Módulo 4. Seguridad

4.1 Seguridad con wordpress.com

Si tu Wordpress lo has dado de alta en wordpress.com, tendrás pocas cosas que preocuparte sobre seguridad, ya que serán los gestiores de wordpress.com quienes se encargarán de actualizar el Wordpress y de mantener los elementos de seguridad necesarios.

Con wordpress.com podrás realizar un backup de los textos de tus páginas y publicaciones, así como de las imágenes que hayas añadido en la librería de medios. Puedes consultar cómo realizarlo en el apartado "**Backup integrado de Wordpress**".

Con tu usuario en wordpress.com, podrás acceder a securizar tu Wordpress mejorando la seguridad en la forma de acceso. Para ello dale clic en el muñequito que está en la esquina superior derecha de la página, y accederás a una zona de configuración de tu ususuario de Wordpress.

usuario wordpress.com.png

Desde ahí, puedes acceder a la sección de **Seguridad** en el menú izquierdo.

seguridad wordpress.com.png

Ahí, podrás cambiar datos de tu **Perfil** de usuario para cambiarte el nombre y apellidos.

Desde el menú **Privacidad**, podrás desactivar "Usa nuestra herramienta de análisis para compartir información sobre el uso que haces de los servicios mientras estás conectado a tu cuenta de WordPress.com.", para que wordpress.com no utilice tus datos de uso.

Desde el ítem de menú **Ajustes de la cuenta,** entre otras cosas, tendrás la opción para dar de baja definitiva tu usuario de wordpress.com dándole clic a "Cerrar la cuenta de forma permanente".

4.2. Seguridad en Wordpress

Conceptos generales sobre seguridad

Desde el panel de administración del Wordpress hay que:

- Mantener **actualizado** Wordpress, Plugins y Temas.
- Tener responsabilidad en la elección e instalación de Plugins y Temas:
  - Instalar sólo plugins que estén registrados en el repositorio oficial de plugins de Worpdress disponible en https://es.wordpress.org/plugins/
  - Conviene encarecidamente realizar búsquedas en Internet sobre posibles vulnerabilidades.
- Instalar y configurar adecuadamente varios plugins de seguridad.
- NOTA: En un Wordpress de wordpress.com no hay que preocuparse de estos puntos, ya que desde wordpress.com se encargan de mantener actualizado el worpdress y sólo usan plugins validados por ellos.

Pero también es necesaria la **involucración** de los usuarios del Wordpress:

- Los usuarios deben usar **contraseñas complejas**.
- No dejarse sesiones abiertas en navegadores.

Y sobre todo, hay que tener **copia de seguridad de todo**. *Si de algo no tienes copia de seguridad, quizás sea porque no te importa mucho perderlo...*

Medidas de seguridad esenciales para Wordpress

- No hay que tener un usuario llamado **admin,** ni un usuario llamado igual que nuestro Wordpress, ya que será el primer usuario que intenten probar para hackear el Wordpress. Otros nombres no recomendados: administrador, wp, wordpress, etc.
- Ocultar los nombres de los usuarios haciendo que cada usuario tenga un "alias" para mostrar diferente de su "nombre de usuario", lo cual se configura en el perfil de cada

usuario.

- Instalar y configurar **Wordfence** (es un plugin completo: escaner y cortafuegos), para realizar escaneos de posibles ataques (actúa como medida de detección y limpieza de malware) y para bloquear conexiones detectadas como maliciosas (actúa como cortafuegos).
- El plugin **Captcha by Bestwebsoft** añade un captcha en la página de login. Un captcha solicita que se introduzca letras o números, con interacción con el usuario, para evitar múltiples intentos de acceso automáticos. Tiene opción de bloqueo de acceso ante errores de login, lo mismo que en Wordfence: Se pueden tener las dos en paralelo, y se aplicará el bloqueo que se dé en primer caso.
- Realizar **copias de seguridad** del Wordpress con UpdraftPlus y guardarlas, por ejemplo en Dropbox.
- El plugin **Really Simple SSL** es MUY interesante, ya que con él se puede activar la conexión segura **https** para tu Wordpress. Si el servidor de alojamiento no tiene conexión segura, la dirección de acceso a tu Wordpress será del estilo

  http://nombredelwordpress.es, y los navegadores marcarán tu sitio Wordpress como un sitio no confiable. En tal caso será muy recomendable que instales y actives el plugin Really Simple SSL, y la dirección de acceso a tu Wordpress será del estilo

  https://nombredelwordpress.es y los navegadores marcarán tu sitio Wordpress como un sitio confiable.

