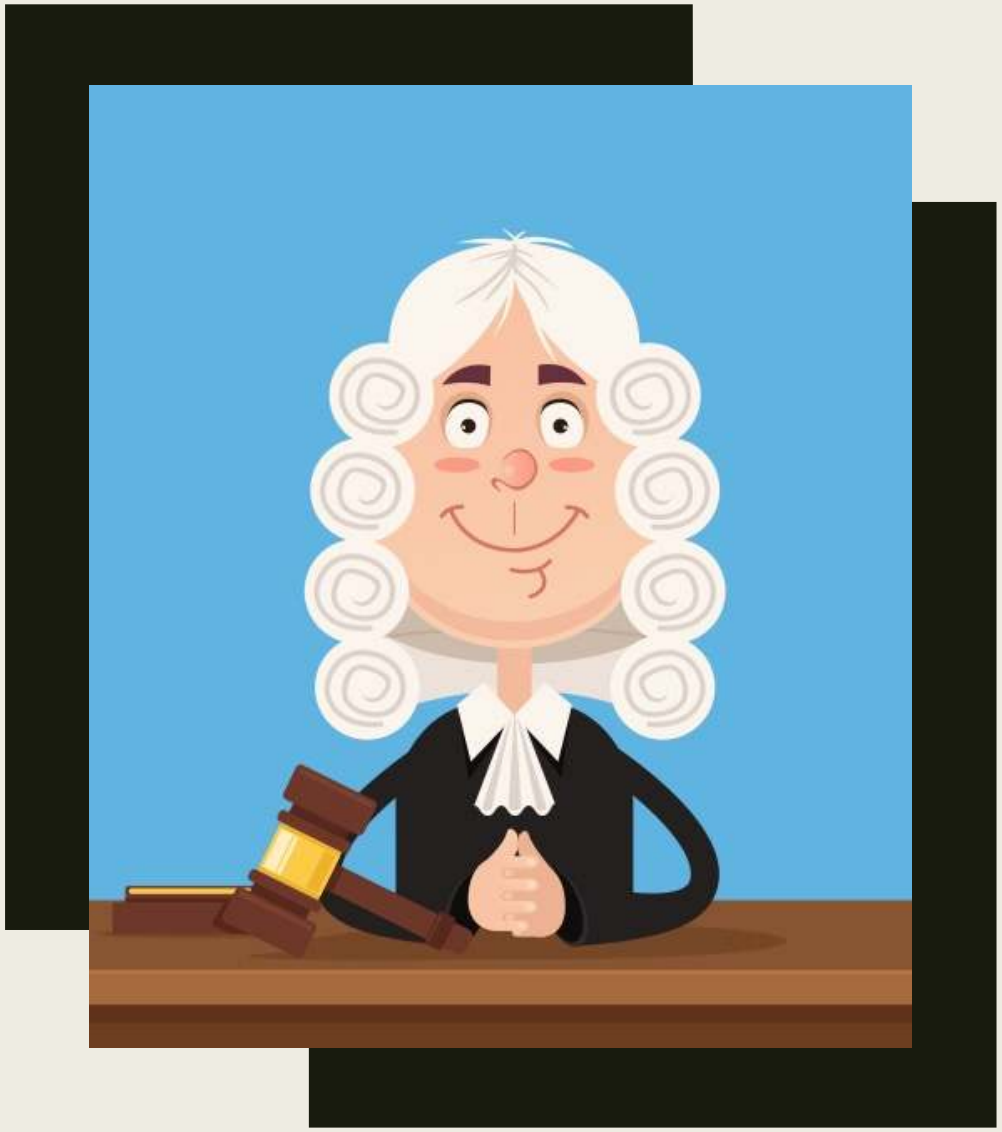
PERO ENTONCES... ¿ES WORDPRESS SEGURO O NO?

Por Néstor Angulo de Ugarte

WordCamp ONLINE ES_

OKAERI!
Irasshai!



ABOGADO DEFENSOR Y FISCAL DEL CASO

Néstor Angulo de Ugarte

@pharar

- Un chico muy curioso
  ... a veces más que un gato.
- Ingeniero informático y consultor tecnológico

- Desde 2015:
  Analista de Seguridad @ **Sucuri**
- Desde 2017:
  Advance Technical Support
  Managed SSL Analyst
  Developer in the WSS backend team
  @ **GoDaddy Security**
- En 2019:
  Interim Head of IT @ **GoDaddy Spain**

Sobre

- Sucuri: **Anaconda**
  (No Securi / Security)
- **Website security**
- Fully remote (> 25 paises)
- 2008: **Fundación**
- 2017: Entra en la familia **GoDaddy**
- **Free scanners:**
  - *Sitecheck (sitecheck.sucuri.net)*
  - *Performance (performance.sucuri.net)*

EL ACUSADO

¿ES WORDPRESS SEGURO O NO?

Vista del 7 de Mayo de 2020

ANTES DE NADA, ENCUESTA AL JURADO

(¡Todos ustedes!)

SCAN ME

kahoot.it

FACTORES DE SEGURIDAD

¿Qué significa que un CMS es ”Seguro”?

