Pasos que debemos seguir cuando nos han hackeado nuestro WordPress

Teléfono: 900 103 253
www.hostalia.com

WordPress se ha convertido en el CMS más utilizado hoy en día a la hora de crear páginas web. La gran cantidad de plantillas desarrollas por terceras personas o las innumerables funcionalidades que se pueden añadir por medio de plugins, han ayudado a que esta herramienta sea conocida en todo el mundo. Pero como suele ser habitual, la fama también ha llamado la atención de los hackers, que dedican parte de su tiempo a buscar cualquier vulnerabilidad que puedan utilizar para llevar a cabo sus fechorías. Si alguna vez vuestro sitio es hackeado, no os preocupéis porque se puede solucionar el problema. Es precisamente esto lo que os vamos a explicar a lo largo de este documento.

Consideraciones previas

Antes de meternos en materia y ver cómo podemos solucionar un hackeo, sería bueno comentar algo que todo el mundo sabe pero que no siempre se lleva a cabo. Lo más importante de todo es prevenir antes que lamentar, y para ello es crucial contar con una instalación de WordPress actualizada siempre a la última versión, ya que la gran comunidad que trabaja para mantener este CMS va continuamente continuamente versiones nuevas, que además de añadir funcionalidades, solucionan problemas de seguridad detectados en el código.

Cuando hablamos de actualización, no sólo nos referimos al CMS, sino también a todos los plugins que utilizamos en nuestra web, ya que contar con versiones antiguas, aumenta el riesgo de sufrir algún tipo de ataque.

Además de lo comentado anteriormente, es muy importante que también llevemos a cabo algún tipo de tareas de backups, para que en caso de sufrir algún tipo de ataque, nos sea más fácil solucionar el problema. Normalmente los proveedores de alojamiento web ofrecen este tipo de servicio, por lo que sería interesante que os informarais para disfrutar de mayor seguridad.

Cambiar todas las contraseñas de acceso

Si hemos sido víctimas de un ataque, hay probabilidades de que los atacantes hayan sido capaces de conseguir nuestras contraseñas, por lo que el primer paso que deberemos hacer será el de cambiar las claves tanto del FTP como de la base de datos, así como las de acceso a la administración de nuestro portal.

a) Cambio claves FTP

Empezaremos explicando cómo realizar el cambio del FTP de nuestro dominio en un alojamiento con Hostalia. Para ello, una vez que hayamos accedido a nuestro panel de control mediante la dirección https://panel.hostalia.com, en el menú de la izquierda pulsaremos en la opción que pone "**Alojamiento Web**".

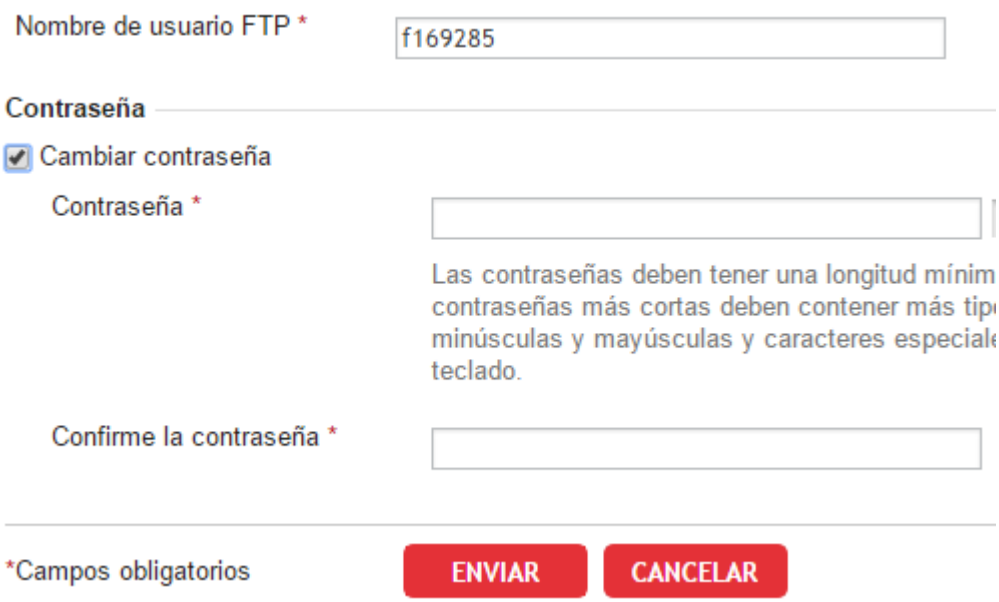
A continuación pulsaremos sobre el botón "**Acceso al hosting**".

Eso nos llevará a una nueva pestaña desde donde podremos gestionar todo lo relativo a nuestro alojamiento contratado. Una vez ahí, para cambiar la clave del FTP, pulsaremos en "**Acceso FTP**".

En la siguiente pantalla, pulsaremos sobre el botón "**Editar**" que nos permitirá modificar los datos de nuestra cuenta FTP.

Si nos fijamos, cuando hayamos pulsado sobre ese botón, podremos cambiar el usuario de nuestra cuenta FTP, pero para cambiar la contraseña, deberemos marcar el checkbox donde pone "**Cambiar contraseña**".

Seleccionada esa opción, ya nos aparecerán los campos para introducir nuestra nueva contraseña.