Recomendable:

- Es muy recomendable instalar y configurar **All in One WP Security**, que es un completo plugin de seguridad. Tiene algunas funcionalidades repetidas con Wordfence, en tales casos sólo convendría tener activadas dichas funcionalidades en uno de los dos plugins.
- **Anti-Malware Security and Brute-Force Firewall**: Escaneo sencillo pero efectivo para detectar hackeos en el Wordpress.
- **Plugin Security Scanner:** Permite revisar vulnerabilidades en tus otros plugins.

Recuperar un Wordpress hackeado (requiere acceso al alojamiento web)

Aun con todo, existen listados de vulnerabilidades conocidas de Wordpress, Plugins y Temas:

https://wpvulndb.com/, y cada día van saliendo nuevas vulnerabilidades. En los siguientes enlaces encontraremos más información sobre qué hacer con un Wordpress hackeado:

https://codex.wordpress.org/FAQ_My_site_was_hacked

https://www.wordfence.com/docs/how-to-clean-a-hacked-wordpress-site-using-wordfence/

A modo de prevención, estas webs serán muy útiles para Administradores informáticos en busca de vulnerabilidades:

- https://wpscans.com/
- https://wpscan.org/

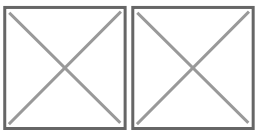
4.2.1. Actualizar Wordpress

La medida de seguridad más esencial a realizar es mantener el Wordpress actualizado. Si tu Wordpress es proporcionado por un servicio de Wordpress tal como wordpress.com, se encargarán de mantener Wordpress actualizado. Si tu Wordpress está instalado en un alojamiento Web, deberás encargarte de actualizar Wordpress. Para ello, desde el Escritorio en la zona de administración, te asivará si existe una nueva versión de Wordpress, junto con un enlace "Por favor, actualiza ahora".

En la siguiente página podrás actualizar Wordpress con un sólo clic en el botón azul "Actualizar ahora":

También habrá que actualizar:

- Plugins
- Temas
- Traducciones



4.2.2. Wordfence

El plugin Wordfence tiene dos pilares básicos:

- Escanear el Wordpress en busca de hackeos
- Activar características para proteger el Wordpress (llamado firewall). Es interesante la opción de limitar el tráfico, ya que evitará que se realicen ataques de fuerza bruta contra tu Wordpress.

ESCANEAR EL WORDPRESS

1º **Wordfence** compara lo que tenemos en nuestro servidor con los repositorios oficiales. **Por ello, primero requiere que tengamos todo actualizado.**

2º Hay que configurar las opciones de escaneo en `Wordfence Scan Options > Options`Hay que activar casi todas las opciones para un escaneo más profundo, revisando estas opciones:

- Scan theme files against repository versions for changes: Activar
- Scan plugin files against repository versions for changes: Activar
- Scan files outside your WordPress installation: Probar a activarlo porque realiza una búsqueda más profunda, pero si se activa, puede que el escaneo tarde muchísimo o que no termine nunca porque entre en un bucle.
- Scan images, binary, and other files as if they were executable: Ralentiza mucho pero puede llegar a ser útil en algún ataque muy concreto.
- Enable HIGH SENSITIVITY scanning (may give false positives): Habilita un escaneo muy sensible, si se activa puede que dé muchos falsos positivos.
- Use low resource scanning (reduces server load by lengthening the scan duration): Requerirá más tiempo para escanear con objeto de no sobrecargar el servidor

3º Se lanza con la opción SCAN:

> Acceso en: Menú > Wordfence > Scan > Botón "Start a Wordfence scan"

Resultados: Si Wordfence muestra que hay alguna vulnerabilidad, en primer lugar deberás analizar si es un falso positivo, que suele ser lo más normal. En caso de que tu Wordpress haya sido objeto de algún ataque real, podrás intentr solucionarlo con las opciones que proporciona Wordfence.

