

 Tomás Sierra

¿El Mantenimiento es importante?

 @Tomycant

WORDCAMP ZARAGOZA
Enero 2018

www.tomassierra.com
[@Tomycant](https://twitter.com/Tomycant)



¿Qué buscan nuestros clientes?

¿Qué buscan nuestros clientes?

1. Web económica



¿Qué buscan nuestros clientes?

2. Web económica



¿Qué buscan nuestros clientes?

3. Web económica



¿Qué buscan nuestros clientes?

(2)

Que no de dolores de cabeza

- Hosting “el más baratito”
- Dominio
- Creación, puesta en marcha y desarrollo
- Diseño: “Que sea como la de...”

¿Qué buscan nuestros clientes?

(3)

Rápida

¿Qué buscan nuestros clientes?

Y sobre todo...

Una web “sencillita”



@TomyCant // #WCZGZ

Y a nosotros nos toca...



Y ahora que sabemos lo que
“quiere”...

¿Cómo le hablamos del mantenimiento?

Y ahora que sabemos lo que “quiere”...

¿Cómo le hablamos del mantenimiento?

¿Mantenimiento? ¿y eso qué es? y ¿para qué?

A tener en cuenta

El cliente no entiende de seguridad

A tener en cuenta

El cliente no entiende de seguridad

Podemos ponerle:

- Ejemplos de hackeos actuales y sus consecuencias

A tener en cuenta

El cliente no entiende de seguridad

Podemos ponerle:

- Ejemplos de hackeos actuales y sus consecuencias
- Ransomware

A tener en cuenta

El cliente no entiende de seguridad

Podemos ponerle:

- Ejemplos de hackeos actuales y sus consecuencias
- Ransomware
- Temas de actualidad
 - Ataques de fuerza bruta a WordPress

¿Y por qué me van a atacar a mi?

¿Y por qué me van a atacar a mi?

Los ataques generalmente no van dirigidos a tí sino a tu CMS

¿Y para qué?

