

Geolocalizacion

31/10/2023

Guillermo Bellettini

Seguridad

Creado por: Nicolas Pavel Ballesteros Barrado



Contenido

Principios Seguridad Informatica Cifrado Simetrico ¡Error! Marcador no definido.

Instalamos nmap	3
Escaneamos la pagina web amoridealmadrid.es	3
Probamos con otra pagina	4
Hacemos ping a la pagina web amoridealmadrid.es.....	4
Vamos a geoip.com.....	5
Nos vamos a geoiptool.de.....	6
Nos vamos a geodatatool.....	7
Nos vamos a nordvpn.com.....	7
Nos vamos a internautas.org	8
Escanemos puertos mas habituales	9
Instalamos extensión	10
Se nos cambia la ip.....	10
Verificamos en geodatatool	11
Verificamos en internautas.org	12
Desactivamos vpn.....	13
Ponemos la ip publica en geoiptool.de.....	14
Verificamos en geodata	16

Instalamos nmap

```
root@ubuntu:~# apt install nmap
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
El paquete indicado a continuación se instaló de forma automática y ya no es necesario.
  liblvm6.0
Utilice «sudo apt autoremove» para eliminarlo.
Se instalarán los siguientes paquetes adicionales:
  libblas3 liblinear3 liblua5.3-0
Paquetes sugeridos:
  liblinear-tools liblinear-dev ndiff
Se instalarán los siguientes paquetes NUEVOS:
  libblas3 liblinear3 liblua5.3-0 nmap
0 actualizados, 4 nuevos se instalarán, 0 para eliminar y 0 no actualizados.
Se necesita descargar 5.467 kB de archivos.
Se utilizarán 25,0 MB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n] s
```

Escaneamos la pagina web amoridealmadrid.es

```
root@ubuntu:~# nmap --script ip-geolocation-geoplugin www.amoridealmadrid.es

Starting Nmap 7.60 ( https://nmap.org ) at 2023-10-31 18:03 CET
Nmap scan report for www.amoridealmadrid.es (185.14.58.130)
Host is up (0.012s latency).
rDNS record for 185.14.58.130: vm290.dnspropio.com
Not shown: 994 filtered ports
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
113/tcp   closed ident
443/tcp   open  https
993/tcp   open  imaps
8010/tcp  closed xmpp

Host script results:
| ip-geolocation-geoplugin:
|_185.14.58.130 (www.amoridealmadrid.es)

Nmap done: 1 IP address (1 host up) scanned in 6.07 seconds
root@ubuntu:~# |
```

Probamos con otra pagina

```
root@ubuntu:~# nmap --script ip-geolocation-geoplugin www.ceu.es

Starting Nmap 7.60 ( https://nmap.org ) at 2023-10-31 18:19 CET
Nmap scan report for www.ceu.es (104.18.9.169)
Host is up (0.0011s latency).
Other addresses for www.ceu.es (not scanned): 104.18.8.169
Not shown: 995 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
113/tcp   closed ident
443/tcp    open  https
8080/tcp   open  http-proxy
8443/tcp   open  https-alt

Host script results:
|_ip-geolocation-geoplugin: ERROR: Script execution failed (use -d to debug)

Nmap done: 1 IP address (1 host up) scanned in 17.04 seconds
root@ubuntu:~# |
```

Hacemos ping a la pagina web amoridealmadrid.es

```
root@ubuntu:~# ping www.amoridealmadrid.es
PING www.amoridealmadrid.es (185.14.58.130) 56(84) bytes of data.

^C
--- www.amoridealmadrid.es ping statistics ---
24 packets transmitted, 0 received, 100% packet loss, time 23567ms

root@ubuntu:~# |
```

Vamos a geoip.com



Enviar

success

Spain

MC

Murcia

Alcantarilla

30820

37.9587

-1.19451

SYS4NET B1

AS202054 GRUPO SYS4NET, S.L.

false

false

185.14.58.130

Your query results will be displayed above

Nos dice de donde es la ip

Nos vamos a geoiptool.de

GEO information for IP 185.14.58.130

We found some Information about this IP.

