

1. INTRODUCCIÓN.

La imagen institucional viene representada de varias formas y una de ellas son los sitios web de la institución, dónde se publican información relativas a las actividades, misión, visión, programas, proyectos y en general información orientada a la prestación de servicios a la ciudadanía.

Este hecho hace que los sitios webs se conviertan en un activo importante para la institución ya que en ella se refleja la imagen institucional y es un referente de información y medio de acceso a otros recursos que provee la institución a la ciudadanía.

Todo sitio web está expuesto a sufrir ataques informáticos que derivan en incidentes de seguridad producto de errores de configuración, vulnerabilidades que se descubren con el paso del tiempo en componentes que no fueron actualizados, uso de contraseñas débiles y otras relacionadas a la administración.

El Centro de Gestión de Incidentes Informáticos ha atendido incidentes de seguridad en sitios web gubernamentales de las que se han identificado errores en la administración que han derivado en determinadas circunstancias en la defacement (Defacement) de la página principal o páginas secundarias que inciden en el daño a la imagen institucional, entre las causas más recurrentes están el uso de contraseñas débiles, uso de componentes con vulnerabilidades para los cuales existen exploits públicos como prueba de concepto, funcionalidades innecesarias u obsoletas expuestas como ser formularios para subir archivos sin restricción por tipo de archivo.

A raíz de estos problemas se elabora el presente documento que expone las prácticas y guías de seguridad que deben ser aplicados en la administración segura de sitios web con la finalidad de minimizar el riesgo de sufrir incidentes de seguridad.

2. ATENCIÓN DE ALERTAS DE SEGURIDAD

- Atender con prioridad las alertas de seguridad y vulnerabilidades reportadas por la AGETIC.
- Reportar los incidentes en un plazo no mayor a veinticuatro (24) horas de conocido el hecho al CGII para contener, corregir, recuperar los servicios afectados y/o alertar al resto de las entidades del sector público, conforme a los procedimientos establecidos por el CGII.

3. SEGURIDAD DEL SOFTWARE DE SERVIDOR WEB

3.1. Deshabilitar el listado de directorio

- El listado de directorios, conocido como "index of", es producido cuando se envía una solicitud de un directorio al servidor.
- Tener activado el listado de directorio puede permitir a personas no autorizadas acceder a carpetas y archivos de forma directa, los cuales podrían contener información sensible.
- Para deshabilitar el listado de directorios se recomienda consultar la guía del Anexo 1.

3.2. Deshabilitar PHPinfo

PHPinfo es la exposición de información de configuración de PHP, el cual permite la divulgación de información potencialmente confidencial a un atacante a través de una URL.

- Para deshabilitar la exposición de información de PHP consultar la guía del Anexo 1.

3.3. Ejecutar actualizaciones de seguridad

Las actualizaciones son modificaciones realizadas sobre los sistemas operativos o aplicaciones y cuya misión es mejorar tanto aspectos de funcionalidad como de seguridad.

Por lo tanto, para preservar la funcionalidad segura del servidor web, es importante actualizar el software periódicamente considerando lo siguiente:

- Tener un ambiente de pruebas igual al servidor en producción para realizar las actualizaciones de seguridad, en caso de no tener ningún problema, proceder a la actualización en producción.
- Aplicar la actualización en el corto plazo.
- Obtener las actualizaciones de seguridad de fuentes oficiales.

Se recomienda suscribirse a canales de seguridad oficiales del software, por ejemplo:

- Para apache: <http://httpd.apache.org/lists.html#http-announce>
- Para productos de Microsoft: <https://msrc.microsoft.com/update-guide>

- Para NGINX: http://nginx.org/en/security_advisories.html

3.4. Configurar el registro logs

- Una de las configuraciones importantes en el servidor web es el registro de logs que permitirá contar con datos de actividad del sitio web y el rendimiento del servidor, así como cualquier otro problema que haya podido ocurrir durante su operación.
- Los registros son importantes para determinar posibles causas de un incidente informático.
- Para ver una guía detallada de la configuración de registros de logs del servidor web consultar la guía del Anexo 1.

3.5. Deshabilitar el despliegue de errores

- Es importante deshabilitar el despliegue de errores en el servidor web, debido a que cualquier mensaje de error mostrado al usuario final incluye no sólo la información del servidor, sino también un mensaje de excepción detallada, pero también el código fuente real de la página donde se produjo el error.
- Para deshabilitar el despliegue de errores consultar el Anexo 1.

4. SEGURIDAD DEL SISTEMA OPERATIVO

Se deben tomar en cuenta las siguientes prácticas de seguridad a nivel de sistema operativo para prevenir potenciales incidentes de seguridad informática que afecten a servicios que se ejecutan en el sistema.

4.1. Asegurar el control de acceso

- Las cuentas de usuarios para el acceso al sistema no deben ser compartidas, ya que eliminan la responsabilidad, aumentan el riesgo y hacen que la auditoría de la actividad del usuario sea imposible.
- Cada usuario debe tener una cuenta individual que lo identifique y esté relacionada a sus datos personales.

- Se deben establecer privilegios a cada cuenta de usuario de acuerdo a sus funciones.
- Los privilegios asignados a cuentas de usuario se deben eliminar cuando ya no sean necesarios.
- Verificar periódicamente los usuarios activos e inhabilitar aquellos que no correspondan.
- Si la política interna de la institución permite el acceso remoto, la misma debe estar sobre un canal seguro, por ejemplo SSH con par de claves con contraseña robusta.