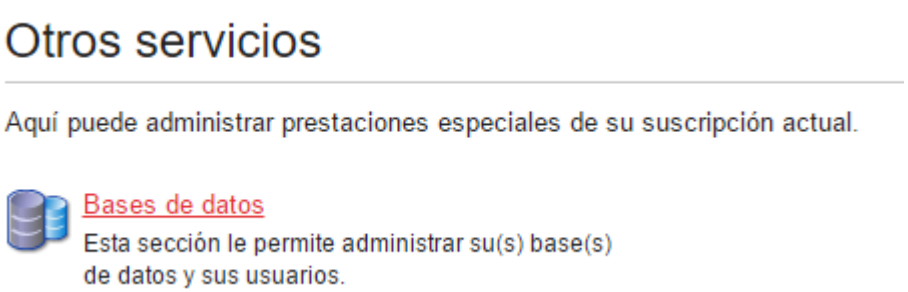


El paso final, será pulsar sobre el botón "**Enviar**" para que se guarden los cambios.

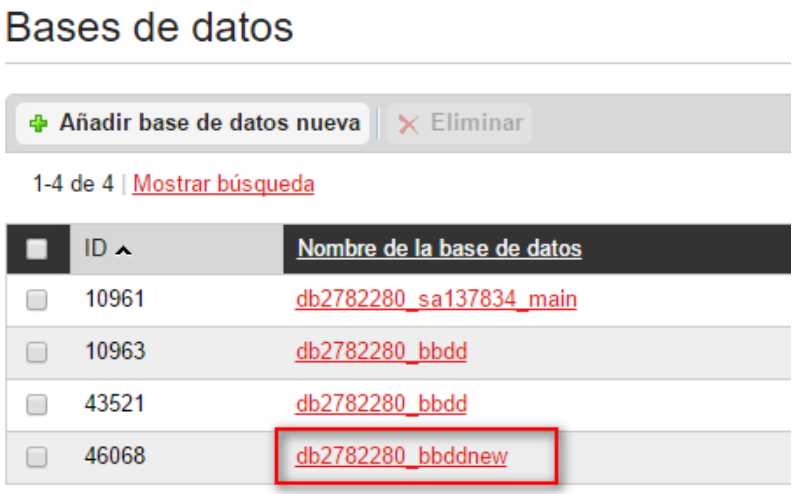
b) Cambiar contraseña de la base de datos

Cambiada la clave del FTP, ahora será el turno de hacer lo mismo con nuestra base de datos. Para ello, una vez estemos en el panel de control de nuestro servidor, pulsaremos sobre la opción "**Otros servicios**" que aparece en el menú superior.

Pulsaremos sobre el icono "**Bases de datos**".



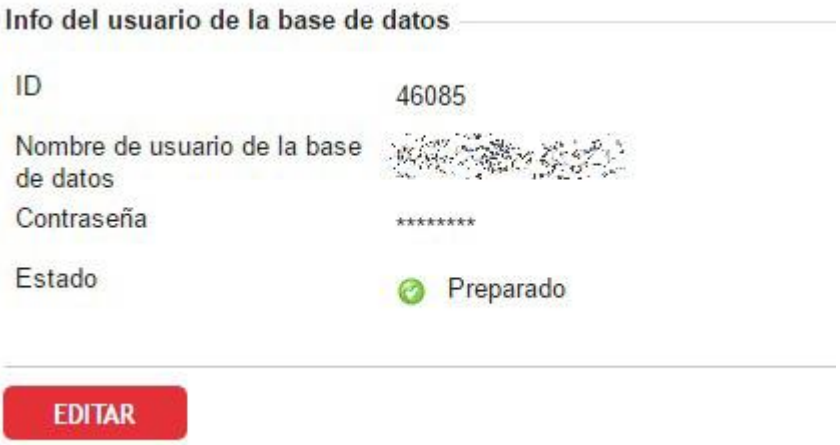
En la siguiente pantalla, nos aparecerán todas las bases de datos que tengamos dadas de alta. Pulsaremos sobre la que queremos hacer el cambio.



Seleccionaremos la opción "**Usuarios**" del menú superior.

A continuación tendremos que pulsar sobre el nombre del usuario del queremos hacer el cambio de contraseña.

Pulsaremos en el botón "**Editar**".



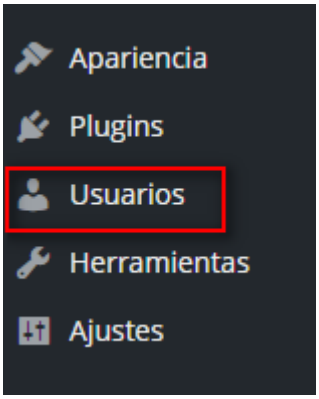
Es entonces cuando nos aparecerá la opción de cambiar la contraseña para la base de datos.

Una vez que se pulsara sobre el botón "**Enviar**", la contraseña quedaría cambiada.

Al hacer todos estos pasos, es muy importante modificar el fichero "**wp-config.php**" de nuestro WordPress para indicar ahí la nueva clave que le hemos puesto en la base de datos.

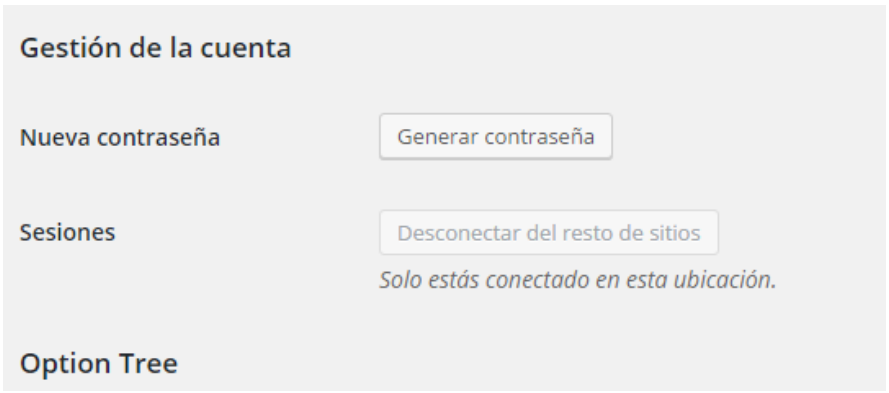
c) Cambiar contraseña acceso al panel de administración de WordPress

Para proceder a cambiar la clave de nuestro usuario de acceso al panel de administración de WordPress, deberemos entrar en él y pulsar sobre la opción de "**Usuarios**" en el menú lateral.

