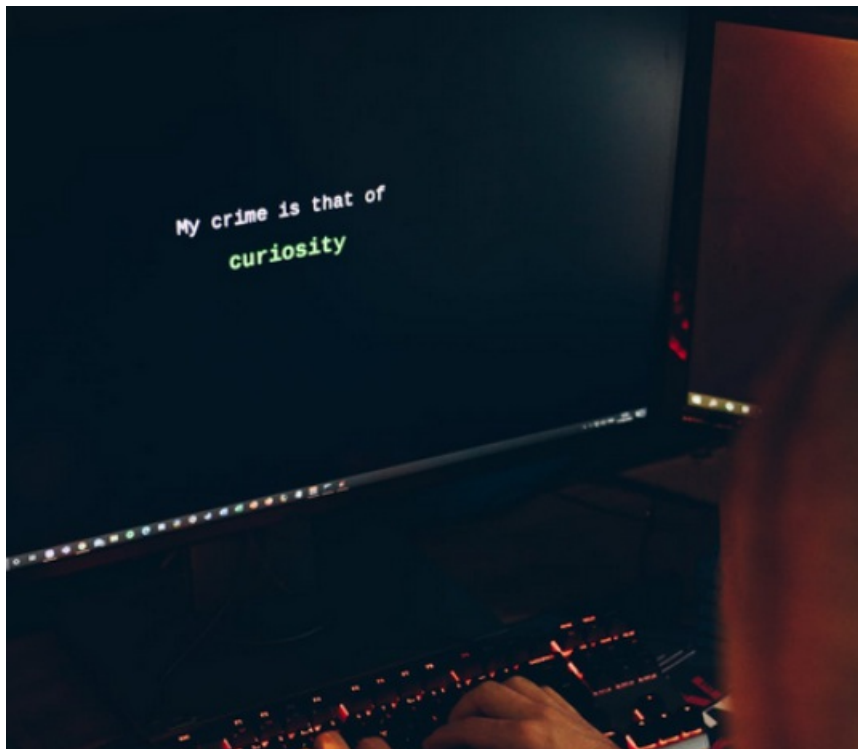


Tu ISP te está atacando, aunque tú no lo sepas (o lo ignores)

Publicado el [El Informatico](#) - 7 de febrero de 2022 -



Cuando usas internet, probablemente pienses que en caso de ataque se trata de algún miembro de alguna organización ilícita o del gobierno de algún país rival como por ejemplo China o Rusia (si resides en algún país miembro de la CEE o de la OTAN). Pero quizás no te hayas parado a pensar que antes de ellos hay actores maliciosos entre tus «amigos», que a base de excusas pueden lograr monitorizar tu tráfico y no sólo eso, también inyectar paquetes en tu tráfico de datos. Uno de esos buenos «amigos» que tienes es tu propio ISP (Internet Service Provider, o el Proveedor de Servicios de Internet. O tu compañía telefónica, para que nos entendamos). ¿Crees que es una teoría de la conspiración? Echa un vistazo a éste artículo y te lo demuestro con pruebas.

Tu ISP bloquea el tráfico a determinadas páginas web por ley

Esto no es nada nuevo, y me imagino que ya estareis tod@s al tanto del tema para

los que residais en España. A raíz de la famosa ley «Sinde», cualquier juez puede ordenar el bloqueo de una página web a los ISP de España de forma inmediata. Esta ley está prevista, en principio, para el bloqueo de páginas web que se dediquen a la distribución de material protegido por derechos de autor o que pudieran suponer una amenaza por algún motivo.

Sin entrar en más detalles sobre ésta ley, **todos estamos de acuerdo en que la distribución con ánimo de lucro de material protegido por derechos de autor no está bien y debe ser sancionado y tratado**. No pienso entrar en éste blog en debates sobre el tema, si bien tengo algunos argumentos en contra (Como el dichoso canon digital que todavía se nos impone y del que mucha gente no está al corriente). Pero si hay algo que trato en éste blog a menudo y que si **tengo muy en contra, son los métodos usados para bloquear éstas páginas web**.

¿Cómo se bloquea una página web?

Hay varios métodos para bloquear una página web. Dependiendo del país en el que residas y del servicio que utilices, tu ISP podría utilizar uno u otro.

Los dos métodos más conocidos y que probablemente a todo el mundo se les venga a la cabeza al hablar de bloquear contenido en la red, **son los bloqueos de IP, y bloqueos de dominio a nivel de DNS**. Estos dos métodos son los más sencillos, pero también son los más fáciles de sortear.