Información y contenido protegido

No comparte con terceros

Es difícil penetrar y establece conexion segura

Gestión adecuada de permisos y jerarquías

Mantenimiento activo y frecuente

Soporte efectivo y rápido

La Cadena de Confianza

A más puertas y ventanas (plugins, temas, etc.), más difícil defender tu fortaleza

¿Confías en tus distribuidores? ¿Cuánto confías?

La confianza es nuestro punto más débil: delegas la responsabilidad en un tercero

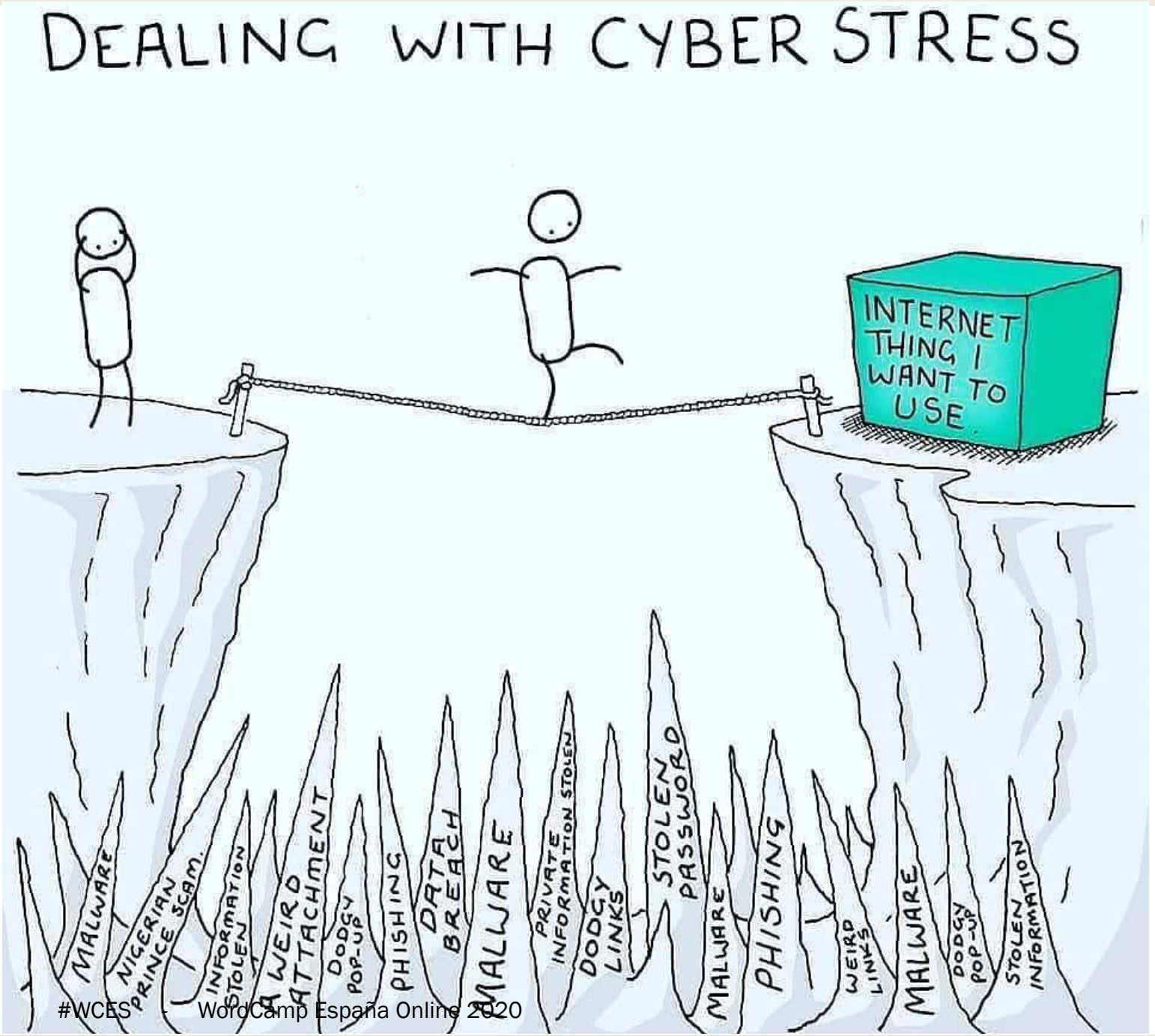
Es necesaria

Seguridad: Modelo por capas simplificado

Capa	Protección
Tú, la capa más débil	Conocimiento
Tu **dispositivo**	Antivirus
Tu **conexión**	SSL
Tu **sitio web**	WAF
Tus **credenciales**	Contraseñas fuertes, 2FA
La seguridad de **tu sitio**	monitor, plugins, updates
La seguridad **del server**	monitor, sysadmin, updates
La **base de datos**	monitor, sysadmin
Tareas de mantenimiento	

HECHOS


There are two types of companies: those who have been hacked, and those who don't yet know they have been hacked.
John Chambers
Chief Executive Officer of Cisco


DEALING WITH CYBER STRESS
INTERNET THING I WANT TO USE
MALWARE
NIGERIAN PRINCE SCAM.
INFORMATION STOLEN
WEIRD ATTACHMENT
DODGY POP-UP
PHISHING
DATA BREACH
MALWARE
PRIVATE INFORMATION STOLEN
DODGY LINKS
STOLEN PASSWORD
MALWARE
PHISHING
WEIRD LINKS
MALWARE
DODGY POP-UP
STOLEN INFORMATION

