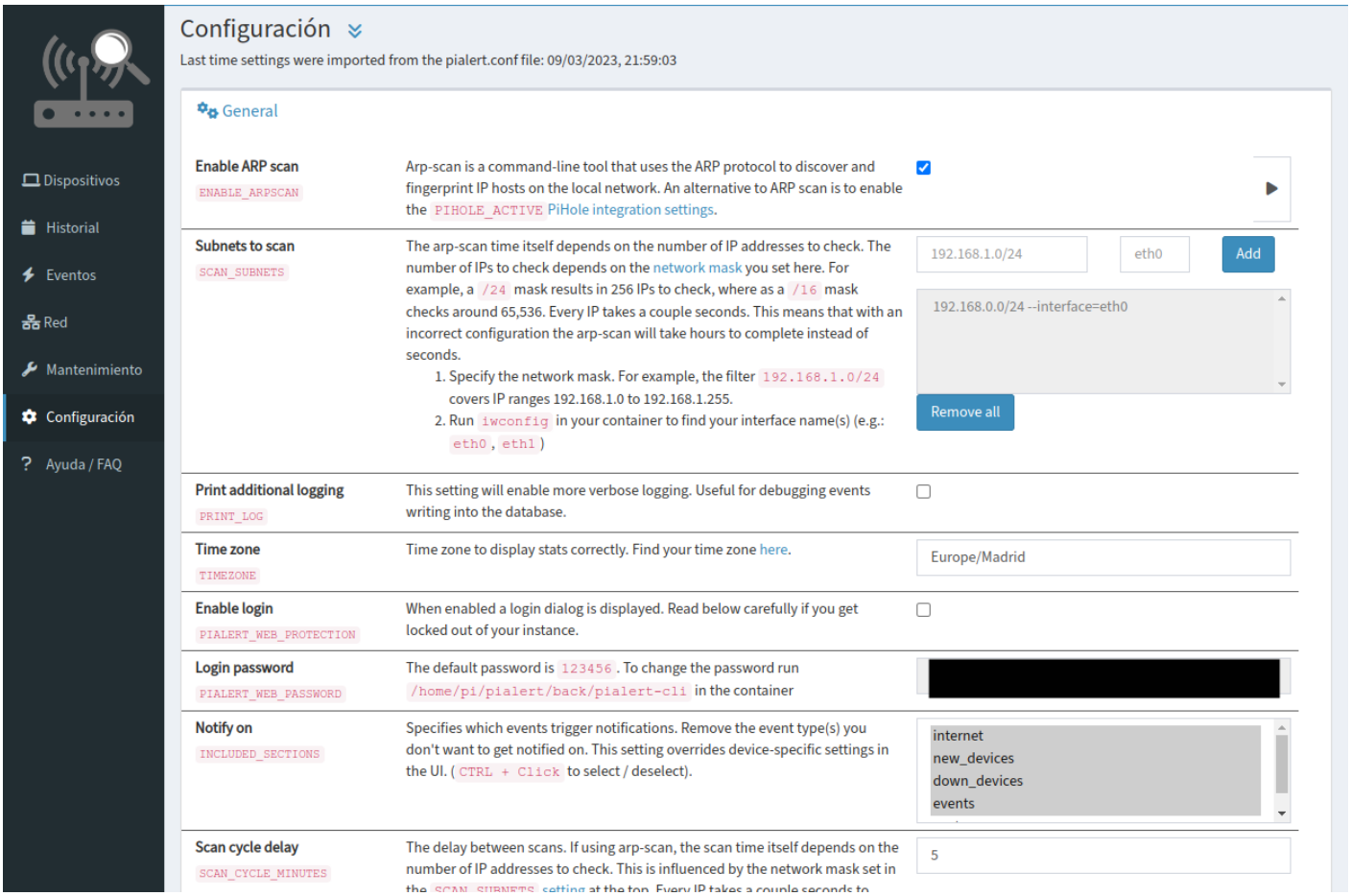
Funcionamiento

Nada mas acceder accederás a una pantalla como la anterior. En la mismas verás 4 partes claramente delimitadas:

- un menú lateral a la izquierda
- una parte central dividida en 3 franjas horizontales:
  - botonera de dispositivos
  - gráfica con las horas y dispositivos encontrados (conectados y no conectados)
  - listado de elementos encontrados (nombre, tipo, IP, MAC, estado,...)

Del menú lateral nos interesará acceder a la sección de Configuración (Settings).

