

VPS

Nov 13, 2024

Deyimar A.

9min de lectura

Cómo usar el comando dig en Linux



El comando **dig**, abreviatura de “**Domain Information Groper**”, es una herramienta potente de red para consultar servidores del sistema de nombres de dominio (DNS).

dig ayuda a diagnosticar y resolver problemas relacionados con el DNS, esenciales para mantener la estabilidad y el rendimiento de la red.

Este artículo proporciona una guía completa sobre el uso del comando dig en Linux, desde su instalación y sintaxis básica hasta sus aplicaciones prácticas.

Al final sabrás cómo utilizar **dig** eficazmente para realizar búsquedas DNS, solucionar problemas de red y supervisar propagaciones.

Esta hoja de trucos hará que los comandos de Linux sean fáciles de usar

Obtener la hoja ya

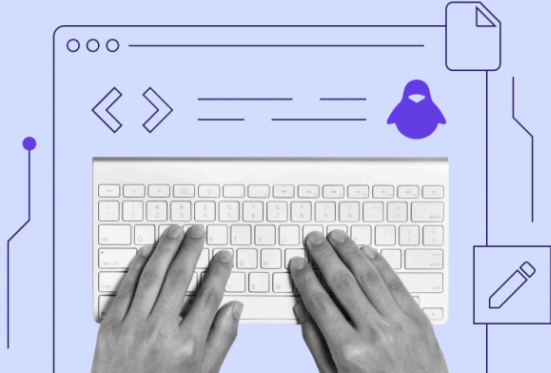


Tabla de Contenidos

- Instalar y configurar dig >
- Sintaxis del comando dig >

Opciones del comando dig >
- Cómo utilizar el comando dig >

Consultar un tipo de registro DNS específico >

Consultar un servidor DNS concreto >

Rastrear la ruta DNS >

Mostrar sólo la sección de respuestas >

Formatear la salida >

Realizar una búsqueda DNS inversa >

Ejecutar consultas por lotes >

Verificar DNSSEC >
- Usos prácticos de dig >
- Comando dig – Preguntas frecuentes >

¿Para qué sirve el comando dig? >

¿Cómo funciona el comando dig? >

¿Qué hace el comando dig? >

Los usuarios de [hosting VPS de Hostinger](#) pueden acceder a su servidor mediante SSH para instalar esta herramienta. Puedes encontrar tus credenciales de acceso navegando al **Vista general VPS → Acceso SSH**.

Vista general

🏠 - VPS - example.vps - Descripción general

Terminal del navegador

Información de VPS	Acceso a la aplicación	Panel de acceso	Acceso SSH	Detalles del plan
IP SSH	45.93.136.109			
Nombre de usuario SSH	root			
Contraseña SSH	Cambiar			
Puerto SSH predeterminado	22			
IPv6	2a02:4780:c:cf11::1			
Terminal	ssh root@45.93.136.109			

Aquí tienes los comandos para instalar **dig** en diferentes [distribuciones Linux](#), todas ellas disponibles en los planes VPS de Hostinger.

Debian y Ubuntu

```
sudo apt-get update
sudo apt-get install dnsutils
```

CentOS

```
sudo yum install bind-utils
```

Fedora

```
sudo dnf install bind-utils
```

Arch Linux

```
sudo pacman -S bind
```

Después, verifica que **dig** está instalado correctamente comprobando su versión:

```
dig -v
```

El resultado debería ser algo parecido a esto:

```
DiG 9.16.1-Ubuntu
```



Sintaxis del comando dig

La sintaxis básica del comando **dig** es la siguiente:

```
dig [server] [name] [type]
```

servidores DNS listados en `/etc/resolv.conf` si se omite.

- **[name]:** el nombre de dominio a consultar. Es el registro de recursos DNS sobre el que quieres información.
- **[type] (opcional):** el tipo de registro DNS a consultar, incluyendo A, MX y NS. **dig** consultará un registro A si no se especifica ningún tipo por defecto.