Hechos

Un hackeo prácticamente **nunca es orientado** a un cliente

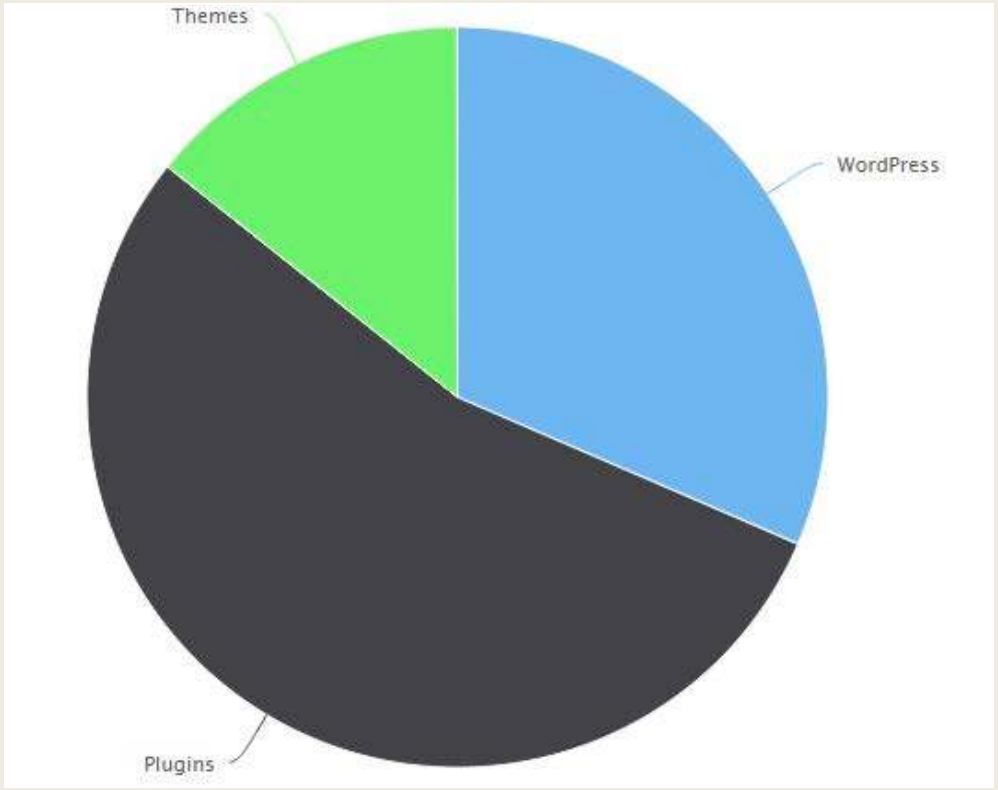
Casi siempre ocurre debido a un **control y mantenimiento deficientes**

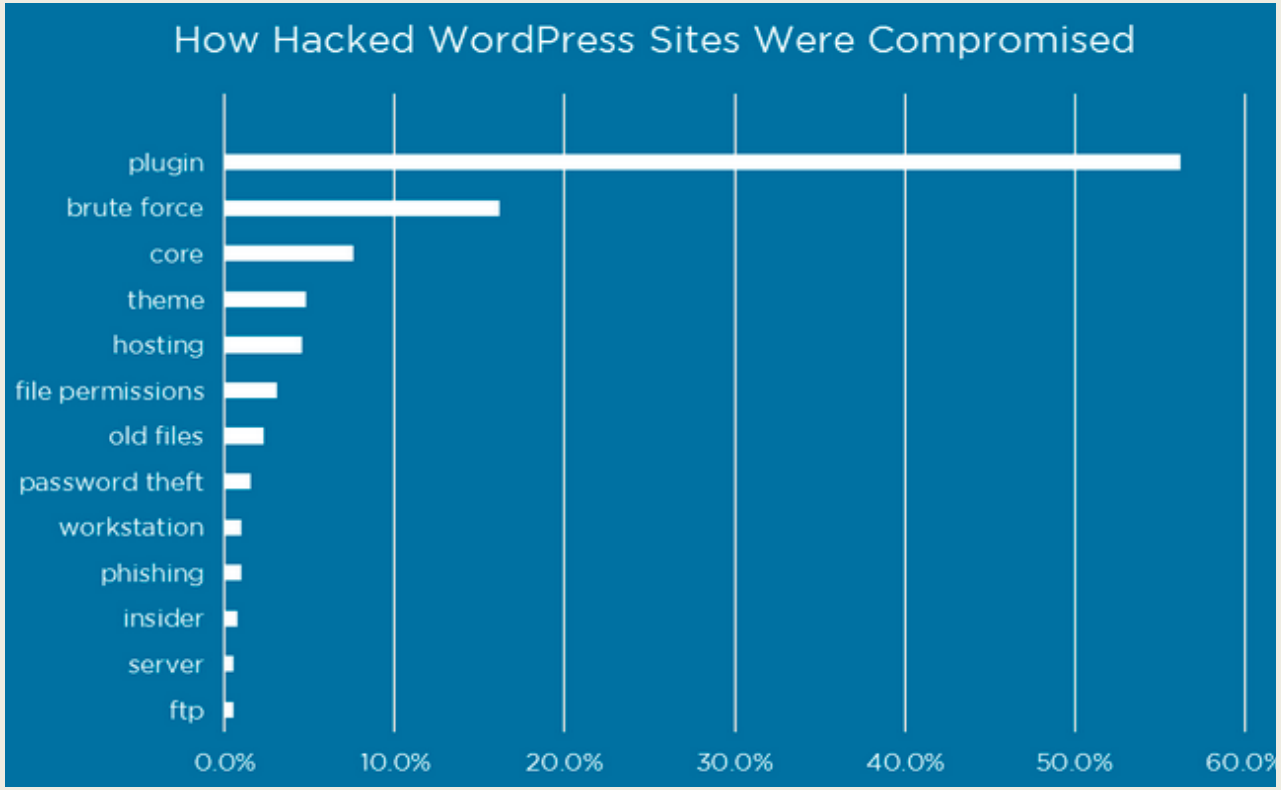
Un certificado **SSL no es un escudo** anti-hacking