Location

Continent	Europe (EU)
Country	Spain (ES)
Region	Murcia (MC)
City	N/A
Postal code	N/A

Location on Map [© OpenStreetMap &

Contributors, CC-BY-SA]



Host name

The corresponding host name for this IP address is `vm290.dnspropio.com`.

Organization

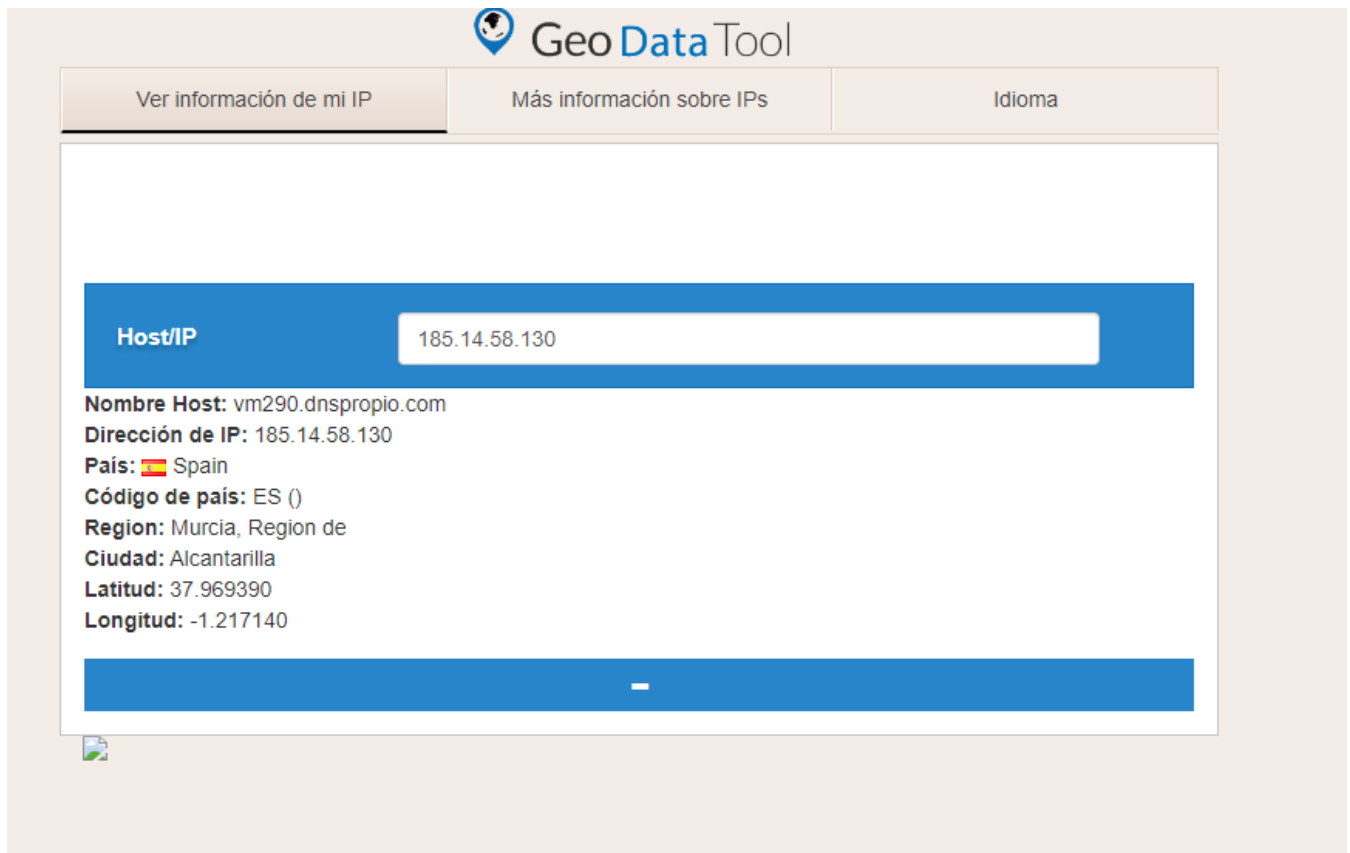
Internet Service Provider (ISP)

Internet Service Provider	Grupo Sys4net, S.L.
Autonomous System Organization	Grupo Sys4net, S.L.
Autonomous System Number	AS202054