Por ejemplo, para consultar un registro A de **ejemplo.com**, puedes ejecutar:

```
dig ejemplo.com
```

Este es el resultado esperado:

```
; <<>> DiG 9.16.1-Ubuntu <<>> ejemplo.com

;; global options: +cmd

;; Got answer:

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 12345

;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 1

;; QUESTION SECTION:

ejemplo.com.      IN  A

;; ANSWER SECTION:

ejemplo.com.      3600 IN  A 93.184.216.34

;; AUTHORITY SECTION:

ejemplo.com.      3600 IN  NS ns1.ejemplo.com.
ejemplo.com.      3600 IN  NS ns2.ejemplo.com.

;; ADDITIONAL SECTION:

ns1.ejemplo.com.  3600 IN  A 192.0.2.1

;; Query time: 10 msec

;; SERVER: 192.0.2.53#53(192.0.2.53)

;; WHEN: Thu Jul 25 14:00:00 UTC 2024

;; MSG SIZE rcvd: 123
```

Opciones del comando dig

El comando **dig** ofrece varias opciones para personalizar las consultas y salidas DNS. Éstas son algunas de las más utilizadas:

- **+short:** muestra sólo la información más relevante, como la dirección IP de un registro A.
- **+noall:** suprime todas las secciones de la salida excepto las solicitadas explícitamente.
- **+answer:** muestra sólo la sección de respuesta de la salida. Suele utilizarse con **+noall**.
- **+trace:** realiza un rastreo completo del proceso de resolución DNS desde los servidores raíz hasta los servidores autoritativos.
- **@server:** especifica un servidor DNS diferente al que consultar en lugar del predeterminado.
- **-x:** realiza una búsqueda DNS inversa, traduciendo una dirección IP a un nombre de dominio.
- **+multi:** formatea la salida para que sea más legible, lo que resulta útil cuando se trabaja con múltiples registros DNS.
- **+nocmd:** omite la línea de órdenes inicial de la salida, mostrando sólo los resultados.
- **+stats:** muestra la sección de estadísticas, que incluye el tiempo de consulta y los detalles del servidor.

```
dig @8.8.8.8 ejemplo.com +short +trace
```

Cuando se ejecuta, muestra lo siguiente:

```
; <<>> DiG 9.16.1-Ubuntu <<>> @8.8.8.8 ejemplo.com +short +trace
;; global options: +cmd
.          518400 IN NS a.root-servers.net.
.          518400 IN NS b.root-servers.net.
...
ejemplo.com. 3600 IN UN 93.184.216.34
```

Cómo utilizar el comando dig

Esta sección muestra cómo utilizar el comando dig en varios escenarios de administración de red.

Consultar un tipo de registro DNS específico

Consultar un tipo de registro DNS exacto te permite obtener información concreta sobre un dominio, como su dirección IP, servidores de correo o servidores de nombres. Aquí tienes diferentes comandos **dig** para consultar tipos de registros DNS concretos:

Registro SOA

El registro de inicio de autoridad (SOA) contiene información administrativa sobre el dominio, incluido el servidor de nombres principal y el correo electrónico registrado del administrador del dominio.

```
dig ejemplo.com SOA
```

Este es el resultado que deberías ver:

```
...
;; QUESTION SECTION:
;ejemplo.com. IN SOA
;; ANSWER SECTION:
ejemplo.com. 3600 IN SOA ns1.ejemplo.com. hostmaster.ejemplo.com.
2021071601 3600 1800 1209600 300
...
```

Registro MX

El registro de intercambio de correo (MX) especifica los servidores de correo responsables de recibir correos electrónicos para el dominio, lo que es vital para configurar y solucionar problemas de los servicios de correo electrónico.

```
dig ejemplo.com MX
```

Al ejecutar el comando anterior se mostrará lo siguiente:

```
...
;; QUESTION SECTION:
;ejemplo.com. IN MX
;; ANSWER SECTION:
ejemplo.com. 3600 IN MX 10 mail.ejemplo.com.
```

...

Registro NS

El registro del servidor de nombres (NS) enumera los servidores de nombres responsables del dominio. Te ayuda a comprender la infraestructura DNS del dominio.

```
dig ejemplo.com NS
```

Este comando mostrará una salida similar a:

```
...

;; QUESTION SECTION:

;ejemplo.com.      IN  NS

;; ANSWER SECTION:

ejemplo.com.  3600  IN  NS ns1.ejemplo.com.

ejemplo.com.  3600 3600  IN  NS ns2.ejemplo.com.

;; ADDITIONAL SECTION:

ns1.ejemplo.com. 3600  IN  A 192.0.2.1

...
```

Consultar un servidor DNS concreto

Puedes utilizar **dig** para pedir información a un servidor DNS concreto en lugar de confiar en los configurados por defecto en tu sistema. Es útil para probar y comparar las respuestas de distintos servidores DNS.