Los parches de seguridad aparecen normalmente **después** de descubrir exploits

Errare Humanum Est

La Seguridad **nunca** garantiza (ni lo hará) un **100% de efectividad**





Factores de seguridad: Cadena de confianza

- Plugins y temas
- Código y contenido embebido
- Gravatar, Google Fonts, emojis, etc.
- Analytics, Firewall, CDN, Hosting. Etc.

Plugin Name	Installations
Easy WP SMTP	400,000
Wp File Manager	500,000
Freemius Library (Multiple plugins are affected)	200,000
Newspaper and other old tagDiv Themes	100,000
WordPress GDPR Compliance	100,000
Social Warfare	70,000
WP Live Chat Support	60,000
Yuzo Related Post	60,000
WP-Piwik	60,000
Sticky Menu on Scroll, Sticky Header for Any Theme	60,000

Factores de seguridad: Mantenimiento y soporte

- El **mantenimiento** de WordPress es **frecuente** y tiene roadmap
- **Código abierto**, así que cualquiera puede proponer mejoras o arreglar bugs (millones de potenciales programadores). Modelo Bazar.

- El **soporte lo da la comunidad** WordPress, funciona como un **foro** y es **multiidioma**
- Es una de las comunidades tecnológicas más grandes del mundo
- En algunas comunidades, como la Española, las preguntas quedan respondidas en el mismo día

Factores de seguridad: Jerarquía, permisos y conexión segura

WordPress tiene sistema de roles y control de acceso.

Es ampliable por plugin

Funciona correctamente a traves de HTTPS

No fuerza HTTPS por defecto ni se puede configurar fácilmente, se necesita un plugin o/y cambios a mano para forzarlo.

Factores de seguridad: Información, privacidad y cesión a terceros

La información sensible se asegura por defecto.

No cede información a terceros.

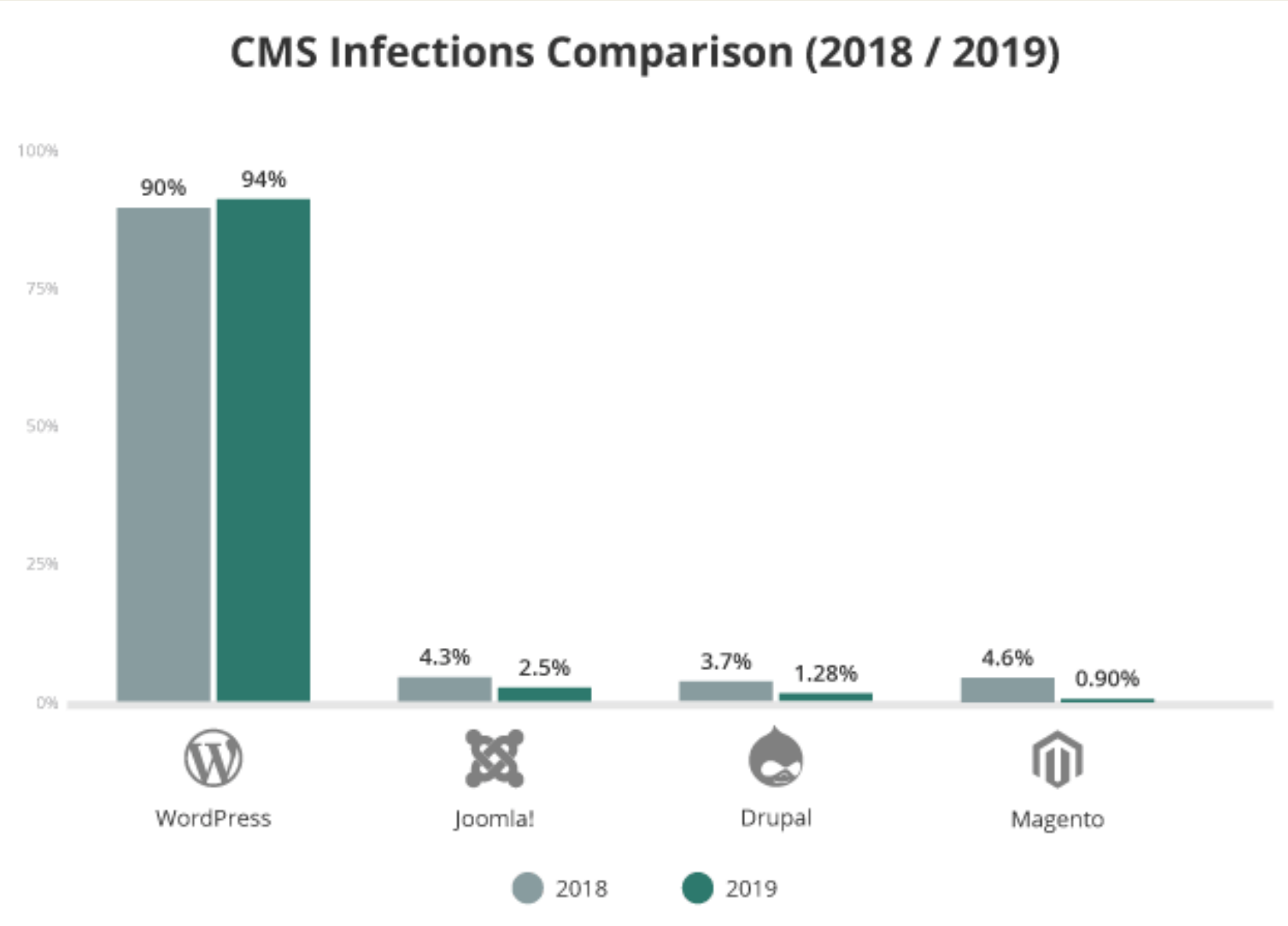
No se fuerza el uso de contraseñas Fuertes ni 2FA por defecto