4.2. Ejecutar actualizaciones de seguridad

- Se deben revisar las actualizaciones del sistema operativo publicadas en sus repositorios oficiales de manera constante, con especial atención de aquellas con riesgo de seguridad crítica.
- Antes de ejecutar la actualización en un sistema en producción, se recomienda probar en un ambiente idéntico para verificar que la funcionalidad no se vea afectada.

4.3. Deshabilitar servicios innecesarios

- Se recomienda que en el sistema operativo ejecute sólo servicios que tienen relación con el funcionamiento del sitio web y deshabilitar servicios innecesarios.
- Se recomienda no habilitar recursos compartidos y servicios de escritorio remoto.

5. SEGURIDAD DE LA BASE DE DATOS

Las bases de datos tienen amenazas que los administradores deben comprender y mitigar. A continuación se presentan buenas prácticas para robustecer la seguridad.

5.1. Proteger el servicio de base de datos

- El servicio de la base de datos debe estar protegido con reglas de control de acceso para denegar conexiones no autorizadas.

- No publicar el servicio de la base de datos hacia internet.

5.2. Separar tareas de administración

- La separación de funciones es una buena práctica de seguridad donde las tareas de administración deben ser divididas entre varios usuarios y no debe existir un usuario con control total de la base de datos.
- La división de tareas de administración hace que sea menos probable que los usuarios abusen de sus privilegios, y reduce la superficie de ataques de cuentas de usuario comprometidas.

5.3. Gestionar cuentas de usuarios

- Las cuentas de usuarios no deben ser compartidas, ya que eliminan la responsabilidad, aumentan el riesgo y hacen que la auditoría de la actividad del usuario sea imposible.
- Cada usuario debe tener una cuenta individual que lo identifique y esté relacionada a sus datos personales.
- Se deben establecer privilegios a cada cuenta de usuario delimitando su relación con los objetos de la base de datos.
- La cuenta de superusuario de la base de datos no debe ser utilizada para la conexión desde aplicaciones o sistemas informáticos.
- Los privilegios asignados a cuentas de usuario se deben eliminar cuando ya no sean necesarios.
- Verificar periódicamente los usuarios activos e inhabilitar aquellos que no correspondan.
- Se debe establecer reglas de registro de logs para la conexión de los usuarios.

5.4. Configurar registros de auditoría

- Se debe capturar el registro de acciones realizadas por las cuentas de usuario, incluyendo acciones como "CREAR USUARIO", "CREAR TABLA",

“CREAR BASE DE DATOS” entre otros, junto con datos de conexión como la dirección IP, fecha y hora del evento.

- Los registros de auditoría permitirán identificar problemas de integridad de datos y acciones ejecutadas en la base de datos por usuarios.

5.5. Ejecutar actualizaciones de seguridad

Se debe revisar las actualizaciones del motor de la base de datos publicadas en sus repositorios oficiales de manera constante, con especial atención de aquellas con riesgo de seguridad crítica.

6. SEGURIDAD DE SISTEMAS DE GESTIÓN DE CONTENIDOS (CMS)

CMS - Content Management System es una herramienta que permite a un editor crear, actualizar, clasificar y publicar cualquier tipo de información en una página web.

Para mejorar la seguridad del sitio web implementado bajo un CMS se han elaborado las siguientes guías de seguridad que incluyen buenas prácticas para una administración segura:

- Anexo 2: Joomla
- Anexo 3: Drupal
- Anexo 4: Wordpress

Adicionalmente se recomienda las siguientes prácticas de seguridad generales:

- Usar contraseñas robustas con alta complejidad.
- Cada usuario debe tener una cuenta individual que lo identifique y esté relacionada a sus datos personales.
- Evitar usar nombres de usuario habituales como "admin" o "administrador".
- Se deben establecer privilegios a cada cuenta de usuario de acuerdo a sus funciones.
- Realizar copias de seguridad de los archivos del sitio web y de la base de datos y almacenarlos en una ubicación distinta al servidor. La periodicidad

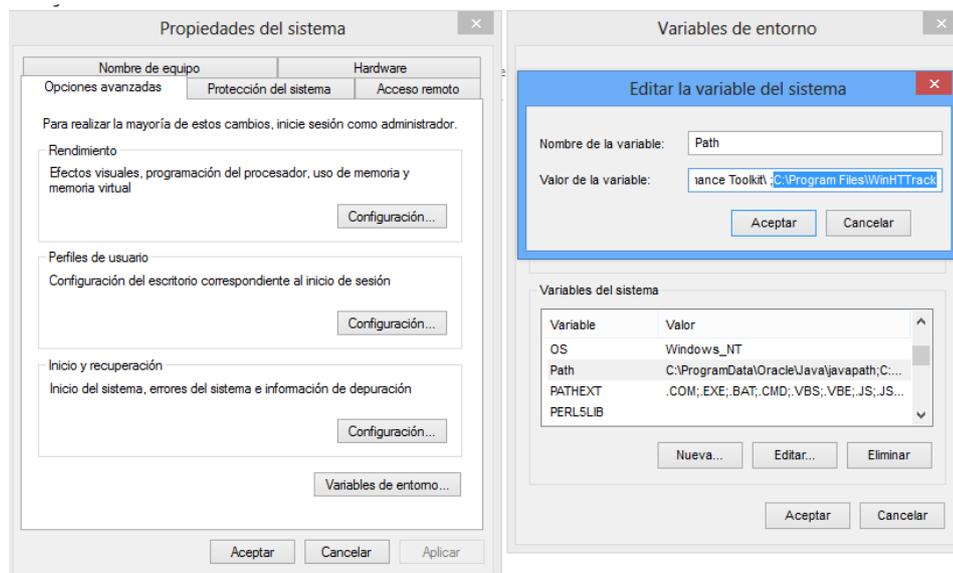
debe estar de acuerdo a las políticas internas o la frecuencia de cambios en el contenido.