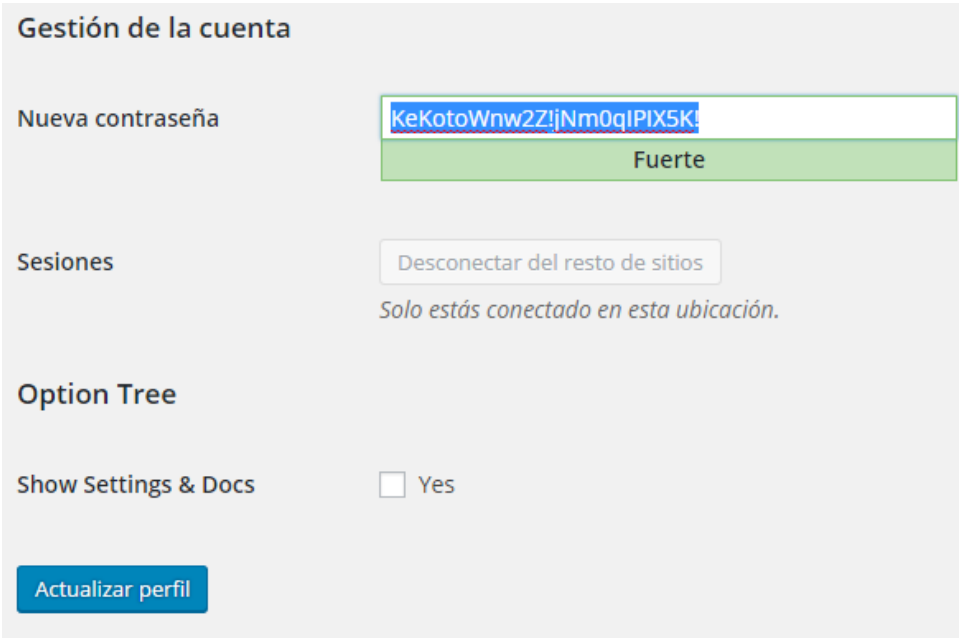


En el listado de usuarios que nos aparecerá, pulsaremos sobre el que queremos editar.

Una vez que se ha cargado la página, bajaremos la pantalla hacia abajo y pulsaremos en el botón "**Generar contraseña**".



Escribiremos la que queramos y pulsaremos en el botón "**Actualizar Perfil**".