Consulta al servidor DNS público de Google.com

El servidor DNS público de Google (**8.8.8.8**) se utiliza a menudo para pruebas y resolución de problemas.

```
dig @8.8.8.8 ejemplo.com
```

Este es el resultado:

```
...

;; QUESTION SECTION:

;ejemplo.com.      IN  A

;; ANSWER SECTION:

ejemplo.com.  3600  IN  A 93.184.216.34

;; AUTHORITY SECTION:

ejemplo.com.  3600  IN  NS ns1.ejemplo.com.

ejemplo.com.  3600  IN  NS ns2.ejemplo.com.

;; ADDITIONAL SECTION:

ns1.ejemplo.com. 3600  IN  A 192.0.2.1

...
```

Consulta a un servidor de nombres autoritativo

Los servidores de nombres autoritativos proporcionan la respuesta definitiva a las consultas DNS sobre

Si tus configuraciones son correctas, verás una salida similar a la anterior.

Rastrear la ruta DNS

Rastrear la ruta DNS implica seguir una consulta DNS desde tu ordenador hasta el servidor de nombres autoritativo. Este proceso te permite ver la ruta que siguen las consultas hasta el servidor DNS final.

Para rastrear la ruta DNS, añade la opción **+trace** a tu comando de la siguiente manera:

```
dig ejemplo.com +trace
```

La salida **dig** muestra los servidores DNS implicados en cada paso:

```
.                518400  IN      NS      a.root-servers.net.
.                518400  IN      NS      b.root-servers.net.

;; Received 512 bytes from 192.0.2.1#53(192.0.2.1) in 5 ms
ejemplo.com.     3600    IN      NS      ns1.ejemplo.com.
ejemplo.com.     3600    IN      NS      ns2.ejemplo.com.

;; Received 200 bytes from 192.0.2.1#53(192.0.2.1) in 10 ms
ejemplo.com.     3600    IN      A       93.184.216.34

;; Received 100 bytes from 192.0.2.2#53(192.0.2.2) in 15 ms
```

Mostrar sólo la sección de respuestas

Utilizando el comando **dig**, puedes filtrar la salida para mostrar una información más limpia y legible, al tiempo que eliminas detalles innecesarios, lo que agiliza el análisis de los resultados.

Utiliza las opciones **+noall** y **+answer** juntas en tu comando **dig**, por ejemplo:

```
dig ejemplo.com +noall +answer
```

Esto proporciona un resultado limpio y conciso que sólo muestra la dirección IP del dominio consultado:

```
ejemplo.com.    3600  IN  A  93.184.216.34
```

Formatear la salida

De forma similar a mostrar sólo la sección de respuestas, formatear la salida te permite personalizar la forma en que se muestran los resultados para hacerlos más legibles y fáciles de analizar. Aquí tienes algunos ejemplos de comandos para su uso:

Usar +short

Esta opción resume los resultados de la consulta. Por ejemplo:

```
dig ejemplo.com +short
```

Deberías ver la siguiente salida:

```
93.184.216.34
```

Usar +multi

Como su nombre indica, **+multi** muestra varios registros en un formato más legible:

```
dig ejemplo.com +multi
```

Este es el resultado:

```
ejemplo.com.    3600  IN  UN  93.184.216.34
```

```
3600 IN NS ns123.ejemplo.com.
```

Usar +nocmd

Utiliza **+nocmd** en tu comando para mostrar sólo los resultados principales:

```
dig ejemplo.com +nocmd
```

Cuando se ejecuta, aparece:

```
;; QUESTION SECTION:
;ejemplo.com. IN A

;; ANSWER SECTION:
ejemplo.com. 3600 IN A 93.184.216.34
```

Utilizar +comments

Con **+comments**, puedes mostrar u ocultar líneas de comentarios en la salida. Por ejemplo, para ocultar los comentarios, ejecuta:

```
dig ejemplo.com +nocmd +noall +answer +nocomments
```

El comando anterior mostrará:

```
ejemplo.com. 3600 IN UN 93.184.216.34
```

Realizar una búsqueda DNS inversa

Una búsqueda inversa convierte una dirección IP en un nombre de dominio, lo contrario de la búsqueda DNS directa, más habitual. Esto ayuda a verificar que la dirección IP está correctamente asignada a un nombre de dominio concreto.