Enviar spam

Utilizar tu web como parte de una botnet

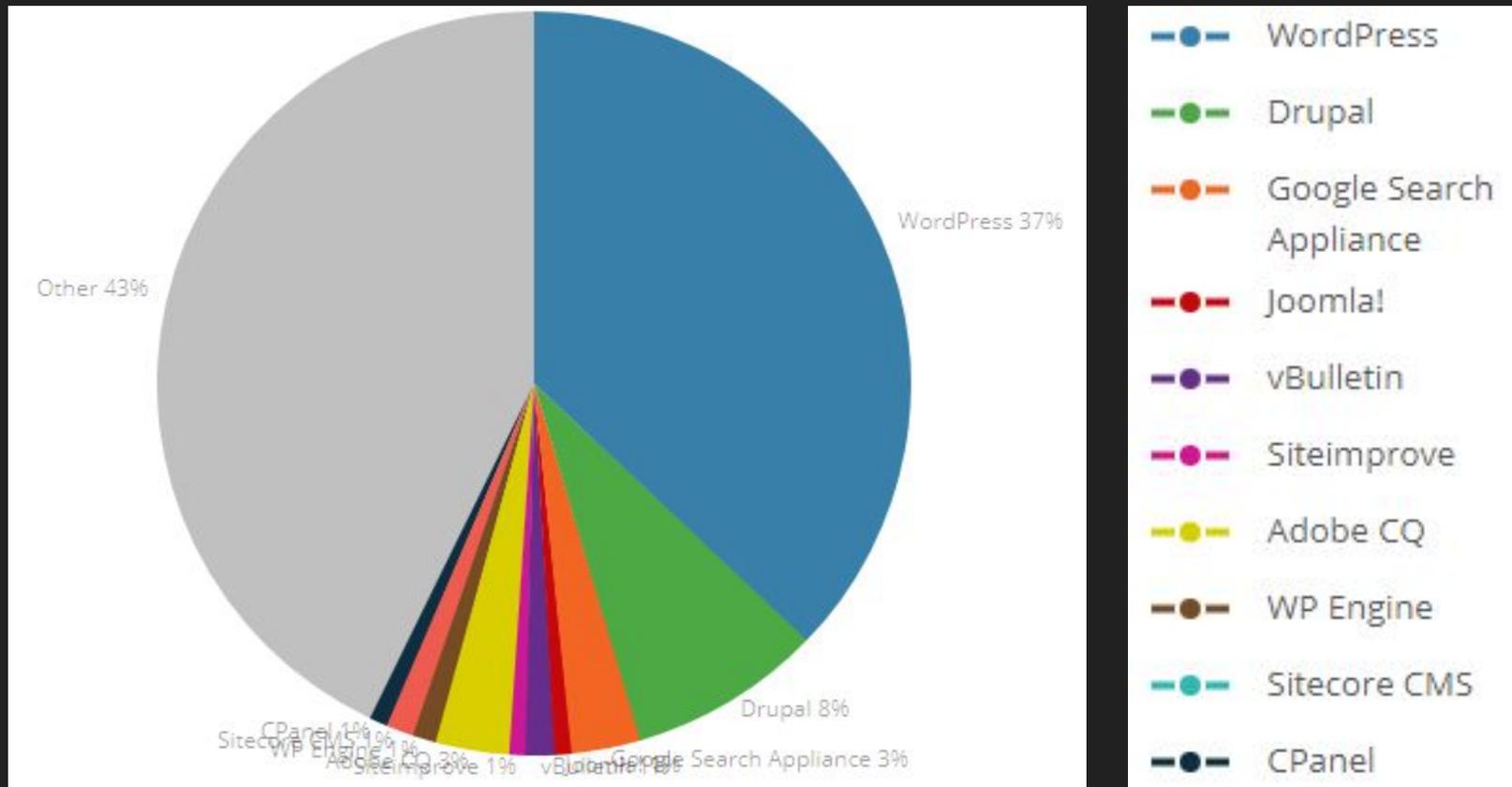
Minar Bitcoins

...

Algo de estadística sobre WordPress

WordPress en el mundo

Más del **37%** de las webs están hechas con WordPress



WordPress en España

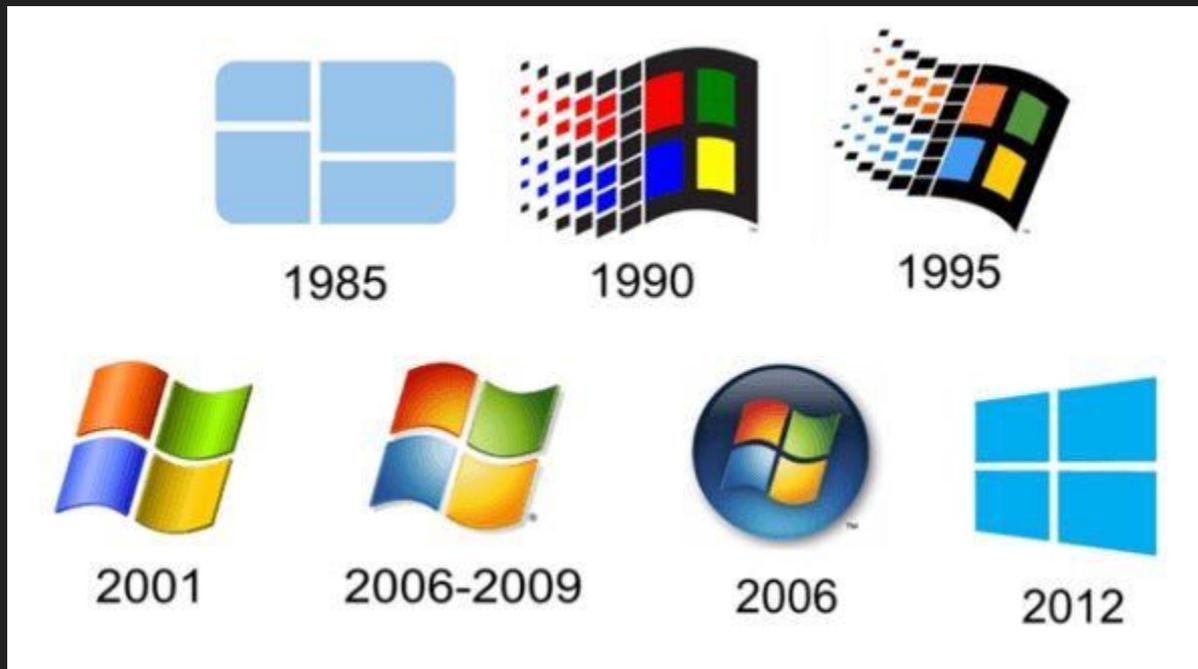
Más del **65%** de las webs en España están creadas con WordPress

(Datos de builtwith.com)



¿Algo de historia?