”Out of the box” no protege la privacidad de manera muy estricta:

Gravatar, emojis, WordPress, contenido embebido, etc.

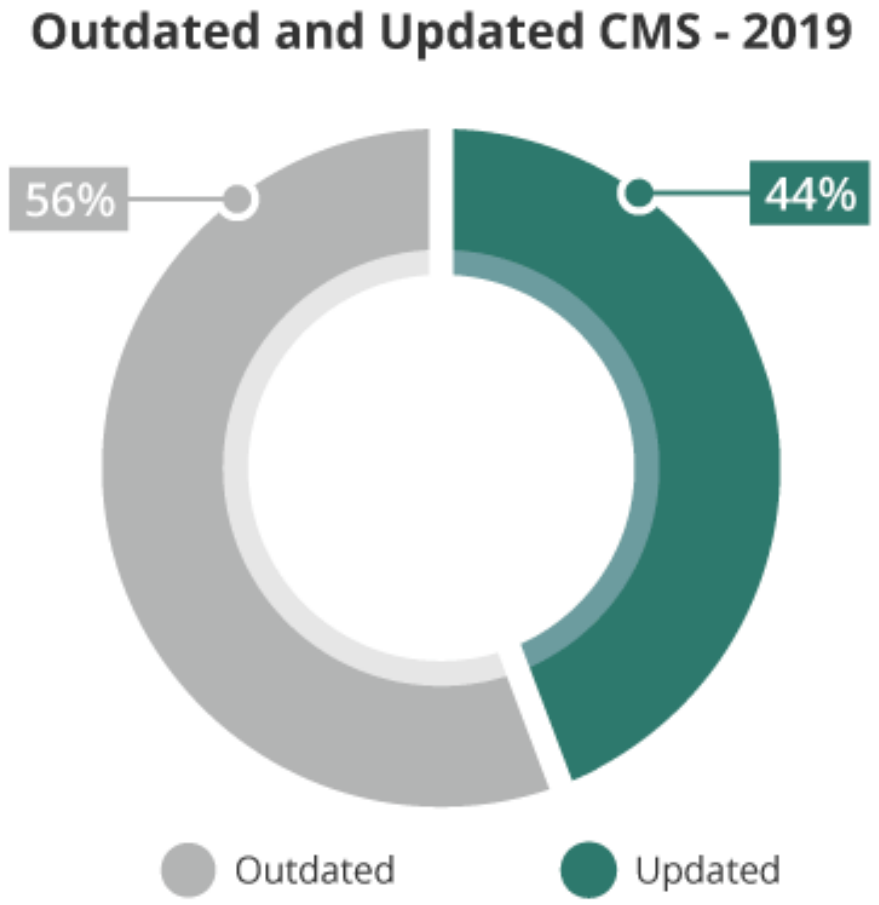
No proporciona soporte nativo GDPR, aviso de cookies, CCPA, etc.