Aquí tienes un ejemplo de búsqueda DNS inversa:

```
dig -x 93.184.216.34
```

Verás una salida similar a:

```
...
;; QUESTION SECTION:
;34.216.184.93.in-addr.arpa. IN PTR

;; ANSWER SECTION:
34.216.184.93.in-addr.arpa. 3600 IN PTR ejemplo.com.
...
```

Ten en cuenta que si no se define un [registro PTR](#) para una dirección IP, no es posible realizar una búsqueda DNS inversa, ya que el registro PTR apunta al dominio o nombre de host.

Ejecutar consultas por lotes

También puedes utilizar **dig** para ejecutar varias búsquedas DNS en un solo comando. Ayuda a consultar información sobre varios nombres de dominio o direcciones IP, ahorrando tiempo y simplificando el proceso.

Para ejecutar consultas por lotes, sigue estos pasos:

1. Crea un archivo llamado **dominios.txt** o con el nombre que prefieras utilizando el [editor de texto nano](#):

```
nano dominios.txt
```

2. Añade las direcciones IP o los dominios que quieras consultar, uno por línea:

```
ejemplo3.com
```

- 3. Guarda tus modificaciones y sal de **nano** pulsando **Ctrl + X → Y → Intro**.
- 4. Ejecuta **dig** con la opción **-f** seguida del nombre de tu archivo:

```
dig -f dominios.txt
```

Cuando se ejecuta, el comando muestra:

```
...

;; QUESTION SECTION:

;ejemplo1.com.    IN  A

;; ANSWER SECTION:

ejemplo1.com.    3600  IN  A 93.184.216.34

;; AUTHORITY SECTION:

ejemplo1.com.    3600  IN  NS ns1.ejemplo1.com.
ejemplo1.com.    3600  IN  NS ns2.ejemplo1.com.

;; ADDITIONAL SECTION:

ns1.ejemplo1.com. 3600  IN  A 192.0.2.1

...

;; QUESTION SECTION:

;ejemplo2.com.    IN  A

;; ANSWER SECTION:

ejemplo2.com.    3600  IN  A 93.184.216.35

;; AUTHORITY SECTION:

ejemplo2.com.    3600  IN  NS ns1.ejemplo2.com.
ejemplo2.com.    3600  IN  NS ns2.ejemplo2.com.

;; ADDITIONAL SECTION:

ns1.ejemplo2.com. 3600  IN  A 192.0.2.2

...

;; QUESTION SECTION:

;ejemplo3.com.    IN  A

;; ANSWER SECTION:

ejemplo3.com.    3600  IN  A 93.184.216.36

;; AUTHORITY SECTION:

ejemplo3.com.    3600  IN  NS ns1.ejemplo3.com.
ejemplo3.com.    3600  IN  NS ns2.ejemplo3.com.

;; ADDITIONAL SECTION:

ns1.ejemplo3.com. 3600  IN  A 192.0.2.3
```


búsqueda DNS. Garantiza que las respuestas son auténticas y no han sido manipuladas. Verificar DNSSEC ayuda a protegerse contra los ataques de suplantación de DNS.

Para verificar DNSSEC con el comando **dig**, añade la opción **+dnssec**:

```
dig ejemplo.com +dnssec
```

La salida incluye registros RRSIG en las secciones **ANSWER** y **AUTHORITY**:

```
...

;; QUESTION SECTION:
;ejemplo.com.      IN  A

;; ANSWER SECTION:
ejemplo.com.      3600 IN  A  93.184.216.34
ejemplo.com.      3600 IN  RRSIG A 13 2 3600 (
20240301000000 20240215000000 12345 ejemplo.com.
hT+pV8JZfCh3U0jP4xB1C2YJmtD5efcd )

;; AUTHORITY SECTION:
ejemplo.com.      3600 IN  NS  ns1.ejemplo.com.
ejemplo.com.      3600 IN  NS  ns2.ejemplo.com.
ejemplo.com.      3600 IN  RRSIG NS 13 2 3600 (
20240301000000 20240215000000 12345 ejemplo.com.
kd9K8vNlF8cD/B8ejq8G8C9Zp7L )

;; ADDITIONAL SECTION:
ns1.ejemplo.com.  3600 IN  A  192.0.2.1
ns1.ejemplo.com.  3600 IN  RRSIG A 13 2 3600 (
20240301000000 20240215000000 12345 ejemplo.com.
y6R/B9e1K5dQ/L5gRk9F400aP8g )

...
```