Copyright 2026

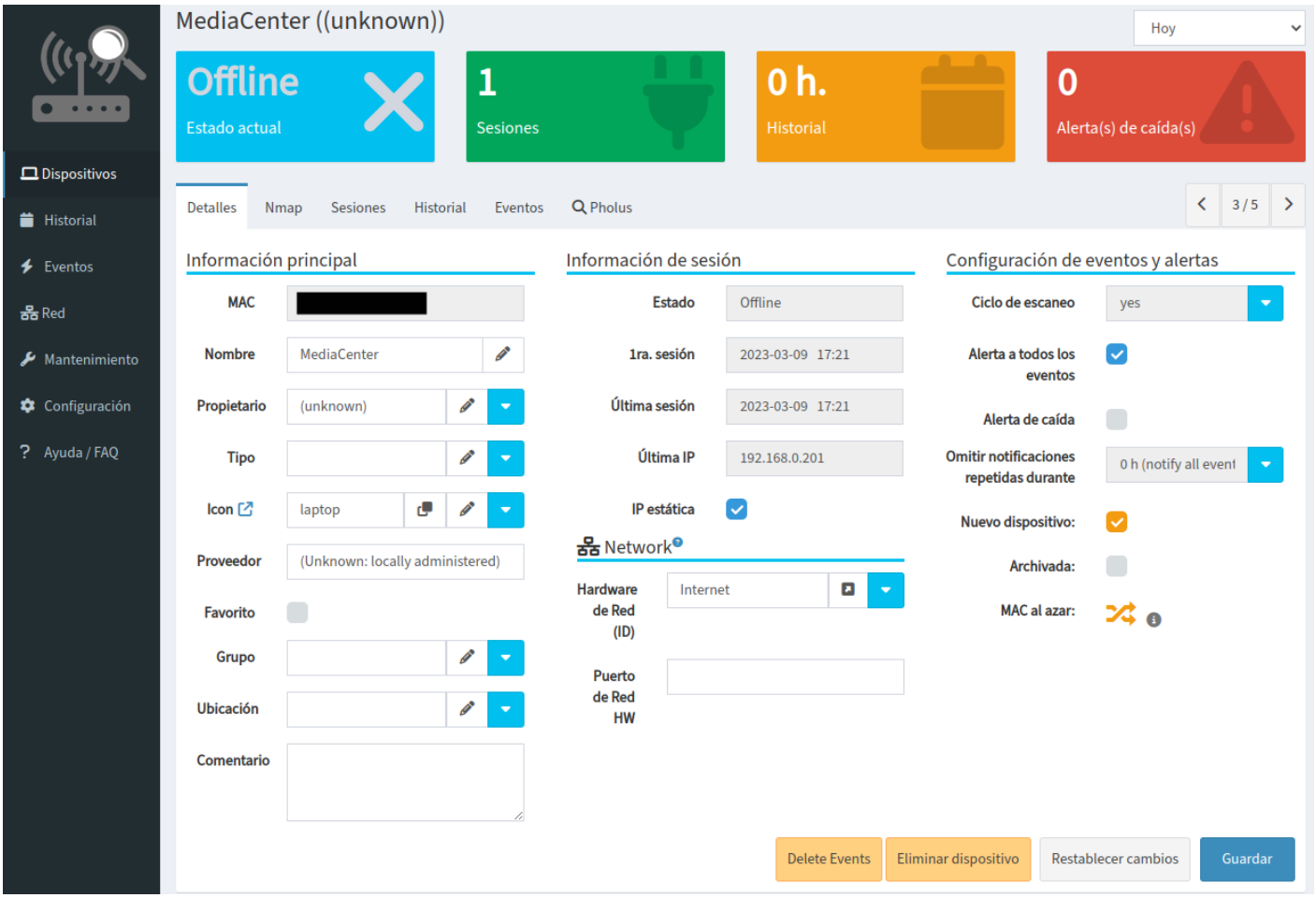


Elaboración propia

En este menú debes prestar especial atención a la opción que dice `Subnets to scan`, es decir, subredes a escanear. En mi caso, la red de mi casa es la 192.168.0.0/24 ¡ojo, lo habitual suele ser 192.168.**1**.0/24! y la interface de red que usa mi raspberry es eth0 de ahí mi configuración. En otras opciones que aparecen mas abajo podéis cambiar el idioma o configurar que os lleguen alertas de intrusión por email, MQTT (lo veremos en el apartado 4 de domótica). Webhooks u otras opciones.

Si pincháis en el nombre de un dispositivo aparecerá una pantalla como la siguiente

Copyright 2026



Elaboración propia

En la cual podréis establecer algunas características del dispositivo como su nombre. Esto os ayudará en el futuro, en las estadísticas, a identificar el dispositivo.

Revision #8
Created 2023-02-04 10:07:35 CET by Pablo Ruiz
Updated 2023-07-20 18:05:30 CEST by Pablo Ruiz