”Out of the box” no posee ningún procedimiento de copia de seguridad o auditoria

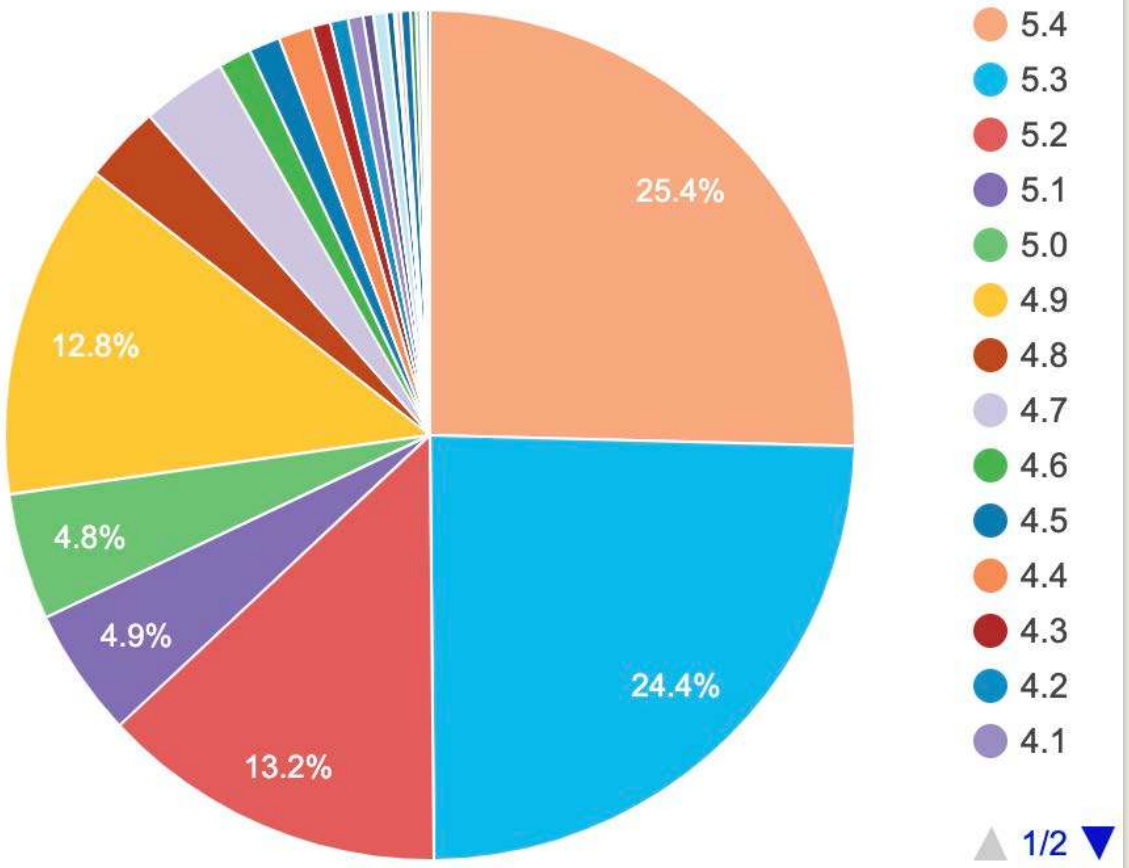


Fuente:
Website Website Threat Research Report 2019 – sucuri.net

- **… Y 1 de cada 3 sitios webs en Internet utiliza WordPress**
- O 2 de cada 3 si hablamos de los sitios web que usan un CMS