Revisar el anexo 5 para las medidas de contención en caso de un incidente de seguridad en el sitio web, éstas deberán ser aplicadas.

6. COPIA ESTÁTICA DEL SITIO WEB

Se recomienda generar una copia estática reciente del sitio web para que pueda ser usada en caso de un incidente de seguridad. Para realizar esta tarea se establecen los siguientes pasos:

- Descargar Httrack <https://www.httrack.com/page/2/en/index.html> y después de instalar modificar la variable de entorno PATH, agregar la ruta del Httrack "C:\Program Files\WinHTTrack":



- Ejecutar el comando para crear la copia estática del sitio web:

```
httrack https://[dominio.gob.bo]/ -r6
```

```
E:\>cd web
E:\web>httrack https://www.mingobierno.gob.bo/ -r6
Mirror launched on Mon, 11 Jan 2021 13:39:26 by HTTrack Website Copier/3.49-2+ht
sswf+htsjava [XR&CO'2014]
mirroring https://www.mingobierno.gob.bo/ with the wizard help..
Done.
Thanks for using HTTrack!
```

Se recomienda realizar estas copias estáticas del sitio web cada vez que tenga un cambio significativo en su contenido.

7. MONITOREO DE SERVICIOS

- Se debe contar con un sistema de monitoreo y/o implementar en caso que no exista, para poder verificar la disponibilidad y cambios no controlados del Sistema Operativo, Software de servidor web, Base de datos y Sistema de gestión de contenidos. Esta tarea es fundamental para la detección oportuna de actividades maliciosas.
- Verificar que el sistema de monitoreo esté en funcionamiento y control continuo por parte del departamento técnico.

8. ANEXOS

Anexo	Código	Descripción del Anexo
1	ANEXO 1	Guía de seguridad para el software del servidor web
2	ANEXO 2	Guía de buenas prácticas de seguridad en Joomla
3	ANEXO 3	Guía de buenas prácticas de seguridad en Drupal
4	ANEXO 4	Guía de buenas prácticas de seguridad en Wordpress
5	ANEXO 5	Medidas de contención en caso de desfiguraciones web

9. CONTROL DE CAMBIOS

Versión	Fecha	Descripción de las modificaciones
1	12/01/2021	Versión nueva del Documento.

ANEXO 1

1. INTRODUCCIÓN

El software del servidor web es propenso a ataques producto de vulnerabilidades descubiertas o configuraciones por defecto que se hayan dejado con la instalación. Por estas razones se presentan las prácticas de seguridad que debemos seguir para contar con un software de servidor web más seguro.

2. SOLUCIONES DE VULNERABILIDADES COMUNES DEL SOFTWARE DEL SERVIDOR WEB

Para solucionar las vulnerabilidades más comunes de software del servidor web, se recomienda las siguientes prácticas de seguridad.

2.1. DESHABILITAR EL LISTADO DE DIRECTORIOS (INDEX OF)

Las siguientes configuraciones fueron realizadas en Apache 2.4 y usuario con privilegios sudo. Dependiendo del caso se puede elegir una de las siguientes opciones para deshabilitar el listado de directorio.



2.1.1. Deshabilitar el módulo autoindex

- Deshabilitar la funcionalidad autoindex a nivel global:

```
$ sudo a2dismod autoindex
```

- Después de ejecutar el comando, se mostrará el mensaje de advertencia el cual se tiene que responder con la siguiente frase:

```
To continue type in the phrase 'Yes, do as I say!' or retry by passing '-f': Yes, do as I say!
```

- Reiniciar el servidor.

```
$ sudo systemctl restart apache2.service
```

2.1.2. Deshabilitar por archivo de configuración del sitio

Este método deshabilita esta funcionalidad solo para el sitio en cuestión. Por ejemplo si se tiene el sitio `www.sitio-de-prueba.com` con el archivo de configuración (virtualhost) ``sitio-de-prueba.conf``.

- Agregar en el archivo la siguiente directiva:

```
<VirtualHost *:80>
```

```
.....
```

```
<Directory /var/www/sitio-de-prueba>  
    Options -Indexes  
</Directory>
```

```
.....
```

```
</VirtualHost>
```

- Guardar y recargar la configuración.

```
$ sudo systemctl reload apache2.service
```

2.1.3. Deshabilitar a través del archivo .htaccess

Es una alternativa similar al archivo de configuración.