Bloqueo de IP

Las direcciones IP son el equivalente al número de una línea telefónica, pero en la red de internet (de hecho, Internet empezó sobre la línea telefónica). Cuando queremos conectar a un servicio en la red, nuestro cliente (por ejemplo, el navegador web) se conecta al servicio haciendo uso de ésta dirección IP.

Un bloqueo de IP consiste en una lista «negra» de direcciones a las que queremos denegar el acceso a los clientes de nuestra red. De modo que cuando se realiza una petición de conexión, si la petición se realiza a una de las direcciones de ésta lista, la conexión es denegada y se le devuelve un mensaje de error al usuario.

No obstante, **es muy sencillo saltarse éste tipo de bloqueos mediante el uso de proxys o VPNs**. Por lo que las ISP no utilizan éste método.

Bloqueo de dominio

Cuando nos conectamos a un servicio web, normalmente escribimos la dirección web en nuestro navegador. Esta dirección web contiene el protocolo, el nombre del dominio (y subdominio), y el 'endpoint' al que queremos acceder dentro de ese dominio. Por ejemplo, para la dirección: *<https://www.youtube.com/watch?>*

`v=dQw4w9WgXcQ`

El protocolo sería 'https' (HTTP + SSL/TLS), el nombre de dominio sería youtube.com, y el endpoint sería '*watch?v=dQw4w9WgXcQ*'.

Para conectar a Youtube, el navegador primero tiene que resolver el nombre de dominio (youtube.com) en una dirección IP para poder realizar la conexión. Esta resolución se realiza mediante un protocolo denominado DNS (*Domain Name System*). Para ello, el navegador manda una petición de resolución a los servidores DNS que tengamos asignados en la configuración del sistema (o los que nos suministre nuestro DHCP). El servidor tiene una tabla de dominios con sus correspondientes direcciones IP, con lo que si el dominio se encuentra en el servidor DNS, dicho servidor responde con la dirección IP correspondiente al dominio.

Normalmente y salvo que nosotros lo modifiquemos, nuestro ISP nos asigna por defecto unos servidores DNS que pertenecen a nuestra compañía de ISP, generalmente a través de la configuración del DHCP en el router a través del cual nos conectamos.

Un bloqueo de dominio consiste simplemente en bloquear cualquier petición DNS a cualquier dirección que nuestro ISP tuviera en una lista negra. De éste modo no hay resolución de dominio y, por tanto, el acceso a la web queda inhabilitado.

Al igual que en el caso de las IPs, **es también muy sencillo saltarse éste tipo de bloqueos simplemente cambiando la dirección del DNS por cualquier otro DNS que no esté censurado** (O usando un proxy DNS). Por ejemplo, cloudflare tiene los servidores 1.1.1.1 y 1.0.0.1. Por tanto, tampoco es un método factible.

El tercer método...

Existe un tercer método para detectar intentos de acceso a páginas web censuradas y que es el que aparentemente están usando nuestros ISP en España y algunos puntos de Europa.

En principio, al comenzar una conexión, todas las conexiones son en texto plano. Esto quiere decir que **al inicio de la conexión, los datos que intercambiamos con el servidor no están encriptados**. Para encriptar los datos mediante SSL y TLS, primero debe de haber un intercambio de claves y de certificado, y un acuerdo entre el cliente y el servidor sobre qué algoritmos de cifrado van a usar durante la comunicación.

Para entendernos, el certificado es el documento que verifica que el servicio al que nos conectamos es quien dice ser, y que no nos estamos conectando a un posible tercer receptor que nada tiene que ver (Para más información, [lee éste artículo](#)). Las claves, por otro lado, se usan para cifrar la conexión (lo explico con más detalle en

éste otro artículo).

Ese intercambio y acuerdo mutuo se realiza en varios pasos. El primero de los pasos para cifrar la comunicación es el saludo inicial (**client hello**).

