SEGURIDAD WORDPRESS

SAMUEL E. CEREZO // MEETUP WORDPRESS MURCIA

¿QUÉ VAMOS A VER?

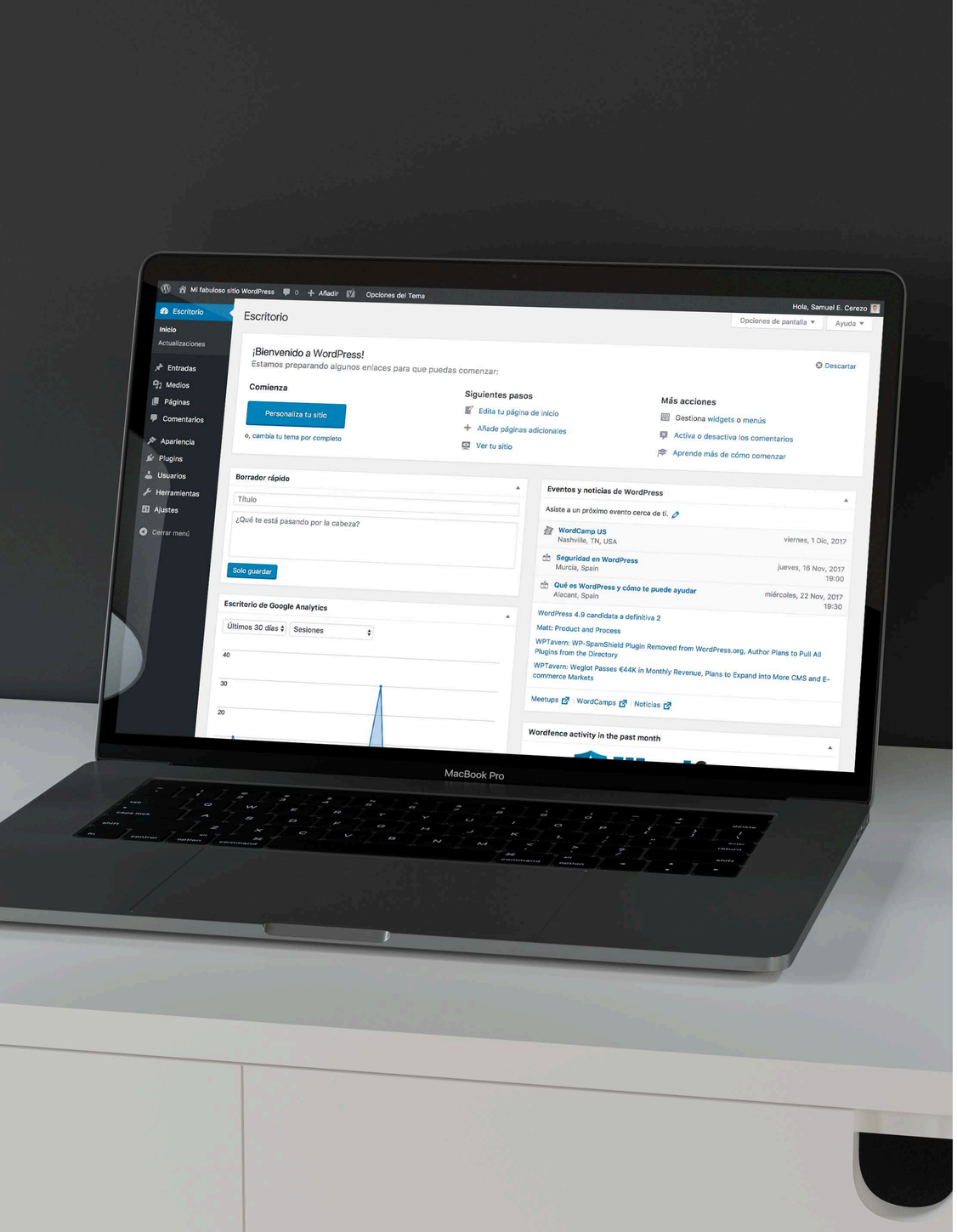
INTRODUCCIÓN

USO WORDPRESS

WordPress es, de lejos, el CMS más usado a nivel mundial. El 53%* de las webs mundiales están programadas sobre WordPress. A nivel nacional, esta estadística aumenta hasta el 65%* de las webs españolas.