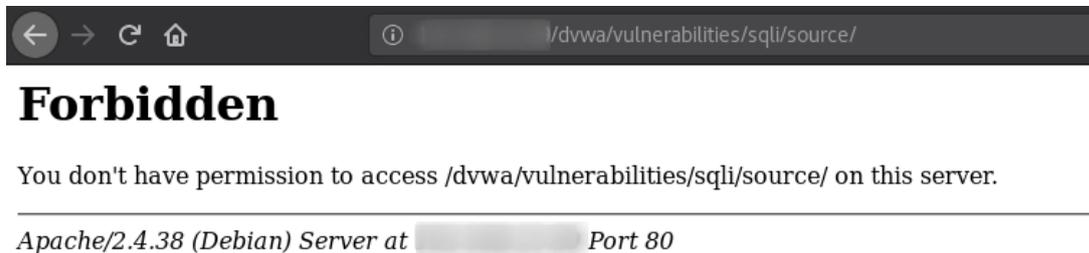
- Agregar en el archivo `.htaccess`:

Options -Indexes

- Guardar el archivo y reiniciar el servidor.

\$ sudo systemctl restart apache2.service

El resultado de aplicar una de las configuraciones anteriores, será la restricción de listar archivos y carpetas.



3. DESHABILITAR EL DESPLIEGUE DE VERSIONES

Por defecto apache despliega su versión utilizada cuando la solicitud a una página del sitio web responde con código de errores 40X.

Not Found

The requested URL was not found on this server.

Apache/2.4.46 (Debian) Server at localhost Port 80

- Para evitar desplegar la versión de apache, se debe editar el archivo de configuración `/etc/apache2/apache2.conf` y agregar las siguientes directivas:

ServerTokens Prod
ServerSignature Off

- El resultado será el siguiente:

Not Found

The requested URL was not found on this server.

4. DESHABILITAR PHPINFO

Estas soluciones fueron probadas en PHP versión 7.2.

- Acceder al archivo `/etc/php/7.2/apache2/php.ini` y añadir el siguiente comando:

```
expose_php = Off
```

- Una opción alternativa es deshabilitar mediante el comando “`disable_funtions`”, para ello se puede añadir “`phpinfo`”:

```
disable_functions = ..., phpinfo
```

5. CONFIGURAR REGISTRO DE LOGS

5.1. HABILITAR EL REGISTRO DE LOGS EN APACHE

En el archivo de configuración de apache (`/etc/apache2/sites-enabled/{subdominio}.conf`), agregar las siguientes directivas:

```
ErrorLog ${APACHE_LOG_DIR}/error.log
```

```
CustomLog ${APACHE_LOG_DIR}/access.log combined
```

Se aconseja tener un `error.log` diferente por sitio web administrado.

5.2. HABILITAR EL REGISTRO DE LOGS EN PHP Y DESHABILITAR EL DESPLIEGUE DE ERRORES

- Editar el archivo `php.ini` para habilitar el registro de logs:

```
error_reporting = E_ALL | E_STRICT;
```

```
log_errors = On;
```

```
display_errors = Off;
```

```
error_log = /var/log/apache2/error_log;
```

6. CONTROL DE CAMBIOS.

Versión	Fecha	Descripción de las modificaciones
1	12/01/2021	Versión nueva del Documento.

ANEXO 2

1. INTRODUCCIÓN

Joomla es un sistema de gestión de contenido (CMS, Content Management System), que permite crear sitios web, su popularidad ha logrado que resulte muy atractivo para los “ciberatacantes”, con el fin de explotar vulnerabilidades.

2. ASEGURANDO JOOMLA

Para mitigar el riesgo de ataques a Joomla, se recomienda las siguientes buenas prácticas de seguridad.

2.1. VERIFICAR PARCHES DE SEGURIDAD

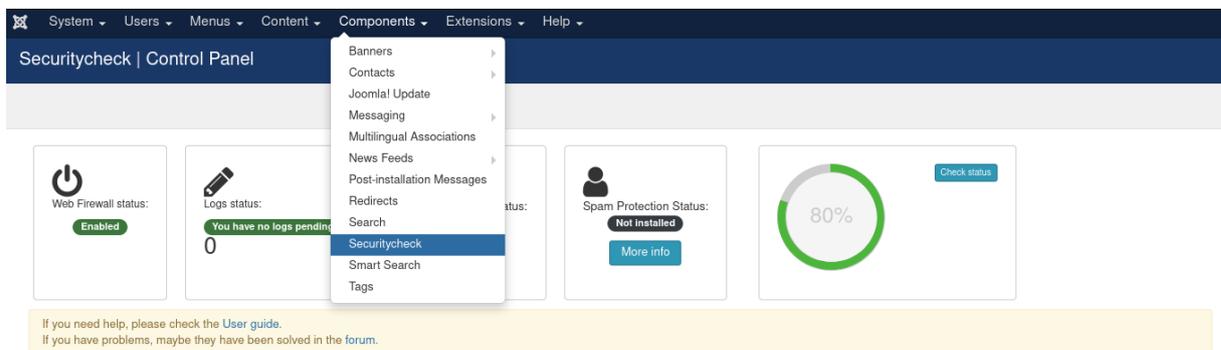
Comprobar regularmente si hay nuevos parches de seguridad disponibles para solucionar vulnerabilidades de seguridad e instalarlos, para ello existe el complemento “Plugin Securitycheck”.