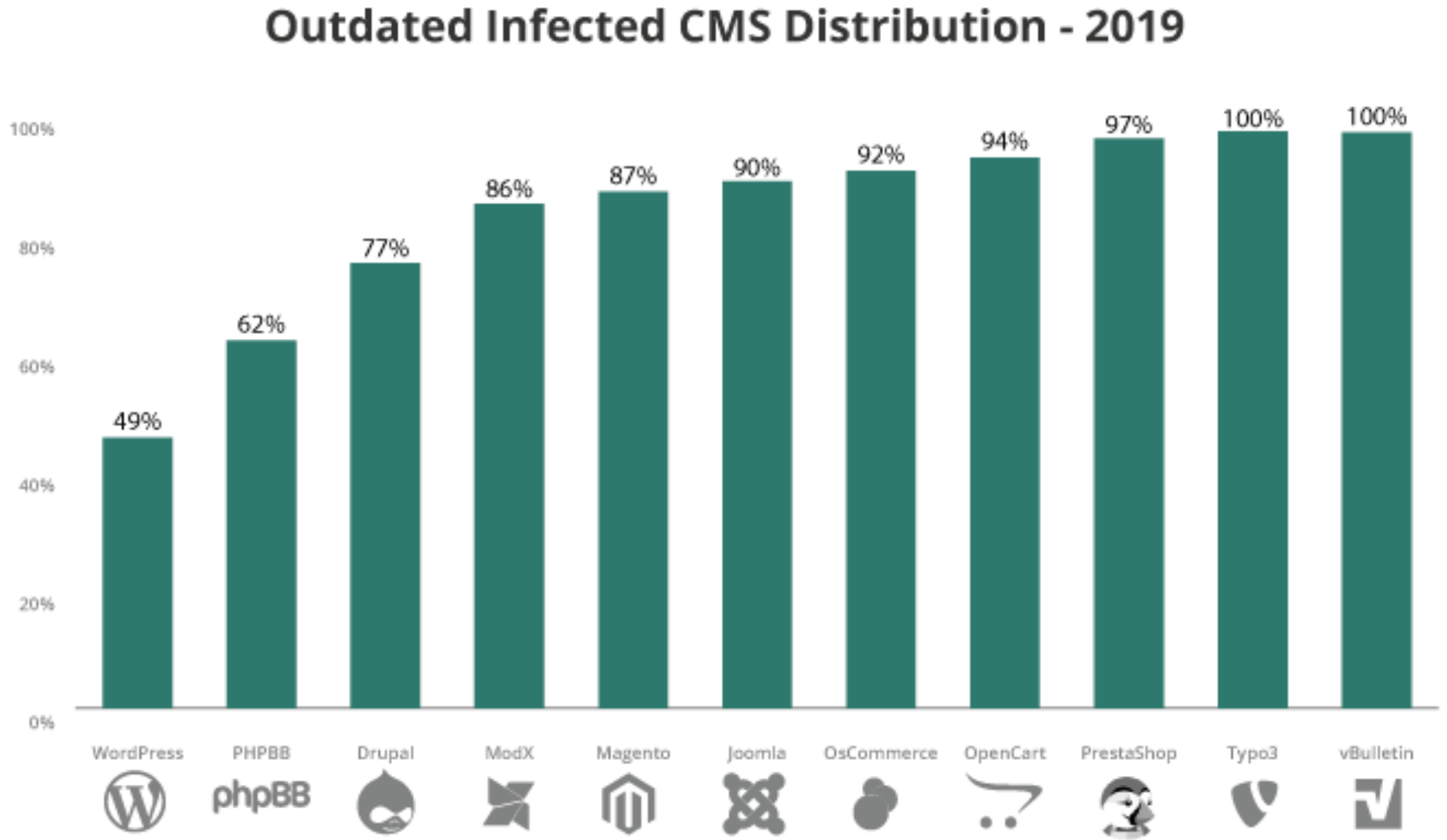


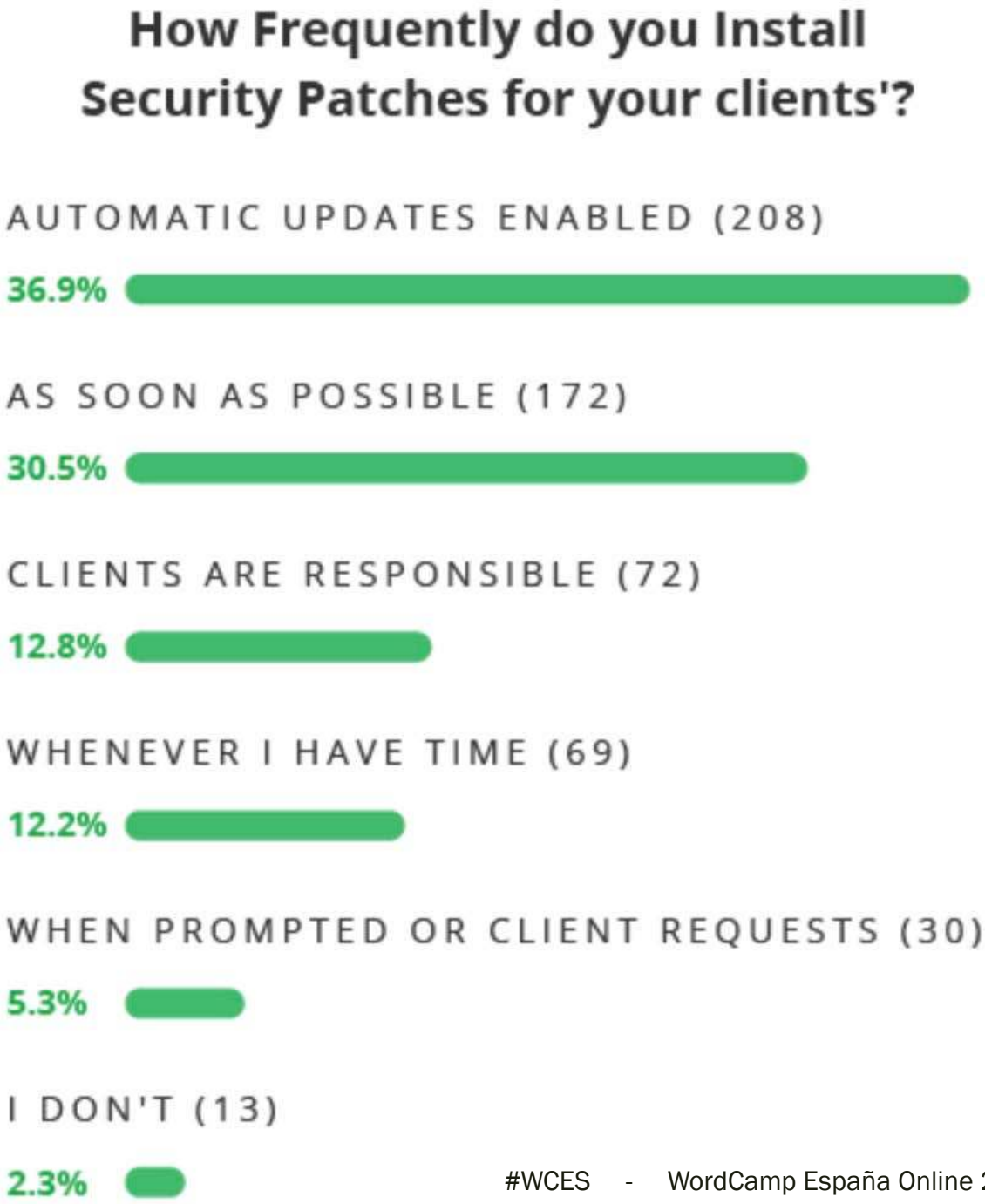
Fuente:
Website Website Threat Research Report 2019
– sucuri.net