Unas estadísticas de uso tan altas lo convier-ten en un blanco perfecto de ataques, ya que encontrada una vulnerabilidad, existe un alto número de webs sobre las que explo-tarla.

** Estadísticas obtenidas del portal builtwith.com*



WORDPRESS

USO GLOBAL

NIVEL MUNDIAL

Casi 20 millones de sitios web utilizan WordPress como gestor de contenido. No se tienen en cuenta las webs de wordpress.com

53%

NIVEL NACIONAL

El 41% de las webs españolas están desarrolladas con la última versión de WordPress.

65%

¿QUÉ VAMOS A VER?

INTRODUCCIÓN

ENTORNO SEGURO

Partimos de la premisa de que, como afirma Panda Security, “No existe la seguridad plena en ningún ambito de la vida, y tampoco en internet”,

¿Quiere decir esto que cualquier protección que tomemos será ineficiente? No, quiere decir que cualquier medida de seguridad tarde o temprano quedará obsoleta y deberemos actualizar la política de seguridad para hacer frente a las nuevas amenazas.

Teniendo presente esta premisa, debemos ser conscientes de la importancia de tener cualquier software o sistema informático actualizado.

OBJETIVO #1

DEFENSA

Crear un entorno seguro y con las menos fisuras posibles. Estar preparadas/os para cualquier ataque.

OBJETIVO #2

ALERTA

Capacidad de reacción frente cualquier ataque, detectarlo y subsanarlo en el menor tiempo posible.

SERVIDOR

PROVEEDOR

SERVICIO CON GARANTÍAS

El primer paso en conseguir un entorno seguro es la elección del servidor donde alojaremos nuestro WordPress.

Debemos escoger un proveedor de confianza, que nos garantice fiabilidad y estabilidad en el sistema.

Desconfiar de proveedores económicos y que desconocemos.

SERVIDOR

SERVIDOR WEB

SSL

Tener un certificado SSL instalado en nuestro servidor web cifrará las conexiones y creará un entorno seguro que aportará confianza al visitante.

Además, si nuestra web no cuenta con un certificado SSL, Google la penalizará.

A día de hoy, muchos proveedores ofrecen certificados SSL gratuitos como Let's Encrypt.

.HTACCESS

Podemos aumentar la seguridad protegiendo los ficheros más sensibles e importantes de nuestra instalación WordPress.

```
<files .htaccess>
order allow,deny
deny from all
</files>
```

```
<files wp-config.php>
order allow,deny
deny from all
</files>
```

WORDPRESS

INSTALACIÓN

NOMBRES DE USUARIO Y CONTRASEÑAS

A la hora de elegir un nombre de usuario y una contraseña (tanto para WordPress como para la base de datos) debemos elegir una cadena de texto segura. Es decir:

Larga y compleja (minúsculas, mayúsculas, dígitos y símbolos).

Esto nos permite tener una instalación más segura frente a ataques de fuerza bruta.

BASE DE DATOS

El prefijo de la base de datos es recomendable que sea distinto al que viene por defecto.

Una medida de seguridad extra es cambiar el “nicename” de los usuarios en la base de datos.

WORDPRESS

INSTALACIÓN

ELIMINAR ARCHIVOS INNECESARIOS

Realizada la instalación de WordPress, se generan varios archivos que es recomendable eliminar:

- **readme.html** Este archivo, al que se puede acceder públicamente, contiene información sobre la versión de WordPress utilizada, con lo que estamos dando información sobre vulnerabilidades existentes.
- **wp-config-sample.php** A pesar de que en principio no entraña ningún peligro, este archivo no tiene ninguna función más alla de la instalación de WordPress.