A continuación se describe los pasos para el uso del Plugin Securitycheck:

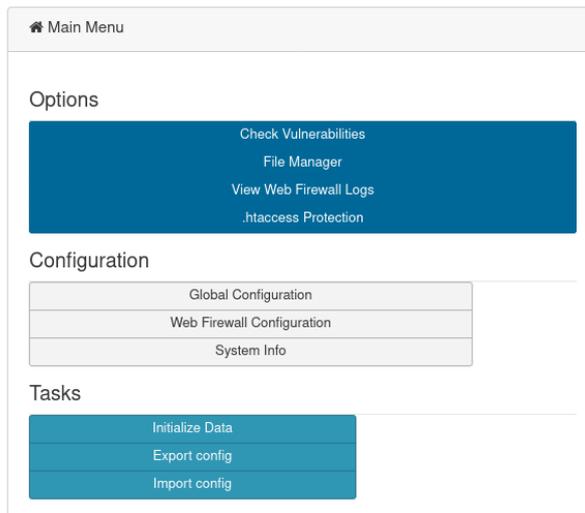
- Instalar el plugin siguiendo el enlace:

<https://extensions.joomla.org/extension/securitycheck/>

- Una vez instalado ir al menú Components → Securitycheck



- Verificar vulnerabilidades en los complementos.



- La columna de “Known vulnerabilities” de todos los complementos listados debe estar en estado “No”.

Color code			
—	Unknown vulnerabilities	—	There is a vulnerability for this extension but Joomla version affected is not specified
—		—	Vulnerable extension
Updated date Nov 23 2020			
Id	Product	Type	Known vulnerabilities
1	Joomla!	Core	No
2	com_actionlogs	Component	No
3	com_admin	Component	No
4	com_ajax	Component	No
5	com_associations	Component	No
6	com_banners	Component	No
7	com_cache	Component	No
8	com_categories	Component	No

Se recomienda suscribirse a canales de seguridad oficiales de Joomla, por ejemplo:

- https://docs.joomla.org/Security_hotfixes_for_Joomla_EOL_versions/es
- <https://developer.joomla.org/security-centre.html>

Se recomienda la actualización de Joomla! a una versión con soporte.

También se recomienda que se considere actualizar las tecnologías complementarias para el uso de Joomla! como es php, mysql y el sistema operativo, tomando en cuenta que estas actualizaciones sean compatibles con la versión de Joomla! que utiliza, aplicando estos cambios primero en un entorno de pruebas.

2.2. ASEGURAR NOMBRE DE USUARIO Y CONTRASEÑA

- No utilizar el nombre de usuario admin predeterminado.
- Utilizar una contraseña robusta, por ejemplo, que contenga mayúsculas, minúsculas, cifras y caracteres especiales.

2.3. PROTEGER EL ARCHIVO DE CONFIGURACIÓN

Proteger el archivo `configuration.php`, que se encuentra en el directorio raíz de la instalación de Joomla! con apache, para impedir que se pueda editar.

- Activar el módulo htaccess:

```
$ sudo nano /etc/apache2/apache2.conf
```

- Buscar las Líneas:

```
<Directory /var/www/>  
  
    Options Indexes FollowSymLinks  
  
    AllowOverride None  
  
    Require all granted  
  
</Directory>
```

- Cambiar a:

```
<Directory /var/www/>  
  
    Options FollowSymLinks  
  
    AllowOverride All  
  
    Require all granted  
  
</Directory>
```

- Reiniciar servidor de apache:

```
$ sudo service apache2 restart
```

- Añadir al archivo `.htaccess`:

```
<FilesMatch "configuration.php">  
    Require all denied  
</FilesMatch>
```

2.4. PROTEGER EL ACCESO AL PANEL DE ADMINISTRADOR

Por defecto el panel de administrador de Joomla! se encuentra en la url `/administrator` de la página. Para evitar que personas no autorizadas intenten acceder al panel de administración seguir los siguientes pasos:

- Crear un directorio que únicamente conozcan los usuarios administradores del sitio web (debe recordar que el directorio miotroadm es solo un ejemplo).

```
$ sudo mkdir miotroadm
```

- Crear un archivo index.php para redireccionar al panel de administración, cambiar la cookie “admin_cookie_code” por una más larga y difícil de adivinar.

```
$ cd miotroadm  
$ sudo nano index.php
```

```
<?php  
$admin_cookie_code="1254789654258"  
setcookie("JoomlaAdminSession",$admin_cookie_code,0,"/");  
header("Location: ../administrator/index.php");  
?>
```

- Adicionar al principio del index.php del directorio “administrator” que solicite la cookie, caso contrario devolver al index.php

```
$ sudo nano administrator/index.php  
if($_COOKIE['JoomlaAdminSession']!="1254789654258")  
{  
setcookie('JoomlaAdminSession', null, -1, '/');  
header("Location: ../index.php");  
}
```

- Añadir al final en el index.php del panel de administración el siguiente comando para eliminar la cookie creada.

```
$ sudo nano index.php  
  
if ($_COOKIE['JoomlaAdminSession']!="")  
{  
setcookie('JoomlaAdminSession', null, -1, '/');  
}
```

2.5. OCULTAR LA VERSIÓN DE Joomla!

Seguir los siguientes pasos para ocultar la versión de Joomla!:

- Borrar la carpeta “installation” ubicada en el directorio raíz de la instalación de Joomla!.

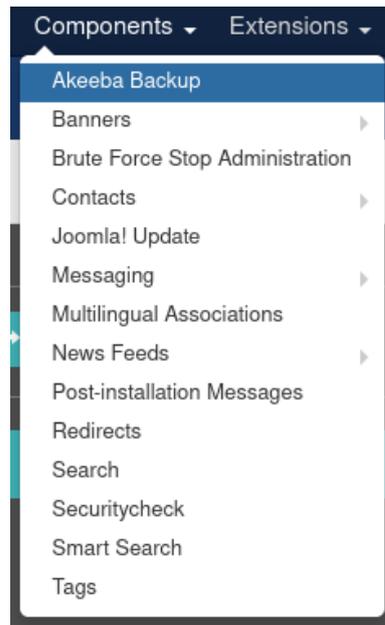
2.6. REALIZAR COPIA DE SEGURIDAD

Para realizar la copia de seguridad de Joomla! puede utilizar el plugin Akeeba Backup.