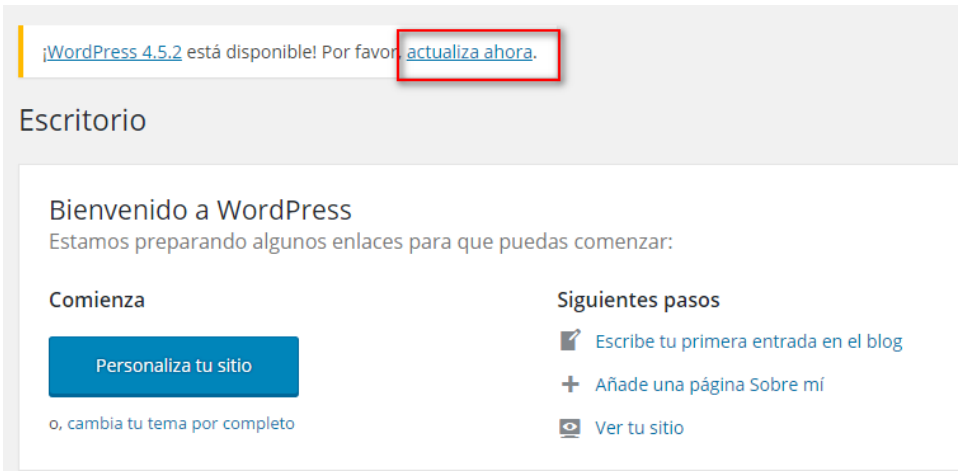


Eliminar todos los archivos sospechosos de WordPress

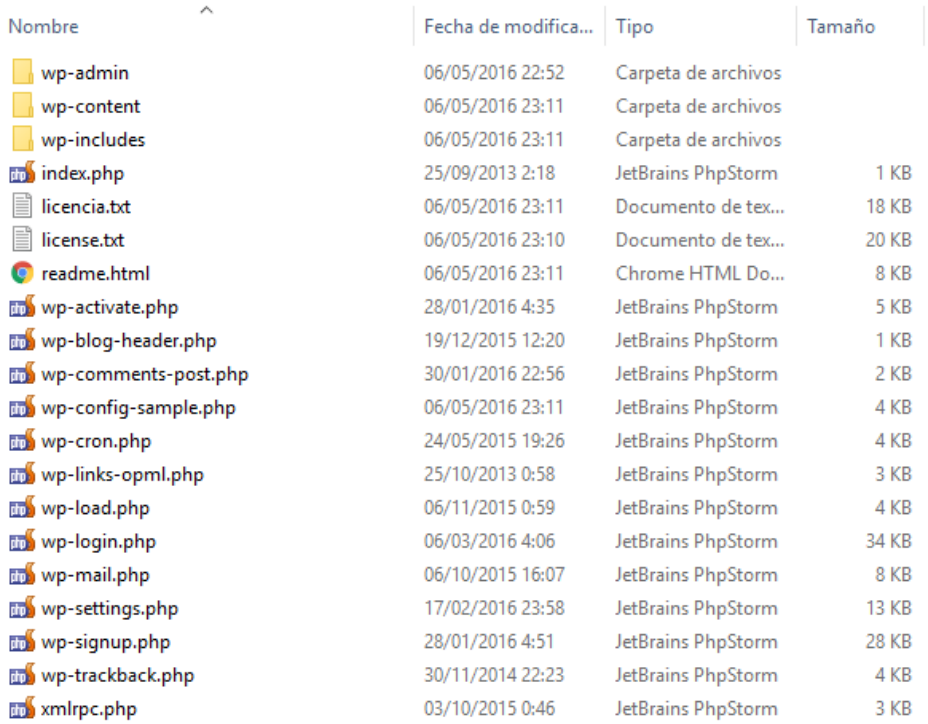
Si no tienes mucha experiencia con WordPress, es muy probable que no puedas reconocer los archivos habituales de este CMS, pero siempre puedes descargar su última versión y echar un vistazo a los archivos que forman parte del proyecto. Una vez familiarizado, puedes acceder a la instalación para intentar detectar esos archivos sospechosos.

Si aun así este proceso de localización de posibles archivos sospechosos te es muy complejo, te explicaremos un método alternativo y que consiste en sustituir todos los archivos que forman parte del WordPress.

Para llevar a cabo esta tarea, nosotros recomendamos que primero actualicéis la versión del CMS a la última versión estable disponible. Para ello, lo podéis hacer desde la administración de nuestra web.

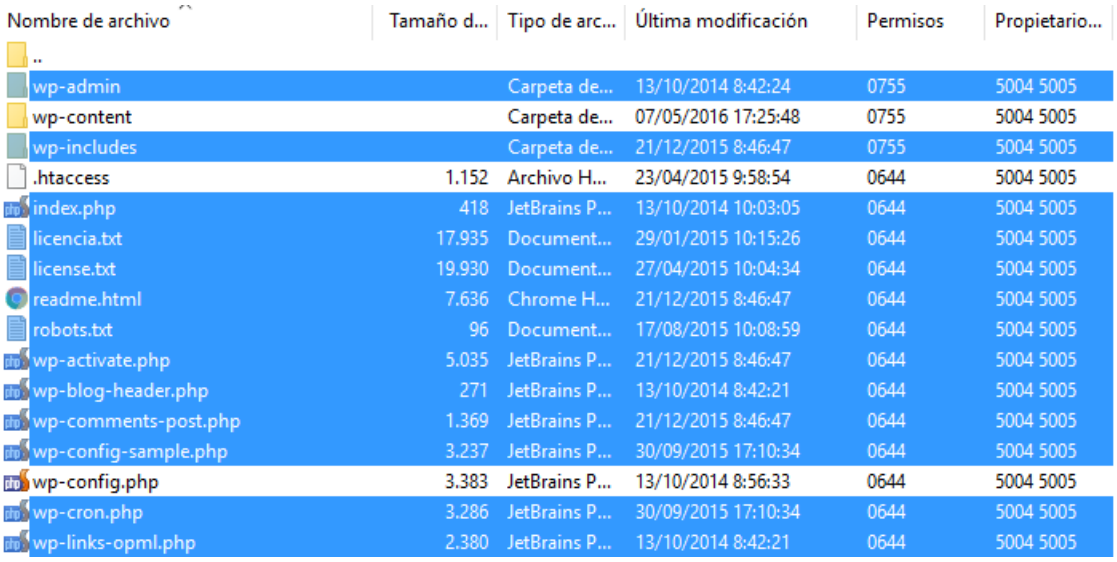


Una vez que esté actualizada, nos descargaremos la última versión de WordPress desde su sitio oficial en nuestro equipo. Cuando lo tengamos descargado, lo descomprimiremos encontrándonos una estructura de carpetas y archivos como la que os mostramos en la siguiente imagen.



Nombre	Fecha de modifica...	Tipo	Tamaño
wp-admin	06/05/2016 22:52	Carpeta de archivos	
wp-content	06/05/2016 23:11	Carpeta de archivos	
wp-includes	06/05/2016 23:11	Carpeta de archivos	
index.php	25/09/2013 2:18	JetBrains PhpStorm	1 KB
licencia.txt	06/05/2016 23:11	Documento de tex...	18 KB
license.txt	06/05/2016 23:10	Documento de tex...	20 KB
readme.html	06/05/2016 23:11	Chrome HTML Do...	8 KB
wp-activate.php	28/01/2016 4:35	JetBrains PhpStorm	5 KB
wp-blog-header.php	19/12/2015 12:20	JetBrains PhpStorm	1 KB
wp-comments-post.php	30/01/2016 22:56	JetBrains PhpStorm	2 KB
wp-config-sample.php	06/05/2016 23:11	JetBrains PhpStorm	4 KB
wp-cron.php	24/05/2015 19:26	JetBrains PhpStorm	4 KB
wp-links-opml.php	25/10/2013 0:58	JetBrains PhpStorm	3 KB
wp-load.php	06/11/2015 0:59	JetBrains PhpStorm	4 KB
wp-login.php	06/03/2016 4:06	JetBrains PhpStorm	34 KB
wp-mail.php	06/10/2015 16:07	JetBrains PhpStorm	8 KB
wp-settings.php	17/02/2016 23:58	JetBrains PhpStorm	13 KB
wp-signup.php	28/01/2016 4:51	JetBrains PhpStorm	28 KB
wp-trackback.php	30/11/2014 22:23	JetBrains PhpStorm	4 KB
xmlrpc.php	03/10/2015 0:46	JetBrains PhpStorm	3 KB

Lo siguiente que haremos, será conectarnos vía FTP a nuestro sitio y eliminar todos los archivos que forman parte de la web excepto la carpeta "**wp-content**" y los archivos "**.htaccess**" y "**wp-config.php**".