Miscellaneous

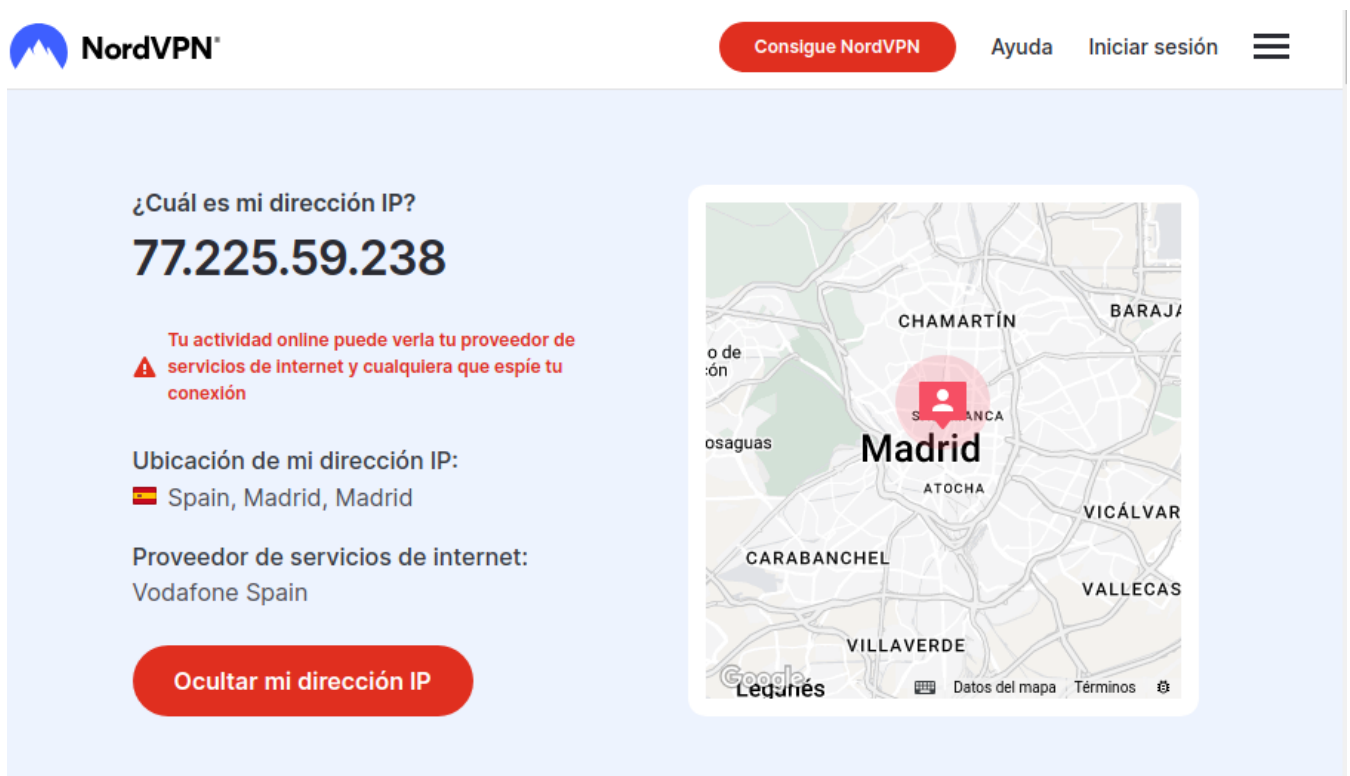
Timezone	Europe/Madrid
Local time	2023-10-31T18:39:04+01:00
Connection type	Cable/DSL

Nos vamos a geodatatool



The screenshot shows the GeoDataTool website interface. At the top, there's a navigation bar with three links: "Ver información de mi IP", "Más información sobre IPs", and "Idioma". Below this, a large blue box contains the "Host/IP" field with the value "185.14.58.130". Underneath, a list of details is provided: "Nombre Host: vm290.dnspropio.com", "Dirección de IP: 185.14.58.130", "País: Spain", "Código de país: ES ()", "Region: Murcia, Region de", "Ciudad: Alcantarilla", "Latitud: 37.969390", and "Longitud: -1.217140". A small map icon is visible at the bottom left of the main content area.