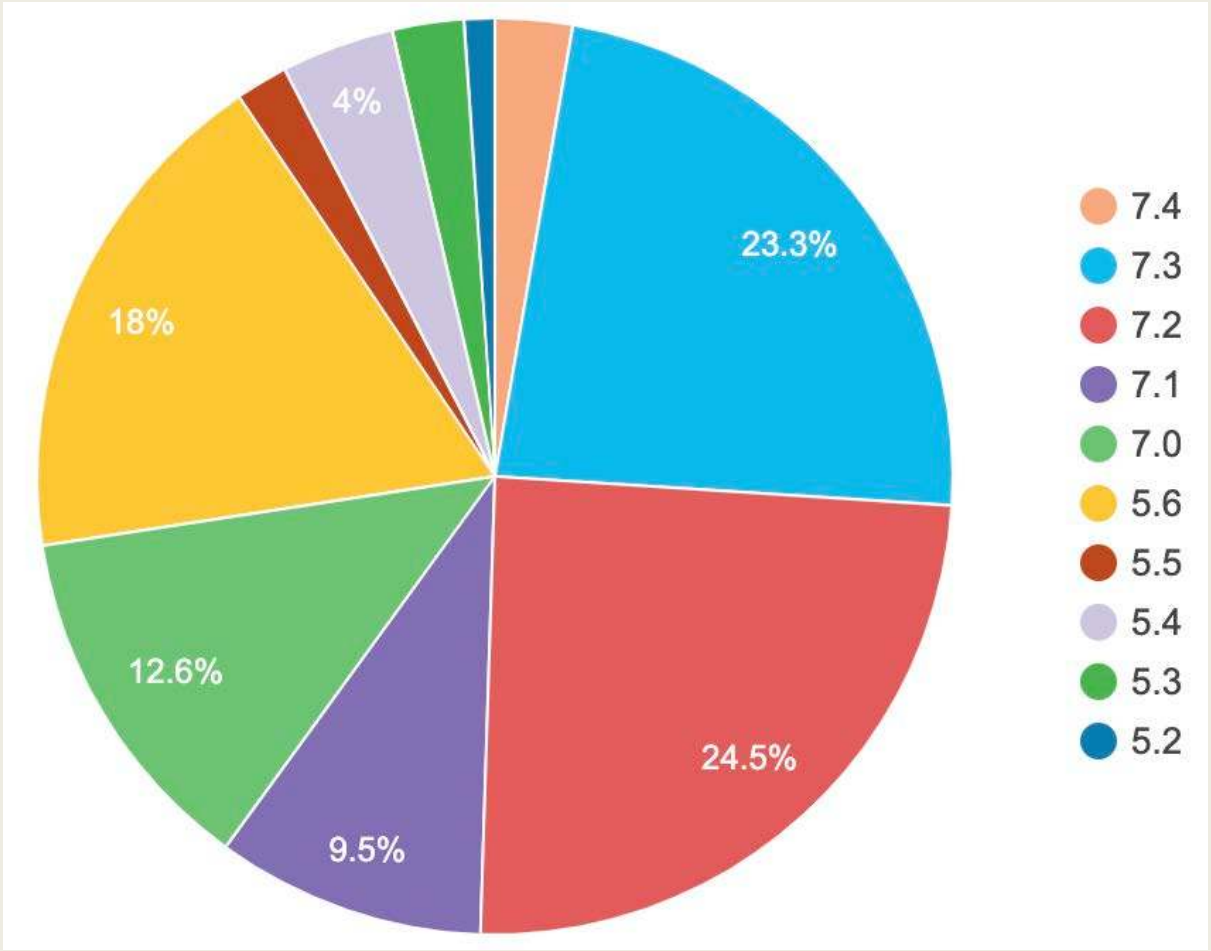
Fuente:
WordPress version distribution at May 2020
– wordpress.org

Fuente: Website Website Threat Research Report 2019
– sucuri.net





Actualizaciones



Fuentes:

Web Professional Security Survey 2019 (Sucuri.net)

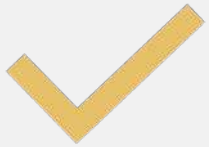
PHP versions distribution May 2020 (wordpress.org)

RESULTADOS

SENTENCIA

¿Es WordPress seguro?

¿Es WordPress seguro?



SI (con reservas)

Al menos todo lo que se puede ser ”out of the box”

ENTONCES, ¿CUÁL ES EL PROBLEMA?

Es EXTREMADAMENTE sencillo hacer un sitio INSEGURO con WordPress

Ejemplo

- Usar usuarios administrador llamado “admin” y contraseñas sencillas
- Instalar plugins no oficiales o freemium o descargados de sitios ”raros”
- No proteger tu sitio usando conexión segura HTTPS (certificado SSL)
- Creer que existe el hosting barato perfecto
- Creer que la seguridad es cosas de paranoicos o que se encarga “otro”
- Creer que a ningún ciberterrorista le interesa tu sitio ni su contenido

¡MIL GRACIAS!

¿Preguntas?