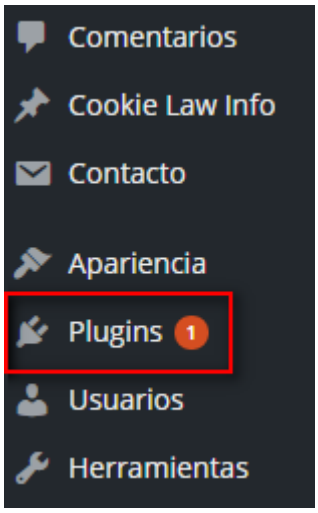
Nombre de archivo	Tamaño d...	Tipo de arc...	Última modificación	Permisos	Propietario...
..					
wp-admin		Carpeta de...	13/10/2014 8:42:24	0755	5004 5005
wp-content		Carpeta de...	07/05/2016 17:25:48	0755	5004 5005
wp-includes		Carpeta de...	21/12/2015 8:46:47	0755	5004 5005
.htaccess	1.152	Archivo H...	23/04/2015 9:58:54	0644	5004 5005
index.php	418	JetBrains P...	13/10/2014 10:03:05	0644	5004 5005
licencia.txt	17.935	Document...	29/01/2015 10:15:26	0644	5004 5005
license.txt	19.930	Document...	27/04/2015 10:04:34	0644	5004 5005
readme.html	7.636	Chrome H...	21/12/2015 8:46:47	0644	5004 5005
robots.txt	96	Document...	17/08/2015 10:08:59	0644	5004 5005
wp-activate.php	5.035	JetBrains P...	21/12/2015 8:46:47	0644	5004 5005
wp-blog-header.php	271	JetBrains P...	13/10/2014 8:42:21	0644	5004 5005
wp-comments-post.php	1.369	JetBrains P...	21/12/2015 8:46:47	0644	5004 5005
wp-config-sample.php	3.237	JetBrains P...	30/09/2015 17:10:34	0644	5004 5005
wp-config.php	3.383	JetBrains P...	13/10/2014 8:56:33	0644	5004 5005
wp-cron.php	3.286	JetBrains P...	30/09/2015 17:10:34	0644	5004 5005
wp-links-opml.php	2.380	JetBrains P...	13/10/2014 8:42:21	0644	5004 5005

Una vez que hayan sido borrados, subiremos todos los archivos de la versión de WordPress que nos hayamos descargado de su sitio oficial.

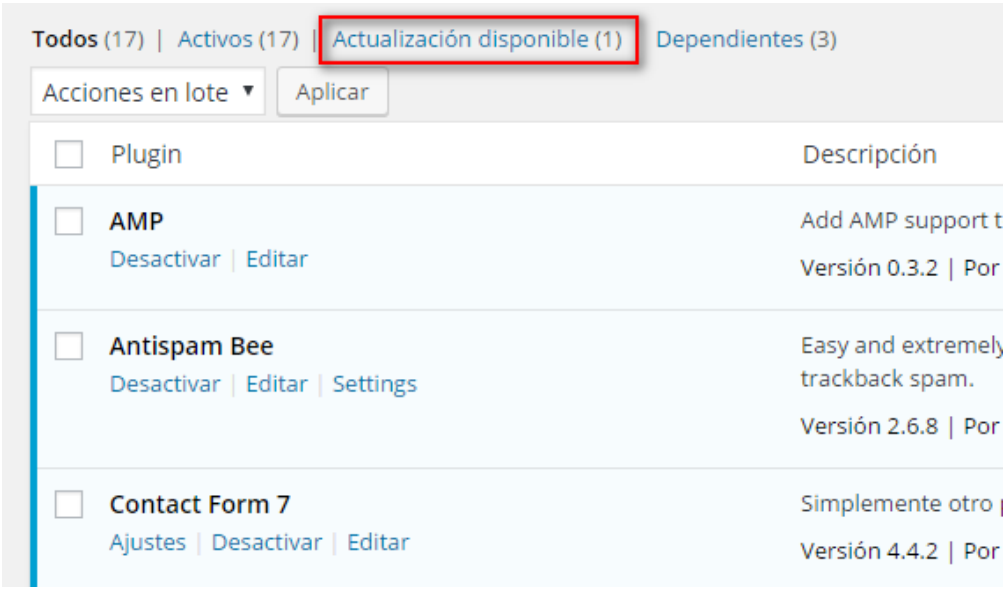
Asegurarse que los plugins estén limpios

Una vez que hemos llevado a cabo el proceso anterior, será hora de investigar si algún plugin también ha podido ser infectado con código malicioso. Como revisar todos los archivos puede ser una tarea muy tediosa, más aún si utilizamos un gran número de estos, nuestra recomendación es que se sustituyan los que utilicemos por descargas completamente limpias. Para esto, al igual que hemos hecho en el caso anterior, es recomendable actualizar aquellos plugins que no estén actualizados.