Durante el *client hello*, el cliente manda información al servidor con la información de cifrado, los algoritmos de cifrado que puede usar, los métodos de compresión de datos que puede usar, una serie de extensiones con información sobre la comunicación, y lo más importante en éste caso, **la información de la conexión remota, incluyendo el nombre de dominio o IP del servicio con el que el cliente está conectando.**

Si capturamos el handshake de una comunicación en SSL/TLS usando un programa de captura de paquetes, podemos ver la información del mismo:

No.	Time	Source	Destination	Protocol	Length	Info
710	9	162.159.136.6	162.159.136.6	TCP	66	61581 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 s=256 SACK_PERM=1
714	9	162.159.136.6	162.159.136.6	TCP	54	61581 → 443 [ACK] Seq=1 Ack=1 Win=263168 Len=0
715	9	162.159.136.6	162.159.136.6	TLSv1.2	571	Client Hello
717	9	162.159.136.6	162.159.136.6	TCP	54	61581 → 443 [ACK] Seq=518 Ack=1917 Win=263168 Len=0
721	9	162.159.136.6	162.159.136.6	TLSv1.2	180	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
728	9	162.159.136.6	162.159.136.6	TLSv1.2	85	Encrypted Alert
728	9	162.159.136.6	162.159.136.6	TCP	54	61581 → 443 [RST, ACK] Seq=675 Ack=2159 Win=0 Len=0


```

Extensions Length: 401
  Extension: server_name (len=21)
    Type: server_name (0)
    Length: 21
  Server Name Indication extension
    Server Name List length: 19
    Server Name Type: host_name (0)
    Server Name length: 16
    Server Name: thepiratebay.org
  > Extension: extended_master_secret (len=0)
  > Extension: renegotiation_info (len=1)
  > Extension: supported_groups (len=14)
  > Extension: ec_point_formats (len=2)
  > Extension: session_ticket (len=0)
  > Extension: application_layer_protocol_negotiation (len=14)
  > Extension: status_request (len=5)

```



```

0000 00 00 10 74 68 65 70 69 72 61 74 65 62 61 79 2e 00 00 0e
0000 5f 72 6f 00 17 00 00 ff 01 00 01 00 00 0a 00 0e
0000 00 0c 00 1d 00 17 00 18 00 19 01 00 01 01 00 00
0000 00 02 01 00 00 23 00 00 10 00 0e 00 0c 02 68 00
0000 32 08 68 74 74 70 2f 31 2e 31 00 05 01 05 01 00
0100 00 00 00 22 00 0a 00 08 04 03 05 a3 06 03 02
0110 03 00 33 00 6b 00 69 00 1d 00 20 15 a3 d2 5b 4b
0120 52 c4 33 c0 58 07 b0 9d 9e fc 62 55 55 e0 48 79
0130 fa ed 74 45 f3 24 cb 6d 94 00 17 00 41 04
0140 30 65 e5 cb 64 7c b2 44 9f 97 22 df b1 87 e1 0f
0150 2f c0 06 7c 28 74 ba 7f d5 74 bb 76 58 66 75 aa
0160 7f 5a 49 2d 63 da 1e 03 9f fe 7b 21 33 a4 9d cc
0170 3f fd 90 3f 71 73 0f 77 21 5e d1 53 9d e6 60 f7
0180 00 2b 00 05 04 03 04 03 03 00 00 18 00 16 04
0190 03 05 03 06 03 00 04 00 05 00 06 04 01 05 01 06
01a0 01 02 03 02 01 00 2d 00 02 01 01 00 1c 00 02 40
01b0 01 00 15 00 86 00 00 00 00 00 00 00 00 00 00
01c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

```

Server Name (tls.handshake.extensions_server_name), 16 byte(s)

Client Handsake con la información del servidor remoto (En éste caso, thepiratebay.org)