Usos prácticos de dig

Una vez que hayas aprendido lo básico, es hora de explorar algunas aplicaciones prácticas del comando **dig**.

Solución de problemas de DNS

Utilizar el comando **dig** para diagnosticar problemas de DNS te ayuda a identificar y resolver eficazmente los problemas de la red. A continuación se indican los pasos generales para solucionar problemas de DNS con este comando:

1. Comprueba la resolución DNS verificando si un nombre de dominio se resuelve correctamente:

```
dig ejemplo.com
```

2. Asegúrate de que los servidores de nombres del dominio están correctamente configurados:

```
dig ejemplo.com NS
```

3. Identifica dónde puede estar fallando la resolución DNS rastreando toda la ruta de búsqueda DNS:

```
dig ejemplo.com +dnssec
```

5. Asegúrate de que una dirección IP se resuelve con el nombre de dominio correcto:

```
dig -x 93.184.216.34
```

6. Para arreglar servicios específicos como el correo electrónico, comprueba los registros DNS correspondientes. Por ejemplo:

```
dig ejemplo.com MX
```

Presta atención a cada salida y asegúrate de que las secciones de **ANSWER** son correctas.

Monitorización de la propagación DNS

Supervisar la propagación DNS implica comprobar el estado de los cambios DNS en diferentes servidores. Garantiza que las actualizaciones de los registros DNS se han propagado correctamente por toda la web.

Sigue estas instrucciones para verificar la propagación del DNS:

- 1. Utiliza la opción **@server** para consultar un servidor DNS concreto, como el servidor DNS público de Google:

```
dig @8.8.8.8 ejemplo.com
```

- 2. Consulta diferentes servidores DNS para comparar sus respuestas. Para el servidor de Cloudflare, ejecuta:

```
dig @1.1.1.1 ejemplo.com
```

Si las secciones **ANSWER** de los distintos servidores coinciden, los cambios DNS se han propagado correctamente.

En caso contrario, es posible que algunos servidores aún tengan que actualizar sus registros. Puedes comprobar periódicamente el estado de propagación.

Pruebas de rendimiento

Medir los tiempos de respuesta DNS es esencial para evaluar el rendimiento de tus servidores DNS. Esto te permite identificar ralentizaciones o problemas que afectan a la velocidad y fiabilidad de tu red.

He aquí cómo medir los tiempos de respuesta DNS:

- 1. Ejecuta el comando básico **dig**. Fíjate en el campo **Query time**, que indica el tiempo que se tarda en obtener una respuesta del servidor DNS:

```
dig ejemplo.com
```

- 2. Consulta diferentes servidores DNS para comparar sus tiempos de respuesta. Esto ayuda a identificar qué servidores funcionan mejor:

```
dig @8.8.8.8 ejemplo.com
dig @1.1.1.1 ejemplo.com
```

- 3. Utiliza la opción **+stats** para obtener estadísticas adicionales sobre los tiempos de consulta y los detalles del servidor:

```
dig ejemplo.com +stats
```

Conclusión

En este artículo hemos tratado los usos esenciales del comando **dig** de Linux, desde las búsquedas DNS fundamentales hasta las consultas más avanzadas y los métodos de resolución de problemas. Además, dominar **dig** puede mejorar tus habilidades de gestión de red.

Practica los ejemplos de comandos de esta guía para sacar el máximo partido a **dig**. Experimentar con distintas opciones te permite comprender mejor el funcionamiento interno del DNS y optimizar el

continuación.

Aprende más sobre comandos y procesos Linux

- [Comando Sudo y archivo Sudoers](#)
- [Comando Kill](#)
- [Comando Ping](#)
- [Cómo administrar procesos en Linux](#)
- [Cómo listar servicios en Linux](#)
- [Cómo cambiar las contraseñas de usuario en Linux](#)

Comando dig – Preguntas frecuentes

Esperamos que esta guía te haya sido de utilidad. Si tienes algún comentario o pregunta, escríbela en la sección de abajo. ¡Buena suerte!