Para saber si tenemos plugins sin actualizar, lo que haremos será entrar en el panel de administración de WordPress y en el menú de la izquierda, pulsar sobre la opción "**Plugins**".



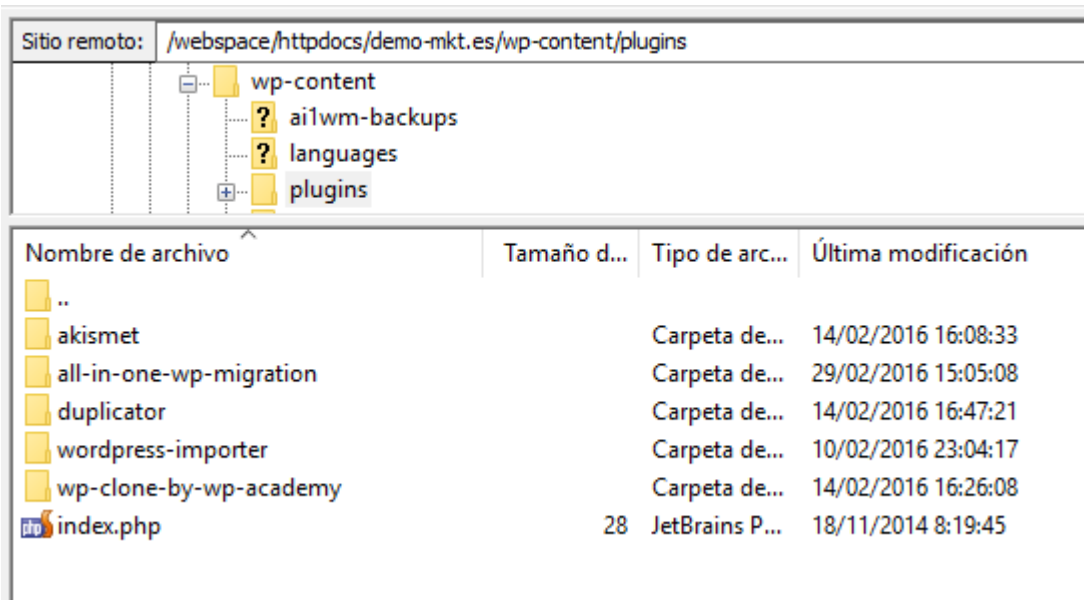
Sabremos que tenemos plugins sin actualizar porque nos aparecerá una opción que pondrá "**Actualización disponible**" en la parte superior del listado de plugins.



Si pulsamos sobre esa opción, nos aparecerá el listado de plugins que podemos actualizar. Sólo tendremos que seleccionarlos y en el menú de acciones por lote, elegir la opción de "**Actualizar**".

Por último, pulsaremos el botón "**Aplicar**" para que se inicie el proceso.

Con esto no nos garantizamos que los plugins se hayan quedado limpios de código malicioso por eso, recomendamos que se borren todos y se vuelvan a subir vía FTP. Para ello, accederemos a la ruta "**wp-content/plugins**" desde dentro de nuestra cuenta FTP.



Cada una de esas carpetas, corresponde a un plugin instalado. Lo que haremos será descargarnos desde el sitio oficial esos plugins y una vez que vayamos eliminando esas carpetas desde el FTP, iremos subiendo las nuevas que nos hayamos descargado.

Si la eliminación de estos plugins lo hiciéramos desde el propio panel de administración de WordPress, primero habría que desactivarlos y luego borrarlos, lo que conllevaría a que se perdiera también la configuración de los plugins, teniendo que volver a configurarlos de nuevo. De la forma que os hemos explicado nosotros, esto no ocurre, y nos aseguraremos de que disponemos de instalaciones totalmente limpias.

Estos mismos pasos que hemos hecho para los plugins, también lo podemos aplicar en el caso del tema utilizado en nuestro portal, pero en este caso, deberíamos trabajar sobre la carpeta "**wp-content/themes**"

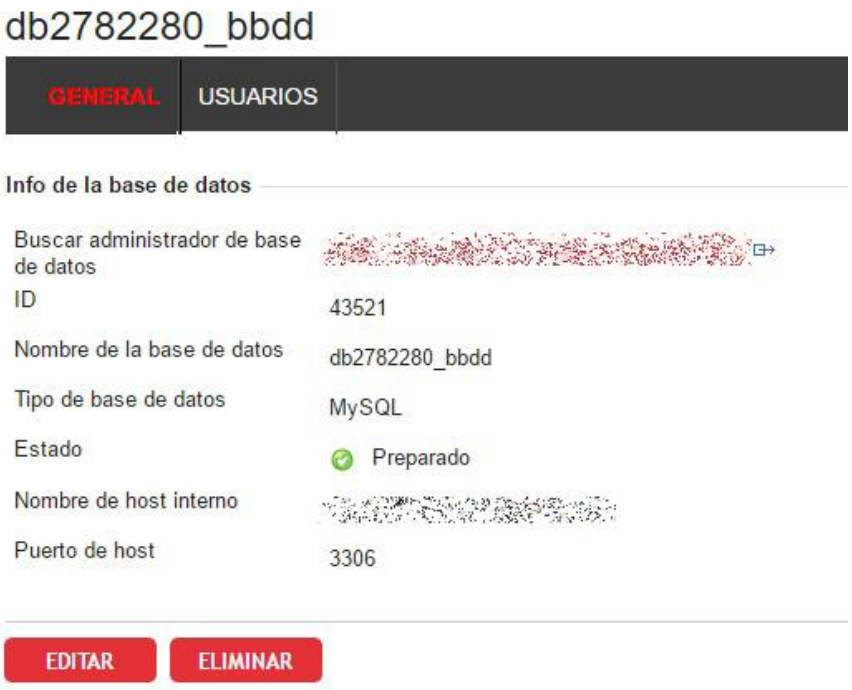
que es donde se almacenan los archivos del tema. El proceso sería el mismo, descargarnos el tema que utilizamos, borrar el que tengamos subido actualmente en nuestro FTP y subir de nuevo el tema.