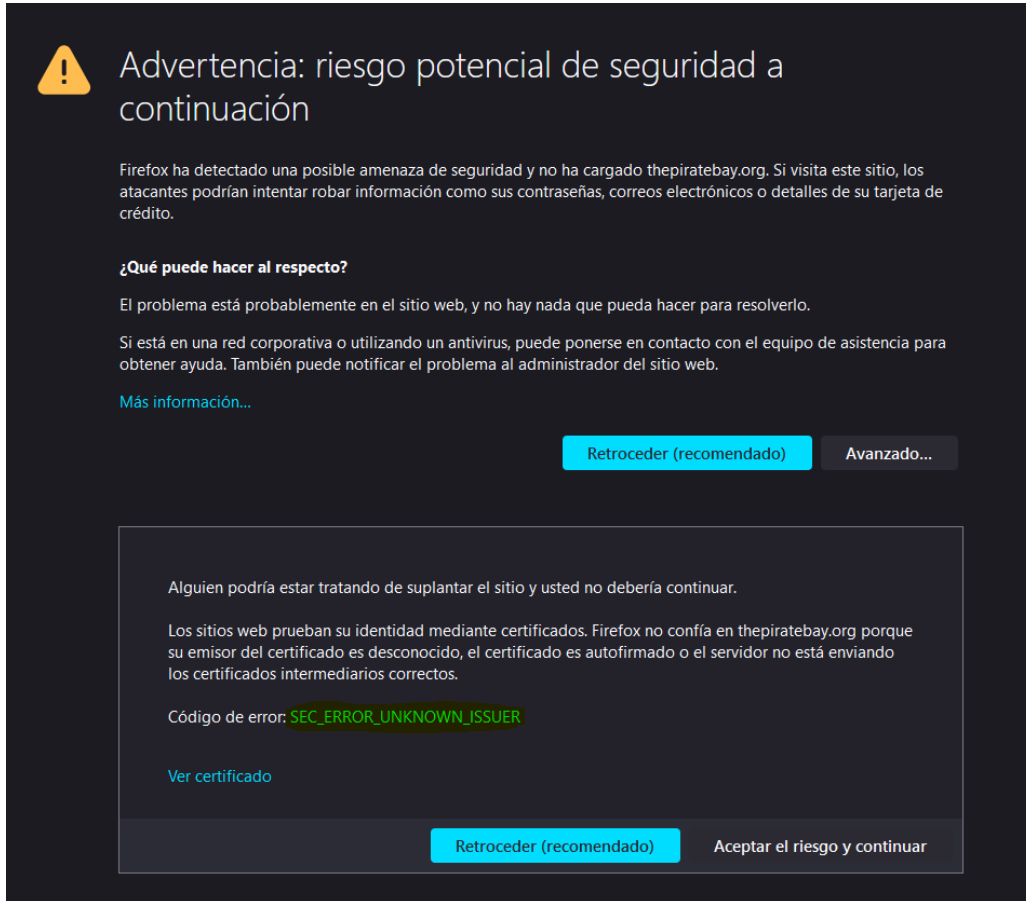
Esta información está obviamente sin encriptar todavía, ya que el proceso de cifrado de la comunicación no se ha completado aún. **Esto quiere decir que nuestro ISP puede leer la información que contienen éstos paquetes, y averiguar a qué servicio nos estamos conectando aunque no usemos sus DNS y siempre que el tráfico viaje a través de sus servidores sin encriptar.** Y lo más importante, y por éste motivo, **nuestro ISP puede saber a qué páginas nos conectamos, aunque no usemos sus DNS.**

Nuestros ISP nos estan realizando un MITM masivo.

Todo lo que he explicado hasta ahora no justifican en ningún caso un ataque. Si

acaso una flagrante violación de nuestra privacidad, al habilitar un filtro en el tráfico que les permite conocer en todo momento a qué páginas nos estamos conectando. Pero la peor parte viene ahora.

Si intentas conectarte a Pirate Bay (censurado en España y algunos países de la UE), obtendrás en tu navegador un mensaje de advertencia similar al siguiente:



The screenshot shows a dark-themed Firefox security warning dialog. At the top left is a yellow warning icon. The title is "Advertencia: riesgo potencial de seguridad a continuación". The main text states that Firefox has detected a possible security threat and that visiting theipiratebay.org could lead to information theft. It offers advice on what to do, such as checking for corporate networks or antivirus. Below this is a link for "Más información...". Two buttons are present: "Retroceder (recomendado)" in blue and "Avanzado..." in grey. A detailed error box follows, explaining that the site's identity cannot be verified because the certificate is self-signed or from an unknown issuer. It displays the error code "SEC_ERROR_UNKNOWN_ISSUER" in green. A link "Ver certificado" is provided. At the bottom of the error box are two buttons: "Retroceder (recomendado)" in blue and "Aceptar el riesgo y continuar" in grey.

Advertencia: riesgo potencial de seguridad a continuación

Firefox ha detectado una posible amenaza de seguridad y no ha cargado theipiratebay.org. Si visita este sitio, los atacantes podrían intentar robar información como sus contraseñas, correos electrónicos o detalles de su tarjeta de crédito.

¿Qué puede hacer al respecto?

El problema está probablemente en el sitio web, y no hay nada que pueda hacer para resolverlo.

Si está en una red corporativa o utilizando un antivirus, puede ponerse en contacto con el equipo de asistencia para obtener ayuda. También puede notificar el problema al administrador del sitio web.

[Más información...](#)

[Retroceder \(recomendado\)](#) [Avanzado...](#)

Alguien podría estar tratando de suplantar el sitio y usted no debería continuar.