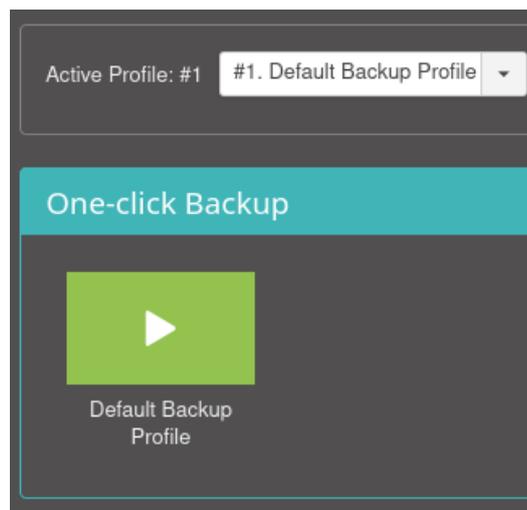
- Instalar el plugin siguiendo el enlace:

Enlace: <https://extensions.joomla.org/extension/akeeba-backup/>

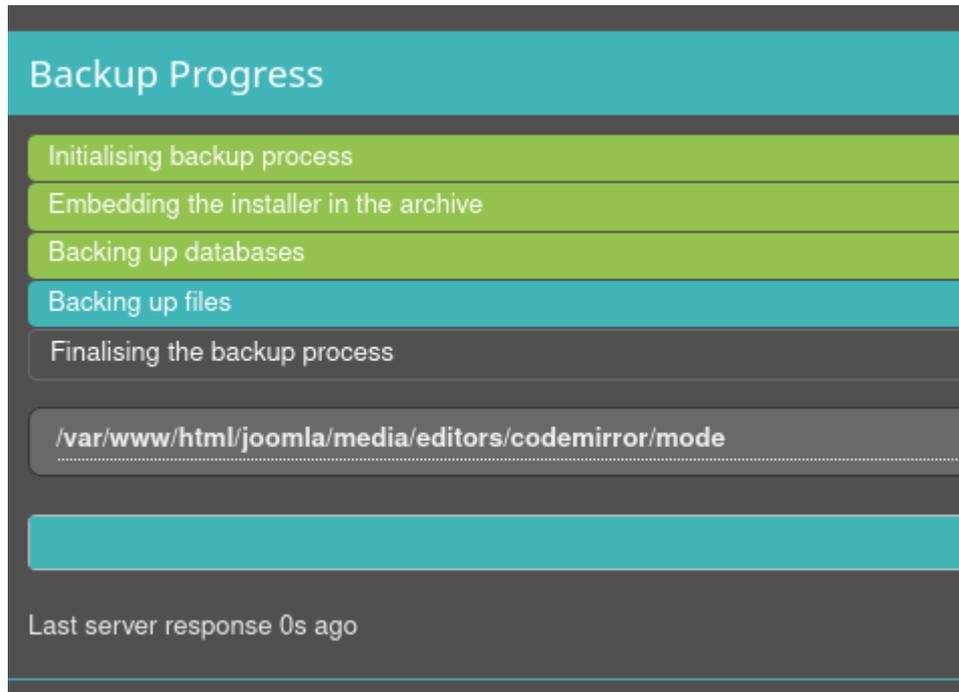
- Una vez instalado ir al menú Components → Akeeba Backup



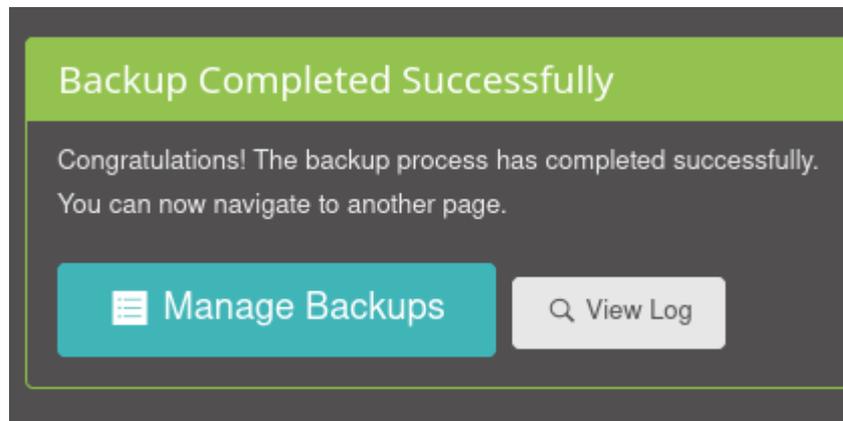
- Hacer clic en “Default Backup Profile” para sacar la copia de seguridad de Joomla!.



- Se despliega el proceso de backup



- Los backups se muestran en Manage Backups.