También sería interesante revisar la carpeta "**wp-content/uploads**" y sus subcarpetas en busca de archivos PHP que pudieran aparecer. En esta ubicación es donde se suben todo los archivos de imágenes, pdf... que utilizamos en nuestro sitio y donde no debería aparecer ningún archivo de programación, únicamente un "**index.php**" vacío sin nada en su interior.

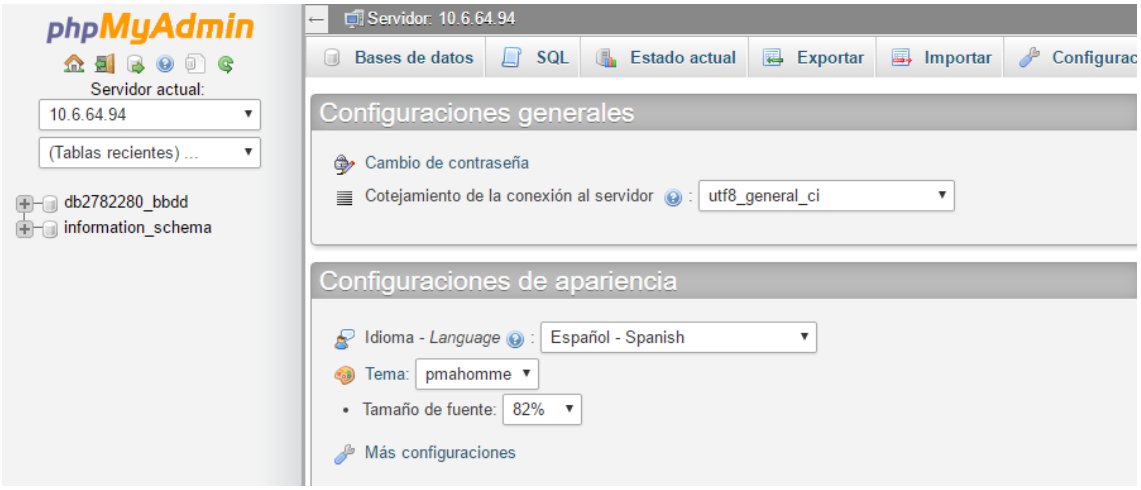
Restaurar copia de seguridad de la base de datos

Este último paso sólo sería necesario hacerlo si realmente nuestra base de datos se ha visto alterada, aunque no es lo más normal pero se puede dar la situación. Para llevarlo a cabo, es muy importante contar con algún backup de nuestro sitio, o bien que tengamos contratado algún tipo de servicio de copia de seguridad con nuestro proveedor de hosting.

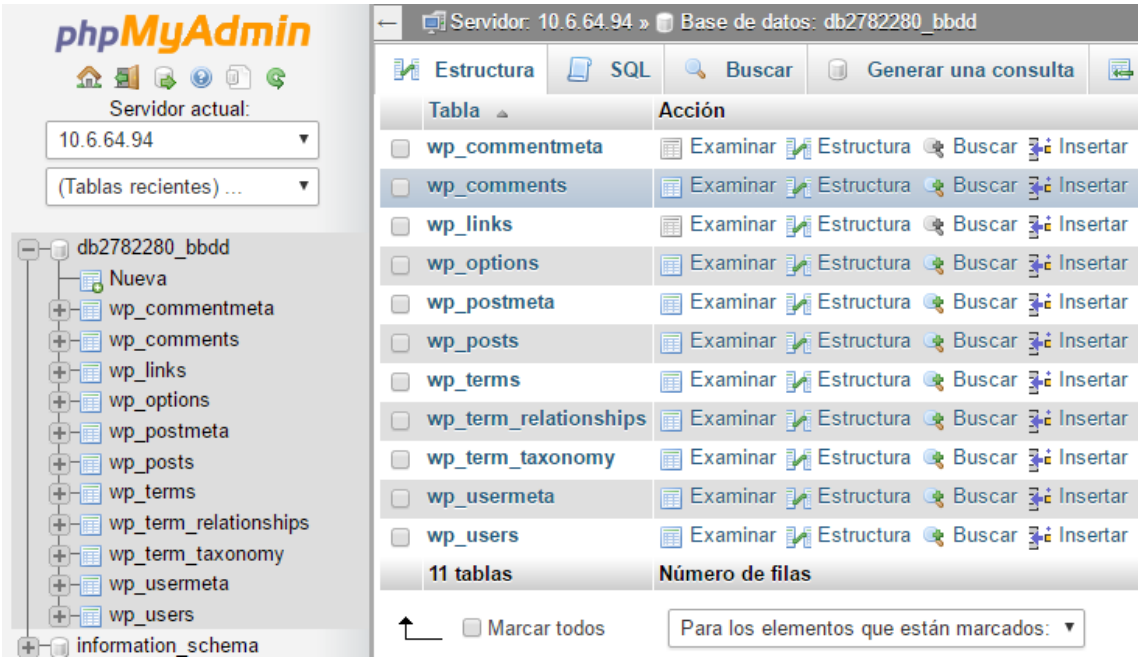
Para llevar a cabo este proceso de restauración de la base de datos, lo primero que deberemos hacer es entrar al phpMyAdmin de nuestro hosting. Para llegar a esta herramienta, debemos seguir los pasos explicados en el punto de cambio de contraseña de la base de datos hasta haber seleccionado la base de datos sobre la que queremos trabajar. Deberemos ver algo parecido a lo que se muestra en la imagen siguiente.



