Curso de Seguridad para WordPress

Días: 15, 16, 17, 18 y 19 de enero 2017
Horario: por las tardes de 16h. a 20h.
Duración: 20 horas
Modalidad: Curso Presencial

Precio: 250 euros
Un ordenador por alumno - Máximo 10 alumnos

Lugar: Aula Ultimobyte (Nueva dirección)
Avd. De Aragón 8 Entlo E
46021 Valencia

Requisitos : Conocimiento de Wordpress a nivel editor | administrador.
La formación propuesta está orientada a usuarios intermedios que ya tengan conocimiento sobre el funcionamiento básico de Wordpress. No es el objetivo de este curso formar al alumnos en el manejo de este gestor de contenidos, sino informarlo sobre los peligros potenciales de Wordpress y las contra-medidas necesarias para su protección.

1.- Consideraciones Generales

- Gestores de contenidos. Tipos.
- Tipos de Usuarios y roles
- Árbol de directorios
- Estructura y funcionamiento
- Actualizaciones
- Mantenimiento del sitio
- Restauración y copias de seguridad
- Limpieza de archivos
- Traslados y migraciones
- Importación y exportación de datos

2.- Instalación de Wordpress con seguridad

- Usuarios y contraseñas
- Instalación local
- Permisos de archivos
- Creación de base de datos y permisos
- Configuración del prefijo de tablas
- Configuración de enlaces permanentes
- Protección del archivo de instalación
- Protección de los archivos de configuración
- Protección del directorio de administración
- Protección de la página de inicio
- Protección de directorios
- Tablas

3.- Protocolos de seguridad básicos

- Análisis de riesgos. Herramientas.
- Equilibrio entre seguridad y usabilidad
- Eliminar versión de WordPress
- Plugins y temas seguros
- Claves de autentificación
- Implementación de cortafuegos
- Bloqueo de accesos
- Ocultación URL de administración
- Bloquear URL de administración
- Seguridad en formularios

4.- Protocolos de seguridad avanzados

- Configuraciones Servicio PHP
- Configuraciones Servidor Web Apache
- Configuraciones Wordpress core
- Introducción a Wordpress Codex

5.- Servidores de alojamiento

- Conceptos y características
- Tipos de servidores
- Servidores seguros
- Servidores especializados
- Sistemas operativos y servicios
- Paneles de control

6.- Información sobre ataques

- Ataques por fuerza bruta
- Ataques por malware
- Ataques por denegación de servicio
- Control de spam
- Hotlinking
- Spam automatizados
- Spam de comentarios
- Hacks
- Robots maliciosos
- Modificación de archivos

7.- Indexamiento en buscadores

- Comprobación salud de dominio
- Comprobación servidor de hospedaje
- Comprobación contenido indexado en buscadores
- Reparación de contenido indexado en buscadores
- Creación de archivo índice en XML
- Tratamiento de imágenes de forma masiva

8.- Velocidad de carga – WPO

- Análisis
- Detección de problemas
- Reducción de solicitudes
- Ordenación de peticiones
- Compresión de código
- Configuraciones de lado de cliente
- Configuraciones de lado de servidor
- Tratamiento de imágenes de forma masiva

9.- Plugins de seguridad

- Creación de contenido de forma masiva
- Formularios de contacto seguros
  Sistemas anti-spam – Captcha
- Control de comentarios
- Problemas con plugins de seguridad
- Sucuri – Wordfence - Wp Segurity