- Se muestra el listado de backups generados

ID	Frozen	Description	Profile	Duration	Status	Size	Manage & Download
6	🔒	Backup taken on Tuesday, 12 January 2021 20:55 UTC 2021-01-12 UTC	#1. Default Backup Profile Full site backup	00:00:07	✅	15.84 MB	Download View Log
5	🔒	Backup taken on Tuesday, 12 January 2021 20:55 UTC 2021-01-12 UTC	#1. Default Backup Profile Full site backup	00:00:06	✅	15.84 MB	Download View Log
4	🔒	Backup taken on Monday, 11 January 2021 17:16 UTC 2021-01-11 UTC	#1. Default Backup Profile Full site backup	00:00:06	✅	15.84 MB	Download View Log
2	🔒	Backup taken on Monday, 11 January 2021 17:13 UTC 2021-01-11 UTC	#1. Default Backup Profile Full site backup	00:00:06	❌	15.84 MB	View Log
1	🔒	Backup taken on Monday, 11 January 2021 17:12 UTC 2021-01-11 UTC	#1. Default Backup Profile Full site backup	00:00:06	❌	15.84 MB	View Log

- Establecer copias de respaldo cada cierto tiempo de acuerdo a la políticas de seguridad.

3. CONTROL DE CAMBIOS.

Versión	Fecha	Descripción de las modificaciones
1	12/01/2021	Versión nueva del Documento.

ANEXO 3

1. INTRODUCCIÓN

Todo sistema de gestión de contenidos está propenso a ataques producto de vulnerabilidades descubiertas o configuraciones por defecto que se hayan dejado con la instalación. Por estas razones se presentan las prácticas de seguridad que debemos seguir para contar con un sitio web más seguro bajo Drupal.

2. ASEGURANDO DRUPAL

Para mitigar el riesgo de ataques a Drupal, recomendamos aplicar las siguientes buenas prácticas de seguridad.

2.1. ACTIVAR NOTIFICACIONES DE ACTUALIZACIONES DE SEGURIDAD

- Habilitar en la administración de Drupal notificaciones al correo electrónico sobre actualizaciones más recientes de seguridad de módulos contribuidos y del core.

Administrar > Informes > Actualizaciones disponibles, pestaña "configuración"



Actualice configuraciones de Administración ☆

Lista Actualizar Configuración

Inicio » Administración » Informes » Actualizaciones disponibles

Comprobar si hay actualizaciones

Diariamente
 Semanalmente

Seleccionar con qué frecuencia quiere comprobar automáticamente si hay nuevas versiones de los módulos y temas gráficos que tiene instalados.

Verificar actualizaciones o módulos y temas desinstalados.

Direcciones de correo electrónico a las que notificar las actualizaciones disponibles

Cada vez que su sitio compruebe si hay nuevas actualizaciones disponibles y encuentre nuevas versiones, puede notificar a una lista de usuarios a través de correo electrónico. Coloque cada dirección en una línea separada. Si lo deja en blanco, no se enviará ningún correo.

Umbral de notificaciones por correo electrónico

Todas las versiones más recientes
 Sólo actualizaciones de seguridad

Puede elegir enviar emails solo si está disponible una actualización de seguridad o ser notificados sobre nuevas versiones. Si hay actualizaciones disponibles de núcleo de Drupal o de cualquiera de los módulos y temas instalados, su sitio mostrará siempre un mensaje en la página de [informe de estado](#) y también mostrará un mensaje de error en las páginas de administración si hay una actualización de seguridad.

Guardar configuración

- Revisar de forma periódica el informe de estado de Drupal donde se muestra el estado de cada módulo y del core sobre actualizaciones funcionales y de

seguridad. Aquellos módulos que ya no cuentan con mantenimiento desde sus repositorios de origen se deben desactivar o migrar a uno con soporte.

Administración > Informes

Errores encontrados

**✘ ESTADO DE ACTUALIZACIÓN DE
 MÓDULOS Y TEMAS GRÁFICOS**

Versión sin mantenimiento

La versión instalada de al menos uno de los módulos o temas ya no tiene mantenimiento. Se le recomienda vivamente actualizarlo o desactivarlo. Consulte la página del proyecto para más detalles. Consulte la página [actualizaciones disponibles](#) para más información e instalar las actualizaciones pendientes.

- Se recomienda seguir la cuenta de seguridad de Drupal en Twitter (@drupalsecurity) para estar al pendiente de las actualizaciones.

2.2. INSTALAR ACTUALIZACIONES DE SEGURIDAD

Como buena práctica de seguridad se debe tener un ambiente de pruebas donde se realicen las actualizaciones para verificar el correcto funcionamiento del sitio web antes de su pase a producción.

- Revisar el panel de actualizaciones disponibles.

Lista Actualizar Configuración

[Inicio](#) » [Administración](#) » [Informes](#) » [Actualizaciones disponibles](#)

Última comprobación: hace 56 minutos 2 segundos ([Comprobar manualmente](#))

La actualización de módulos y temas requiere **acceso de FTP** a su servidor. Ver [Extendiendo Drupal 8](#) para otros métodos de actualización.

<input type="checkbox"/> NOMBRE	VERSIÓN INSTALADA	VERSIÓN RECOMENDADA
<input type="checkbox"/> Metatag	8.x-1.13	8.x-1.15 (Notas de la versión)
<input type="checkbox"/> Token	8.x-1.7	8.x-1.9 (Notas de la versión)
<input type="checkbox"/> Webform	8.x-5.16	8.x-5.23 (Notas de la versión)

[Descargar estas actualizaciones](#)

Hacen falta actualizaciones manuales

Las actualizaciones automáticas del núcleo de Drupal no están soportadas en este momento.