Los sitios web prueban su identidad mediante certificados. Firefox no confía en theipiratebay.org porque su emisor del certificado es desconocido, el certificado es autofirmado o el servidor no está enviando los certificados intermediarios correctos.

Código de error: **SEC_ERROR_UNKNOWN_ISSUER**

[Ver certificado](#)

[Retroceder \(recomendado\)](#) [Aceptar el riesgo y continuar](#)

Alerta de error en el certificado SSL/TLS de Firefox

Lo más importante de éste mensaje es el error. SEC_ERROR_UNKNOWN_ISSUER. Lo que significa un error al verificar el certificado SSL (Más información:

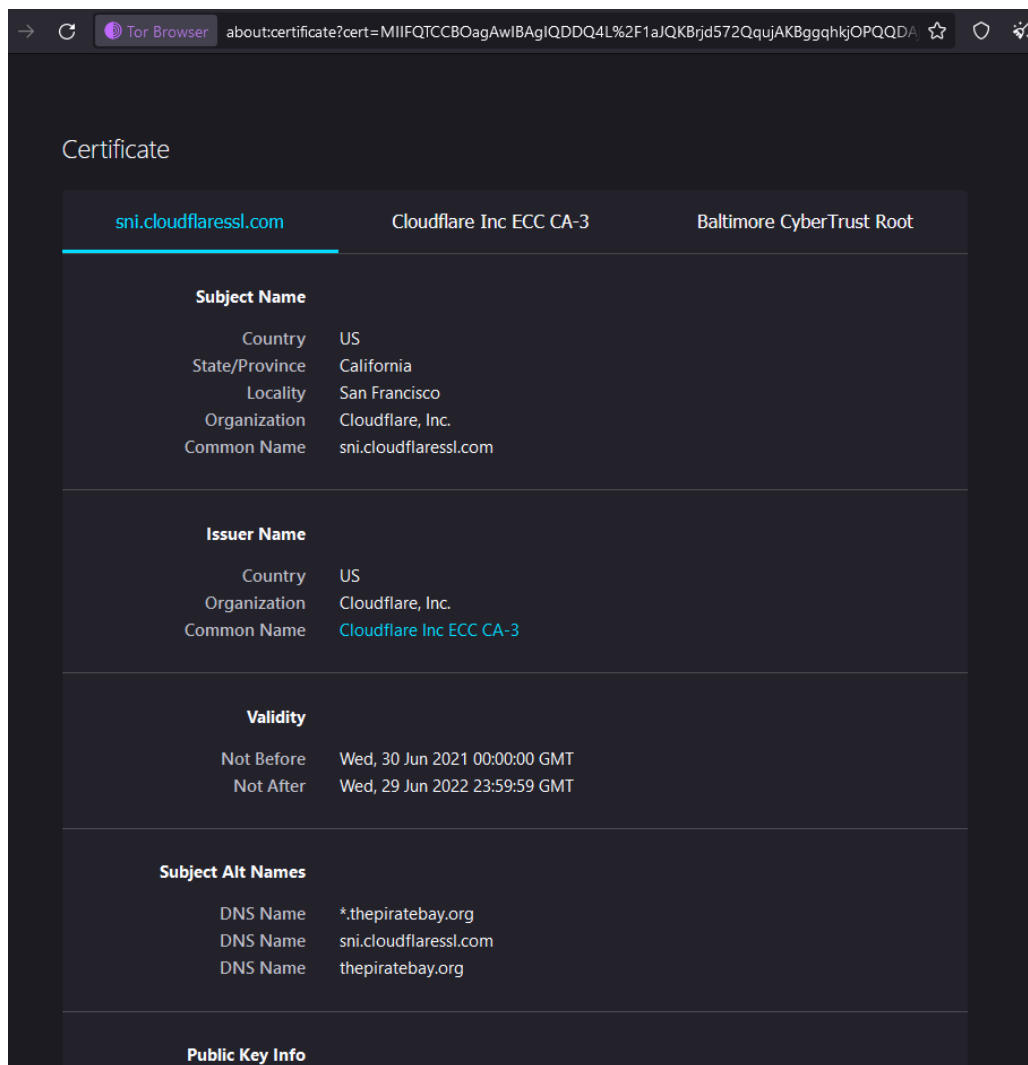
https://support.mozilla.org/es/kb/como-solucionar-el-codigo-de-error-sec_error_unknown_issuer-paginas-seguras). Este error se produce normalmente cuando alguno de los certificados en la cadena están caducados, contienen información errónea, o como en éste caso, **no pertenecen al dominio asociado**.