FIREWALL

Wordfence incluye reglas para cortar conexiones que son detectadas como maliciosas. Las opciones de configuración de ataques de acceso al Escritorio por fuerza bruta son las más importantes para incrementar la seguridad. Entre ellas, se destaca configurar las siguientes opciones:

> Acceso en: Menú > Wordfence > Firewall > Brute Force Protection

- **Enforce strong passwords**: Activado. Sirve para exigir uso de passwords fuertes a todos o a determinados roles de usuario
- **Lock out after how many login failures**: Bloquea (*) el acceso al Wordpress después de 20 fallos de login. Mejor reducir a 5 para incrementar la seguridad.
- **Lock out after how many forgot password attempta:** Bloquea (*) el acceso al Wordpress después de 20 fallos de recuperación de contraseña. Mejor reducir a 5 para incrementar la seguridad.
- **Count failures over what time period:** Elegir periodo para contabilizar el número de fallos permitidos. Por ejemplo, en la última hora.
- **Amount of time a user is locked out:** Tiempo en que se mantiene bloqueado el acceso a un usuario. Por ejemplo, durante 6 horas.
- **Immediately lock out invalid usernames:** Desactivado. Si se activara, en caso que te equivoques una vez al hacer login, te bloquea inmediatamente. Es una opción que incrementa la seguridad, pero cuidado, ya que puedes bloquearte el acceso con un único fallo.
- **Don't let WordPress reveal valid users in login errors**: Activado. No mostrar si el usuario con el que se ha intentado acceder era válido, para así no dar pistas a los posibles atacantes.
- **Prevent users registering 'admin' username if it doesn't exist:** Activado. Evitar que exista un usuario admin en el Wordpress, ya que es el primer nombre de usuario al que los atacantes intentarán adivinarle la contraseña.
- **Immediately block the IP of users who try to sign in as these usernames:** Bloquear la IP de alguien que intenta entrar con esos usuarios. Por ej conviene poner: admin, administrator, wordpress, user, etc.

(*) El bloqueo de acceso a Wordpress se realiza por IP, no por nombre de usuario. La IP será la dirección pública del router de conexión a Internet. Es decir, si desde tu casa (o desde tu centro educativo) te equivocas repetidas veces al escribir tu nombre de usuario y contraseña, se bloqueará el acceso desde cualquier ordenador de tu casa (o desde cualquier ordenador de tu centro educativo).

LIMITAR TRÁFICO

Podemos visualizar el tráfico que hay en el instante:

> Acceso en: Menú > Wordfence > Live Traffic

Wordfence permite limitar el tráfico de datos que se genera para evitar sobrecargas y caídas.

> Acceso en: Menú > Wordfence > Firewall > Rate Limiting

- **Throttle =** regular el acceso: Wordpress responderá error 503 pero se seguirá permitiendo acceso posteriormente
- **Block =** bloquear acceso definitivamente. Poner block si tienes problemas con mucho tráfico de robots
- Immediately block fake Google crawlers: Activar
- How should we treat Google's crawlers: Treat Google like any other Crawler
- If anyone's requests exceed: 240 - throttle
- If a crawler's page views exceed: 240 - throttle
- If a crawler's pages not found (404s) exceed: 30 - block, para evitar que escaneen tu sitio ante vulnerabilidades
- If a human's page views exceed: 240 - throttle
- If a human's pages not found (404s) exceed: 30 - block
- If 404s for known vulnerable URLs exceed: 15 - block

How long is an IP address blocked when it breaks a rule: 1 hora

Parámetros sugeridos obtenidos de la ayuda de Wordfence:
https://docs.wordfence.com/en/Wordfence_options?utm_source=plugin&utm_medium=pluginUI&utm_campaign=docsIcon#Rate_Limiting_Rules

4.2.3. All In One WP Security

Permite habilitar numerosas medidas de seguridad (algunas ya están en Wordfence) para nuestro Wordpress. Este plugin indica el grado de protección que tenemos con un interesante gráfico en forma de cuentakilómetros.