WORDPRESS

PLUGINS

CONCEPTOS GENERALES

A la hora de instalar un plugin, debemos realizar la instalación desde el respositorio de WordPress para asegurarnos que:

- Es de un desarrollador de confianza.
- El plugin no se ha modificado.

Si instalamos plugins de terceros fuera del repositorio, debemos estar seguros de que son seguros y no afectarán a nuestra instalación.

PLUGINS DE SEGURIDAD

En el repositorio de WordPress contamos con distintas soluciones de seguridad, muchas gratuitas, que nos permitirán monitorizar la actividad y nos alertarán de amenazas:

- Wordfence
- All in One WP Security & Firewall
- iThemes Security
- Centrora Security

WORDPRESS

WORDFENCE

SEGURIDAD Y CORTAFUEGOS

Uno de los mejores plugins de seguridad es Wordfence. Dispone de opciones como bloquear el acceso a países enteros, bloquear a determinados nombres de usuarios o alertar de fallos de seguridad.

Instalar y activar es suficiente para que comience a monitorizar en tiempo real la actividad que tiene lugar en nuestro sitio web.

WORDPRESS

PLUGINS

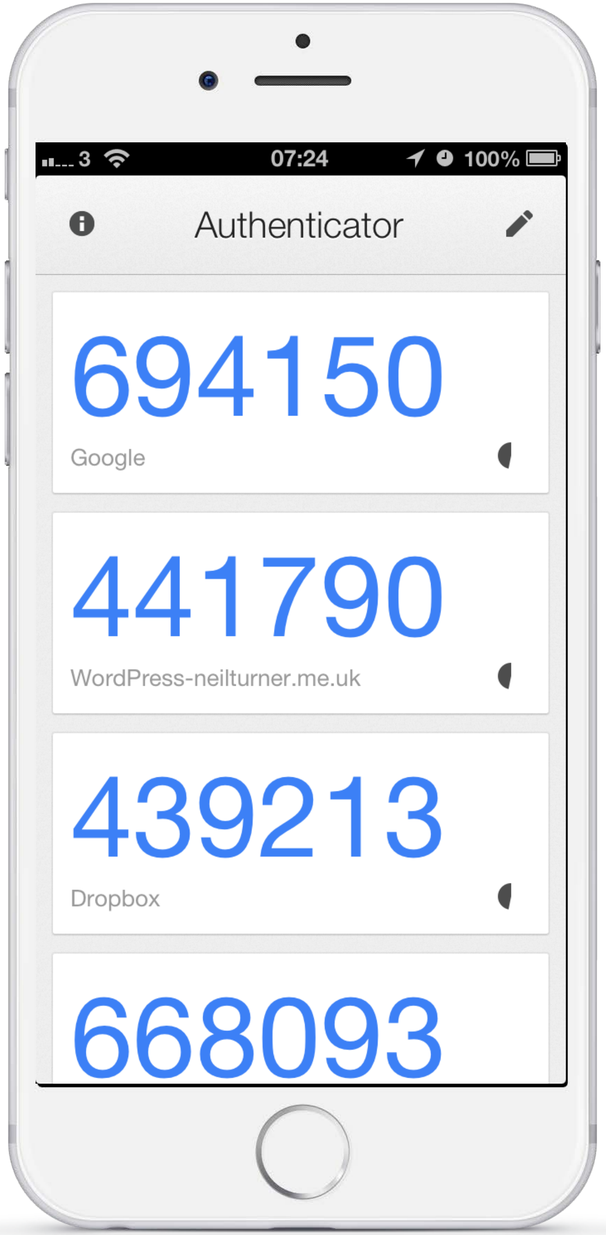
AUMENTAR LA SEGURIDAD

Aparte de los plugins mencionados que protegen frente a ataques y permiten llevar un seguimiento de la actividad en la web, en el repositorio de WordPress contamos con una serie de plugins que aumentan la seguridad.