¿Por qué es necesario el mantenimiento en WordPress?



Servidor elegido

¿Tu servidor pone medidas de seguridad adecuadas?

¿Hackeos?

Vulnerabilidades

- Plugins
- Plantillas de temas
- Core

<https://wpvulndb.com/>

¿Hackeos?

Exploits

<https://www.exploit-db.com>

Recogida de datos

WPScan

Recogida de datos

```
Aplicaciones Lugares > dom 25 de oct, 18:19 root
root@kali: ~
Archivo Editar Ver Buscar Terminal Ayuda

  W P S S C A N
WordPress Security Scanner by the WPScan Team
Version 2.8
Sponsored by Sucuri - https://sucuri.net
@_WPScan_, @ethicalhack3r, @erwan_lr, pvd1, @_FireFart_

[+] URL: http://carlos-sanchez.es/
[+] Started: Sun Oct 25 18:19:08 2015

[+] robots.txt available under: 'http://carlos-sanchez.es/robots.txt'
[+] Interesting header: CF-RAY: 23af95c43be025ec-MRS
[+] Interesting header: SERVER: cloudflare-nginx
[+] Interesting header: X-POWERED-BY: W3 Total Cache/0.9.4.1

[+] WordPress version 4.3.1 identified from meta generator

[+] WordPress theme in use: Avada-Child-Theme

[+] Name: Avada-Child-Theme
| Location: http://carlos-sanchez.es/contenido/themes/Avada-Child-Theme/
```

Recogida de datos

WPDanger

www.wpdanger.com

Recogida de datos

 WPdanger

[User](#) [Language](#) ▾

WordPress security analysis, for free

WordPress URL

WordPress site (with [http://] or [https://]).

Mail

We will send you a notification when we are done.

[Analyze WordPress](#)

Developed with ❤️ by [Javier Casares](#).
Technology based on [WPScan](#).
Thanks to [WordPress Barcelona](#).

Recogida de datos

WPDoctor (www.wpdoctor.es)

Recogida de datos

WordPress (91 / 100)	
Theme	
i Nombre	Theme Name: Jupiter
i Descripción	A Beautiful, Professional and Ultimate Wordpress Theme Made by Artbees. Jupiter is a Clean, Flexible, fully responsive and retina ready Wordpress theme. Its smart and hand crafted environment allows you to Build outstanding websites easy and fast.
i Versión	5.9.7
i Autor	Artbees
i URL	http://demos.artbees.net/jupiter5
i Licencia	http://www.gnu.org/licenses/gpl-2.0.html
✓ Versión HTML	HTML5
✓ Diseño adaptable	Sí Más info
i Uso de CDN	NO
i Style.css	http://josefacchin.com/wp-content/themes/jupiter/style.css
i Path	wp-content/themes/jupiter/
i Metas HTTP Equiv	<ul style="list-style-type: none">X-UA-Compatible: IE=edge,chrome=1 Más info

Recogida de datos

Wappalizer (complemento Firefox)

Recogida de datos

Google Dorks

Recogida de datos

Google Dorks

`inurl:"/wp-content/plugins/wp-shopping-cart/"`

`inurl:/wp-content/uploads/ filetype:sql`

`/wp-content/themes/SMWF/inc/download.php?file=../wp-config.php`

`/wp-content/themes/markant/download.php?file=../../wp-config.php`

`/wp-content/themes/yakimabait/download.php?file=../wp-config.php`

Administrar WordPress



INFINITEWP



 CMS Commander

WPREMOTE

Tomás Sierra

Muchas gracias

 @TomyCant

tomassierra.com
@Tomycant