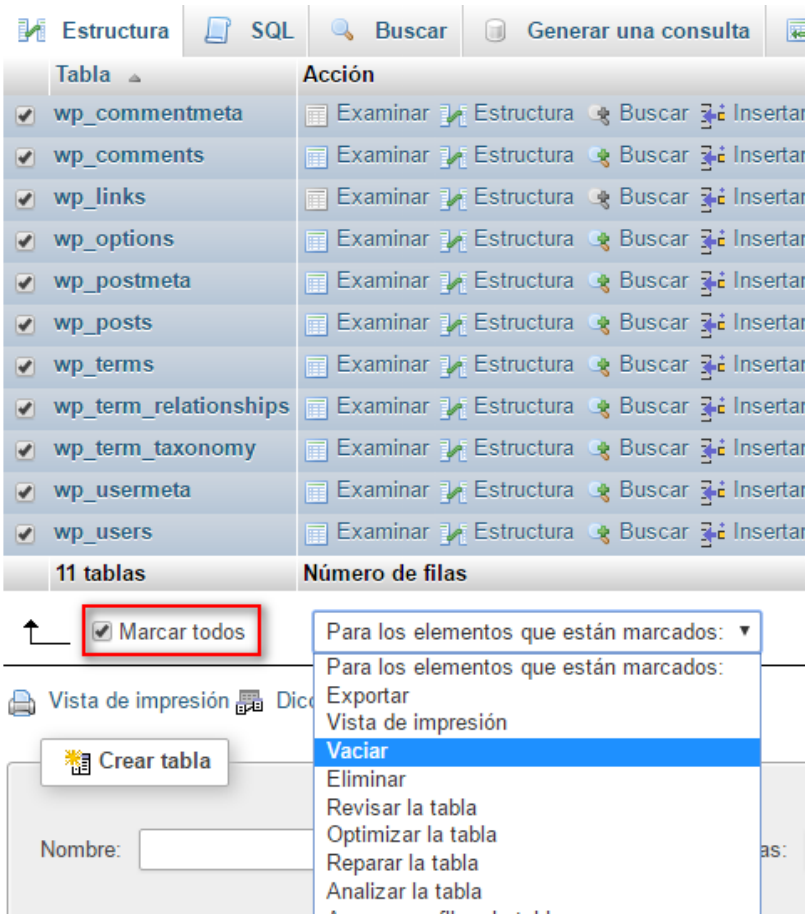
Para acceder al phpMyAdmin, pulsaremos sobre el enlace de la sección "**Buscar administrador de base de datos**".



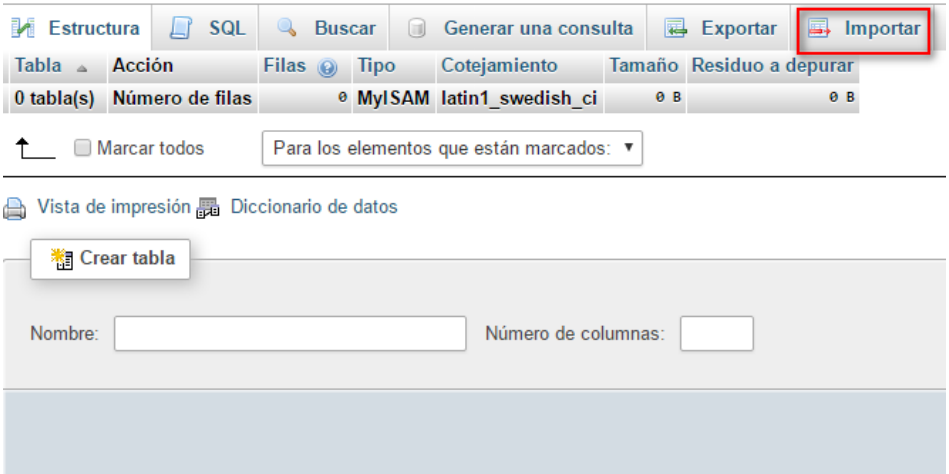
En el menú de la izquierda, pulsaremos sobre el nombre de la base de datos, en nuestro ejemplo "**db2782280_bbdd**" lo que hará que se nos muestre el listado de tablas que forman parte de la base de datos.



Tendremos que eliminar todas las tablas, para ello marcaremos la casilla donde pone "**Marcar todos**" y en el menú desplegable seleccionaremos la opción "**Vaciar**".



Una vez que han sido borradas, lo que tocaría ahora sería subir nuestra copia. Para ello pulsaremos sobre la opción "**Importar**" que aparece en el menú superior.



En la siguiente pantalla, pulsaremos sobre el botón "**Seleccionar archivo**" y buscaremos en nuestro equipo nuestra copia de la base de datos que queremos restaurar.

Por último, quedará pulsar sobre el botón "**Continuar**" que aparece al final de esa pantalla para terminar con todo el proceso y asegurarnos de que nuestro WordPress está limpio de cualquier tipo de amenazas.

Si alguna vez sufrimos algún tipo de hackeo en nuestra web desarrollada con WordPress, sólo deberemos seguir los pasos vistos en este libro blanco para poder solucionar el problema.