SEGURIDAD EN EL INICIO DE SESIÓN

Estos plugins presentan distintas soluciones que crean una capa de seguridad extra a la hora de iniciar sesión:

- Captcha
- Verificación en dos pasos



WORDPRESS

PLUGINS

VERIFICACIÓN EN DOS PASOS

Una de las medidas de seguridad más potentes a día de hoy es la verificación en dos pasos. Consiste en la solicitud a la/el usuaria/o un código temporal de vida muy corta que se genera normalmente en una aplicación instalada en un dispositivo de confianza previamente configurado.

Es el caso de **Google Authenticator**.

WORDPRESS

COMENTARIOS

PUERTA DE ENTRADA

El formulario de comentarios de WordPress es una puerta de entrada de código malicioso y de SPAM. Debemos tener una correcta configuración de los mismos y desconfiar de códigos o enlaces sospechosos que entren por esta vía para evitar ataques indeseados.

Una buena configuración podría ser que los comentarios se deben aprobar previamente a menos que el autor tenga ya algún comentario aprobado anteriormente.
Por supuesto, no pulsar sobre ningún enlace sospechoso.

WORDPRESS

USUARIOS

REGISTRO

Si nuestro sitio web tiene habilitado el registro de usuarios, debemos asegurarnos que el rol por defecto a la hora de registrarse no le permite acceder al panel de WordPress y que sus habilidades están acotadas.

?AUTHOR=0

Una de las variables que maneja WordPress es la variable author en la url. Si añadimos “?author=0” a la url, nos llevará a la página del usuario que ejecutó la instalación, y por tanto, administrador. Debemos limitar la información que se da en esta página, cambiar el nicename o eliminar el usuario inicial.

WORDPRESS

BACKUPS

COPIAS DE SEGURIDAD PERIÓDICAS

Una medida de seguridad pasiva consiste en realizar copias de seguridad de manera periódica. Si sufrimos un ataque o perdemos información y contamos con una copia de seguridad reciente con la que realizar una restauración, el daño será menor.

Y SI...

WEB ATACADA

QUÉ HACER

Si llegamos a la indeseable situación de que nuestra web ha sido atacada, debemos mantener la calma y seguir una serie de pasos para revertir la situación

CAMBIAR CONTRASEÑAS

El primer paso es cambiar las contrasñeas de WordPress, base de datos y del servidor, así como verificar que la información de los usuarios es la correcta.

EVALUAR LOS DAÑOS

A continuación debemos evaluar los daños e intentar averiguar qué sucede. Muchas veces se inyecta un código javascript que crea una redirección y con eliminar la línea de código que genera la redirección es suficiente.

RESTAURAR COPIA DE SEGURIDAD

Si la web se ha visto comprometida seriamente, se ha perdido contenido o no podemos determinar el alcance del ataque y disponemos de una copia de seguridad reciente, debemos proceder a restaurarla.

En caso de que no tengamos copia de seguridad, debemos contactar con el proveedor donde se aloja la web y preguntar si disponen de una copia de seguridad para realizar una restauración.

REVISAR LA POLÍTICA DE SEGURIDAD

Una vez restaurada la web, debemos revisar y actualizar la política de seguridad. Esto implica actualizar el motor de WordPress, temas y plugin, revisar los archivos principales para comprobar que no tienen código malicioso (.htaccess y wp-config.php) y adoptar medidas de seguridad extra que impidan que la situación se pueda volver a repetir.

MUCHAS

GRACIAS

SAMUEL E. CEREZO

TWITTER

@samuelcerezo

MAIL

hola@samuelcerezo.com

LINKEDIN

/samuelcerezo