Nos vamos a nordvpn.com



The screenshot shows the NordVPN website interface. At the top, there's a navigation bar with the NordVPN logo, a red button "Consigue NordVPN", and links for "Ayuda", "Iniciar sesión", and a menu icon. The main content area has a light blue background. On the left, it asks "¿Cuál es mi dirección IP?" and displays "77.225.59.238" in large bold text. Below this, a warning icon and text state: "Tu actividad online puede verla tu proveedor de servicios de Internet y cualquiera que espíe tu conexión". Further down, it shows "Ubicación de mi dirección IP:" followed by "Spain, Madrid, Madrid" and "Proveedor de servicios de internet: Vodafone Spain". A red button "Ocultar mi dirección IP" is at the bottom left. On the right, there's a map of Madrid with a red location pin and the word "Madrid" in bold. The map shows various districts like CHAMARTÍN, BARAJA, ATOCHA, VICÁLVAR, VALLECAS, VILLAVERDE, and CARABANCHEL. The Google Maps logo and "Legués" are visible at the bottom of the map.

Cogemos ip

Nos vamos a internautas.org

Este es un escan de puertos (que son los puertos) y muy simple que se realiza a algunos de los principales puertos de tu PC desde nuestro servidor. Solo se comprueban si estan abiertos (recuadro rojo en columna de Estado) o, si estan cerrados o no existen

El visualizar esta página puede ser interpretado por determinados Firewalls como intentos de ataque desde el servidor en que internautas.org esta alojado. Se recomienda que pongas en conocimiento de tu administrador de red este hecho, ya que el mismo detectará el acceso a esta página como intento de ataque a puertos

[Listado de Puertos \(COMPLETO\)](#)

Escanea los puertos más habituales

Escaner a puertos específicos

Selecciona los puertos a escanear, máximo 5 puertos, separados por comas

Escanear

Escanemos puertos mas habituales

Puerto	Desc.	Estado	Observaciones
20	FTP	cerrado	Utilizado por FTP
21	FTP	cerrado	Utilizado por FTP
22	SSH	cerrado	Secure Shell.
23	TELNET	cerrado	Acceso remoto
25	SMTP	cerrado	Servidor de correo SMTP
53	DNS	cerrado	Servidor DNS
79	FINGER	cerrado	Servidor de información de usuarios de un PC
80	HTTP	cerrado	Servidor web
110	POP3	cerrado	Servidor de correo POP3
119	NNTP	cerrado	Servidor de noticias
135	DCOM-scm	cerrado	Solo se puede cerrar a través de un cortafuegos
139	NETBIOS	cerrado	Compartición de Ficheros a través de una red
143	IMAP	cerrado	Servidor de correo IMAP
389	LDAP	cerrado	LDAP. Tambien Puede ser utilizado por Neetmeting
443	HTTPS	cerrado	Servidor web seguro
445	MSFT DS	cerrado	Server Message Block.
631	IPP	cerrado	Servidor de Impresion
1433	MS SQL	cerrado	Base de Datos de Microsoft
3306	MYSQL	cerrado	Base de Datos. MYSQL
5000	UDnP	cerrado	En windows está activado este

Instalamos extensión

IO > Extensiones > UltraSurf Security, Privacy & Unblock VPN



UltraSurf Security, Privacy & Unblock VPN

Desi

Destacado

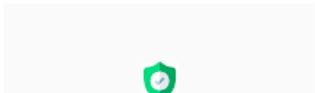
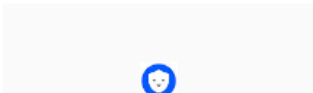
★★★★★ 18.602 ⓘ | Productividad | 900.000+ usuarios

Descripción general

Prácticas de privacidad

Reseñas

Relacionados



Se nos cambia la ip

¿Cuál es mi dirección IP?