Al inspeccionar el certificado, **podemos comprobar que el certificado, en efecto, no pertenece a ThePirateBay y es falso**. De hecho, pertenece a una compañía de ciberseguridad llamada «Allot», y su procedencia viene en éste caso de Madrid (cuando TPB no opera en España, lógicamente).

thepiratebay.org		allot.com/emailAddress=info@allot.com	
Nombre del asunto			
Nombre común		thepiratebay.org	
Nombre del emisor			
País		ES	
Estado/Provincia		Madrid	
Localidad		Madrid	
Organización		Allot	
Unidad organizativa		Allot	
Nombre común		allot.com/emailAddress=info@allot.com	
Validez			
No antes		Fri, 16 Dec 2016 13:07:49 GMT	
No después		Wed, 16 Dec 2026 13:07:49 GMT	
Nombres alternativos del sujeto			
Nombre de la DNS		thepiratebay.org	
Información de clave pública			
Algoritmo		Elliptic Curve	
Tamaño de la clave		256	
Curva		P-256	
Valor público		04:CA:EF:CD:0A:A1:D0:1C:92:2A:B3:F4:FA:6C:83:D7:23:A6:21:13:2B:2E:17:EC:CC:D...	

Certificado falso de The Pirate Bay

El certificado original de la página lo suministra Cloudflare, con sede en San Francisco (California, US). y el certificado raíz es de Baltimore CyberTrust, no de Allot como en el caso anterior.



Certificado original

Esto sólo puede significar una cosa: **que nuestros ISP no están sólo escaneando nuestro tráfico, sino que además están inyectando tráfico de datos en nuestra conexión**. En el argót informático, se trata de un **ataque MITM** (Man in the middle) en toda regla. Siendo nuestro ISP el intermediario en éste caso, inyectando un falso certificado en nuestra comunicación sin permitir en ningún momento que éste llegue a donde le corresponde, y (Casi) sin que el usuario se entere de lo que está pasando (salvo por el mensaje de error).

Conclusión

Como ya he dicho, no pienso entrar en detalles sobre la legalidad de éstos sitios ya que no entra dentro de la temática de éste blog, ni tampoco voy a entrar en mucho detalle sobre cómo saltarse estas restricciones porque todo el mundo que entra aquí sabe usar google, y tiene la respuesta a escasos clicks (En éste blog ya hay bastante información al respecto). No obstante, me avergüenza que nuestro gobierno fuerce a las ISP a realizar éste tipo de prácticas con el fin de censurar una página web.

Por un lado, están claramente analizando nuestro tráfico, algo que ya de por sí hace saltar todas mis alarmas por ser una clara vulnerabilidad a nuestro derecho a la

privacidad y la intimidad, y que abre la puerta a otro tipo de abusos. Por otro lado, llegan tan lejos como para atacarnos, con la finalidad de proteger los bolsillos de los dueños de las discográficas y las cinematográficas, lo cuál a mi me parece muy grave independientemente de la motivación. No, señores. Así no es como funcionan las cosas.



ANTERIOR

[La memoria del ordenador, a fondo](#)

SIGUIENTE

[Juegos y aplicaciones de MS-DOS con DOSBOX \(Actualizado\)](#)

Buscar ...



Entradas Recientes

- [Estoy hasta las narices de la web moderna](#)
- [Ingeniería inversa básica con Ghidra](#)
- [Acerca de la nueva ley transgénero \(Y sobre la disforia de género\)](#)
- [Depresiones causadas por las redes sociales](#)
- [¿Necesito saber matemáticas para aprender informática?](#)
- [¿Es el fin de los discos duros tradicionales?](#)

Categorías

[Actualidad](#)[Android](#)[Básicos](#)[Ciberseguridad](#)[Clima](#)[Criptografía](#)[Electronica](#)[Emulación / Virtualización](#)[FOSS](#)[Hacking](#)[Hardware](#)[Informática](#)[Internet](#)[Juegos](#)[Opinion](#)[Otros](#)[Personal](#)[Privacidad](#)[Programación](#)[Tecnología](#)[Time Machine](#)[Tutoriales](#)

RSS

[Subscribirse al feed RSS](#)

Inicio
Catálogo
PDFs
Manuales
Política de privacidad
Política de Cookies
Acerca de mi
Acerca de ElInformati.co