> Se configura en: Menú > Seguridad WP

Cambiar la dirección de acceso al Escritorio de Wordpress

La opción más interesante a configurar consiste en **cambiar la dirección de acceso al Escritorio de Wordpress**, de forma que ya no sea http://nombredelwordpress.es/wp-admin/, sino que escojamos una dirección diferente a **wp-admin**, para evitar que los hacker maliciosos intenten acceder a nuestro Wordpress entrando por la dirección por defecto wp-admin que es conocida por todo el mundo. Una vez cambiada la dirección de acceso, desconocerán cual es la dirección de acceso al Escritorio y se reducirá la cantidad de intentos de acceso fraudulentos. Si procedes a cambiar la dirección de acceso al Escritorio, será muy importante que apuntes tu nueva dirección de acceso al Escritorio de tu Wordpress, sino correrás el riesgo de quedarte sin acceso a administrar tu propio Wordpress.

> Se configura en: Menú > Seguridad WP > Fuerza Bruta > Cambiar el nombre de la página de entrada
> Login Page URL (por ejemplo): mizonadegestion

Ahí conviene que cada administrador de Wordpress escoja el nombre que desee, incluso con un nombre diferente a "mizonadegestion", para que no sea tan genérico. De esta forma, la nueva dirección de acceso al Escritorio será similar a:

http://nombredelwordpress.es/mizonadegestion/

Otras opciones a revisar de este plugin:

- Opciones > WP Version Info: Eliminar generador WP Meta Info: SI
- Cuentas de usuario > Mostrar nombre: Revisa que los Nombres de usuario estén ocultos y se muestre el alias
- Ingreso de usuarios > Activar característica de bloqueo de inicio de sesión: SI
- Ingreso de usuarios > Cerrar inicio de sesión: múltiples opciones

- Ingreso de usuarios > Forzar salir > Habilitar el cierre de sesión de usuario de Fuerza WP: si
- Ingreso de usuarios > Mostrar mensaje de error genérico: SI
- Seguridad del sistema de archivos: Deshabilitar "Edición archivo PHP".
- Seguridad del sistema de archivos > WP acceso archivo > Impedir el Acceso a Archivos de Instalación Predeterminada de WP: si
- Cortafuegos > Reglas basicas de Cortafuegos > Habilitar proteccion basica de Firewall: SI
- Cortafuegos > Reglas basicas de Cortafuegos > Bloquear el Acceso al Archivo debug.log : SI
- Cortafuegos > Reglas basicas de Cortafuegos > Bots de Internet > Bloquear falsos Googlebots: SI
- Cortafuegos > Prevenir enlaces activos > Evitar Hotlinking de Una Imagen: SI
- **Fuerza Bruta > Login Captcha > Habilitar Capcha en pagina de ingreso: SI** (*)
- **Fuerza Bruta > Login Captcha > Habilitar Captcha en Página de recuperar contraseña: SI** (*)
- Fuerza Bruta > Honeypot > Habilitar Honeypot En La Página De Entrada : SI
- Escáner: detección de cambios en los archivos, porque si hay cambios no deseados es probable que sean hackeos.

(*) Las opciones de habilitar **Captcha** proporcionan un gran incremento en la seguridad del Wordpress, ya que evitan que se realicen ataques automatizados intentando adivinar las contraseñas los usuarios del Wordpress.

4.3. Copia de seguridad

Copia de seguridad

Wordpress incluye un sistema de creación de Backups, que realiza copia sólo del contenido de las entradas.

Se recomienda utilizar el plugin **UpdraftPlus** para realizar las copias de seguridad, porque realiza una copia completa del sitio web, además de permitir restaurar el sitio desde el Escritorio de Wordpress, y alojar la copia de seguridad en almacenamientos externos como Google Drive o Dropbox.