¿Para qué sirve el comando dig?

El comando **dig** se utiliza para consultar servidores de nombres DNS. Recupera información DNS sobre numerosos registros, como A, MX y NS, lo que ayuda a diagnosticar y resolver problemas relacionados con la red.

¿Cómo funciona el comando dig?

El comando dig funciona enviando una consulta DNS al servidor especificado. A continuación, muestra la respuesta, que incluye información sobre los registros DNS del dominio consultado, lo que permite a los administradores de red solucionar los problemas.

¿Qué hace el comando dig?

El comando de Linux dig se utiliza habitualmente para realizar búsquedas DNS, consultar tipos de registro específicos, rastrear rutas de resolución DNS, verificar DNSSEC y solucionar problemas de propagación y resolución.

EL AUTOR

Deyimar A.

Deyi es una entusiasta del marketing digital, con experiencia en diseño de páginas web, creación de contenido, copywrite y SEO. Forma parte del equipo de SEO & Localization de Hostinger. En su tiempo libre, le gusta desarrollar proyectos, leer un libro o ver una buena película.

Más de Deyimar A.



Tutoriales relacionados

26 Dec • [VPS](#)

[Cómo instalar LAMP en Ubuntu de forma automática y manual](#)

LAMP es un acrónimo para Linux, Apache, MySQL y PHP, un stack popular para crear y desplegar aplicaciones web dinámicas. En este stack, Linux sirve...

[Por Luis Jordán](#)

19 Dec • [VPS](#)

[¿Qué es GitLab? Principales funciones y casos de uso](#)

Muchos dueños de empresas digitales confían en DevOps para mejorar la productividad mediante la automatización y la colaboración. Estos...

[Por Diego Vargas](#)

12 Dec • [VPS](#)

Cómo instalar OpenCart para tu negocio online: 2 métodos sencillos

La plataforma de comercio electrónico de código abierto OpenCart proporciona herramientas y funciones preconstruidas para crear una tienda online...

Por Diego Vargas

Lo que dicen nuestros clientes

Excelente



En base a 37.793 opiniones



Deja una respuesta

Comentar*

Nombre*

Email*

☐ Al utilizar este formulario, aceptas que tus datos personales serán procesados de acuerdo con nuestra [Política de privacidad](#).

Enviar



Somos un proveedor de hosting web con la misión de llevar el éxito a todos los que están en Internet. Lo hacemos mejorando constantemente la tecnología del servidor, brindando soporte profesional y haciendo que la experiencia de hosting web sea perfecta.



HOSTING

- [Hosting web](#)
- [Hosting para profesionales](#)
- [VPS Hosting](#)
- [Hosting Minecraft](#)
- [CyberPanel](#)
- [Cloud hosting](#)
- [Hosting para WordPress](#)
- [Correo corporativo](#)
- [Hosting CMS](#)
- [Hosting eCommerce](#)
- [Tienda online](#)
- [Creador de páginas web](#)
- [Creador de logos](#)
- [Generador de nombres para empresas](#)

DOMINIOS

- [Comprar dominio](#)
- [Transferir dominio](#)
- [Dominio gratis](#)
- [Dominio .xyz](#)
- [Dominios baratos](#)
- [Extensiones de Dominio](#)
- [WHOIS](#)
- [Certificado SSL gratis](#)

AYUDA

- [Tutoriales](#)
- [Base de Conocimientos](#)
- [Reportar abuso](#)

INFORMACIÓN

- [Migrar a Hostinger](#)
- [Estado del sistema](#)
- [Programa de afiliados](#)
- [Formas de pago](#)
- [Muro de la fama](#)
- [Opiniones](#)
- [Precios](#)
- [Mapa del sitio](#)

[Tecnología](#)

[Mapa del sitio \(inglés\).](#)

[Contáctanos](#)

[Blog](#)

LEGAL

[Política de privacidad](#)

[Términos de servicio](#)



© 2004-2025 hostinger.es - Servicios de Hosting Web Premium, Cloud, VPS & Registro de Dominios.

Los precios no incluyen IVA