74.82.60.22

Tu actividad online puede verla tu proveedor de servicios de internet y cualquiera que espíe tu conexión

Ubicación de mi dirección IP:

United States, California, Fremont

Proveedor de servicios de internet:

Hurricane Electric

Ocultar mi dirección IP



Verificamos en geodatatool

Host/IP

Nombre Host:

74.82.60.22

Dirección de IP:

74.82.60.22

País:

 United States

Código de país:

US ()

Region:

Wyoming

Ciudad:

Cheyenne

Latitud:

41.141572

Longitud:


-104.791325



Verificamos en internautas.org

Puerto	Desc.	Estado	Observaciones
20	FTP	cerrado	Utilizado por FTP
21	FTP	cerrado	Utilizado por FTP
22	SSH	cerrado	Secure Shell.
23	TELNET	cerrado	Acceso remoto
25	SMTP	cerrado	Servidor de correo SMTP
53	DNS	cerrado	Servidor DNS
79	FINGER	cerrado	Servidor de información de usuarios de un PC
80	HTTP	cerrado	Servidor web
110	POP3	cerrado	Servidor de correo POP3
119	NNTP	cerrado	Servidor de noticias
135	DCOM-scm	cerrado	Solo se puede cerrar a través de un cortafuegos
139	NETBIOS	cerrado	Compartición de Ficheros a través de una red
143	IMAP	cerrado	Servidor de correo IMAP
389	LDAP	cerrado	LDAP. Tambien Puede ser utilizado por Neetmeting
443	HTTPS	abierto	Servidor web seguro
445	MSFT DS	cerrado	Server Message Block.
631	IPP	cerrado	Servidor de Impresion
1433	MS SQL	cerrado	Base de Datos de Microsoft
3306	MYSQL	cerrado	Base de Datos. MYSQL
5000	UDP	cerrado	En windows está activado este

Desactivamos vpn

 **NordVPN®**

Consigue NordVPN

Ayuda

Iniciar sesión

☰

¿Cuál es mi dirección IP?

77.225.59.238

Tu actividad online puede verla tu proveedor de servicios de Internet y cualquiera que espíe tu conexión

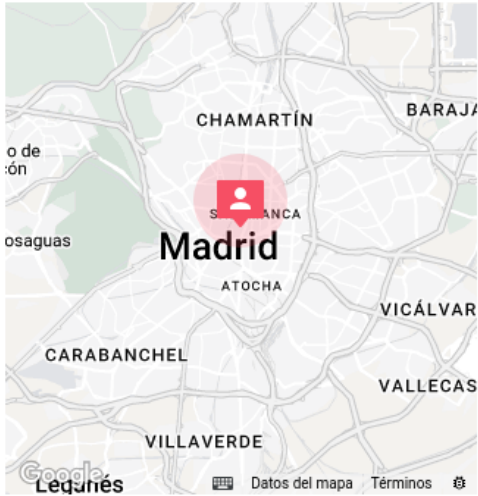
Ubicación de mi dirección IP:

🇪🇸 Spain, Madrid, Madrid

Proveedor de servicios de internet:

Vodafone Spain

Ocultar mi dirección IP



Por qué cambiar tu IP

¿Qué es una dirección IP?

Cómo encontrar tu IP

IPv4 frente a IPv6

IPv6: ¿a qué se debe el retraso?

>

Y volvemos a tener la ip de antes

Ponemos la ip publica en geoiptool.de

GEO information for IP 77.225.59.238

We found some Information about this IP.

Location

Continent	Europe (EU)
Country	Spain (ES)
Region	N/A
City	N/A
Postal code	N/A

Organization

Location on Map [© OpenStreetMap & Contributors, CC-BY-SA]



Host name

The corresponding host name for this IP address is **static-238-59-225-77.ipcom.comunitel.net**.

Region	N/A
--------	-----

City	N/A
------	-----

Postal code	N/A
-------------	-----



Host name

The corresponding host name for this IP address is **static-238-59-225-77.ipcom.comunitel.net**.

Organization

The IP address 77.225.59.238 is currently being used by **Vodafone Spain**.

Internet Service Provider (ISP)

Internet Service Provider	Vodafone Spain
---------------------------	----------------

Autonomous System Organization	Vodafone Spain
--------------------------------	----------------

Autonomous System Number	AS12430
--------------------------	---------

Miscellaneous

Timezone	Europe/Madrid
----------	---------------

Local time	2023-10-31T19:01:21+01:00
------------	---------------------------

Connection type	Cable/DSL
-----------------	-----------

Verificamos en geodata