Otro plugin para realizar copias de seguridad completas es BackWPup, pero a diferencia de UpdraftPlus no permite restaurar el sitio desde el Escritorio de Wordpress.

4.3.1. Backup integrado de Wordpress

Sirve para copiar únicamente los **contenidos** de un sitio web Wordpress a otro sitio Wordpress.

Importante: no copia la apariencia, configuración, plugins, etc.

El proceso a realizar es el siguiente:

1º exportar:

> Acceso en: Menú > Herramientas > Exportar

- Se genera un archivo .xml que se guarda en tu PC, que puede abrirse con un editor de textos (recomendado usar notepad++)
- Se guardan: Páginas, Entradas, Comentarios, Menú.
- **No se guarda: imágenes, plugins, temas, etc...**

2º Importar

> Acceso en: Menú > Herramientas > Importar

- Se utiliza el archivo .xml que se ha exportado a tu PC con anterioridad
- El sitio Wordpress antiguo **DEBE ESTAR FUNCIONANDO**
- En el proceso de "importación" las imágenes se copiarán desde el sitio Wordpress antiguo al nuevo sitio Wordpress
- Es necesario instalar temas y plugins y activar plugins en el sitio Wordpress destino

CONCLUSIÓN: Para realizar una copia integral del sitio web, necesitaremos una herramienta de copia de seguridad más completa: UpdraftPlus o BackWPup, por ejemplo.

4.3.2. UpdraftPlus

Backup con UpdraftPlus

Una vez instalado y activado el plugin, su funcionalidad está accesible desde la barra superior.

REALIZAR UN RESPALDO

> Acceso en: Menú > UpdraftPlus > Estado actual / Respaldar ahora > botón "Respaldar ahora"

El respaldo se guarda en el mismo servidor, lo cual tiene desventajas:

- Ocupará mucho en nuestro espacio web
- Si el sitio "cae", el respaldo es posible que también lo perdamos.

Habrá que **Descargar** el respaldo realizado a nuestro PC.

DESCARGAR EL RESPALDO

Se descargan 5 archivos diferentes: base de datos, plugins, temas, ficheros subidos y otros.

BORRAR EL RESPALDO DEL SERVIDOR

SUBIR EL RESPALDO DESDE NUESTRO PC AL SERVIDOR

Habrá que subir los 5 archivos al servidor.

RESTAURAR RESPALDO

4.3.3. UpdraftPlus con Dropbox y Google Drive

UpdraftPlus

Configurar que el respaldo de UpdraftPlus se realice en DROPBOX

Inicia sesión en Dropbox en otra pestaña del navegador. Y vuelve al Wordpress en la opción `UpdraftPlus > Ajustes`:

Podemos elegir si queremos que la copia se haga automáticamente con la periodicidad que digamos, o que la copia haya que hacerla manualmente.

Al terminar el proceso, la copia de respaldo estará en **Dropbox > Aplicaciones > UpdraftPlus.Com**

Si se lanza otra copia de respaldo hacia Dropbox, se guardará en esta misma carpeta UpdraftPlus.Com. El nombre de los archivos de respaldo incluyen la fecha y la hora del respaldo.

Al terminar el proceso, si no hubiéramos marcado la opción de "Borrar respaldos locales", la copia de respaldo la tendríamos **en el servidor,** ocupando un valioso espacio, y podríamos verlo con el plugin **File-Manager** en: `public_html > wp-content > updraft`

Configurar que el respaldo de UpdraftPlus se realice en GOOGLE DRIVE

Suponemos que ya tenemos creado un Proyecto en Google API. A ese proyecto, vamos a crearle unas nuevas "Credenciales" de "ID de cliente de OAuth" para permitir que UpdraftPlus se conecet a nuestra API de Google

1. Asegurarse que la Drive API está Habilitada: en https://console.developers.google.com/ > Panel de Control > Habilitar API > Drive API
2. Crear unas "Credenciales" de "ID de cliente de OAuth" tipo "Web" y obtendremos un ID y Secreto de cliente
3. Introducir ID y Secreto de cliente en Wordpress > UpdraftPlus > Ajustes