NOMBRE	VERSIÓN INSTALADA	VERSIÓN RECOMENDADA
Drupal core	8.9.10	8.9.12 (Notas de la versión)

- Replicar el ambiente de producción al ambiente de pruebas.
- Proceder con la actualización del core y módulos en el ambiente de pruebas.
- Verificar que las actualizaciones se hayan aplicado correctamente.

- Realizar las pruebas funcionales.
- En caso de que todo esté correcto, replicar el ambiente de pruebas a producción en un horario donde no afecte a los usuarios.

2.3. GESTIONAR USUARIOS

- En Drupal se encuentra habilitada por defecto la opción de creación de cuentas por usuarios anónimos. Una buena práctica de seguridad es deshabilitar esta opción.

Administración > Configuración > Usuarios > Configuración de la cuenta

▼ **CREACIÓN Y CANCELACIÓN DE CUENTAS**

¿Quién puede crear cuentas?

Sólo los administradores

Visitantes

Visitantes, pero es necesaria la aprobación de los administradores

Solicitar verificación por correo electrónico cuando un visitante crea una cuenta
Se requerirán nuevos usuarios para validar su dirección de correo electrónico antes de iniciar sesión en el sitio, y se les asignará una contraseña y sus propias contraseñas durante el registro.

Habilitar el indicador de fortaleza de una contraseña

Al cancelar una cuenta de usuario

Desactivar la cuenta y mantener su contenido.

Desactivar la cuenta y retirar de la publicación su contenido.

Eliminar la cuenta y atribuir todo su contenido al usuario *Anónimo*.

Los usuarios con los [Seleccionar el método para cancelar la cuenta.](#) o [Administrar usuarios permisos](#) pueden anular este método predeterminado.

2.3.1. CONFIGURAR PERMISOS

- Crear nuevos roles de acuerdo a las necesidades funcionales del sitio, estableciendo permisos específicos en módulos instalados.

Administración > Usuarios > Permisos

PERMISO	USUARIO ANÓNIMO	USUARIO AUTENTICADO	ADMINISTRADOR
de contenido.			
Revertir todas las revisiones Para revertir una revisión, también necesita permiso para editar el elemento de contenido.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Ver todas las revisiones Para ver una revisión, también necesita permiso para ver el elemento de contenido.	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Ver contenido publicado	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Ver el contenido propio sin publicar	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Path			
Administrar alias de URL	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

2.4. PROTEGER FORMULARIOS CON CAPTCHA

El captcha previene intentos automatizados de inicios de sesión y envíos masivos (spam) de datos a través de formularios.

- Instalar el módulo captcha (<https://www.drupal.org/project/captcha>) y habilitar.
- Entre las configuraciones se puede establecer el tipo de desafío del captcha matemático, imagen o personalizada con preguntas y respuestas pre establecidas.

▼ **DESAFÍO MATH POR MÓDULO CAPTCHA**

Pregunta matemática *

9 + 0 =

Resuelva este simple problema matemático y escriba la solución; por ejemplo: Para 1+3, escriba 4.
[Diez ejemplos más de esta pregunta.](#)

▼ **DESAFÍO IMAGE POR MÓDULO IMAGE_CAPTCHA**



¿Cuál es el código de la imagen? *

Introduzca los caracteres mostrados en la imagen.
[Diez ejemplos más de esta pregunta.](#)

▼ **DESAFÍO RIDDLER POR MÓDULO RIDDLER**

¿Quién publico la Teoría de la Relatividad?

Responda la pregunta aquí: *

[Diez ejemplos más de esta pregunta.](#)

- Por ejemplo se habilita el captcha en el formulario de inicio de sesión, seleccionando el tipo de desafío.

Edit CAPTCHA point ☆

Inicio » Administración » Configuración » Usuarios » CAPTCHA settings » CAPTCHA configuration

ID del formulario *

Formulario inicio de sesion Nombre de sistema: user_login_form [Editar]

Also works with the base form ID.

Tipo de pregunta

Riddler (del módulo riddler) ▼

- Tipo de pregunta predefinida
- Math (del módulo captcha)
- Image (del módulo image_captcha)
- Riddler (del módulo riddler)**

2.5. UTILIZAR MÓDULOS CON SELLO DE SEGURIDAD

- Sólo utilizar módulos que estén en fase estable y priorizar aquellos con el sello verde del Security Team de Drupal.

Project information

Module categories: [Content Access Control](#), [Security](#), [Spam Prevention](#), [User Access & Authentication](#), [User Management](#)

📊 **287,844** sites report using this module

➡ **Drupal 9 is here!**
Captcha 1.1 is now Drupal 9 compatible.

🛡️ Stable releases for this project are covered by the [security advisory policy](#).
Look for the shield icon below.

Downloads

8.x-1.1 🛡️ released 3 June 2020
Requires Drupal: ^8.8 || ^9
✓ Recommended by the project's maintainer.
↓ [tar.gz \(112.75 KB\)](#) | [zip \(146.67 KB\)](#)

Development version: [8.x-1.x-dev](#) updated 3 Jun 2020 at 04:18 UTC
Testing result: [PHP 7.2 & MySQL 5.5, D8.8.6 26 pass](#) [all results](#)

7.x-1.7 🛡️ released 21 February 2020
Requires Drupal: 7.x
✓ Recommended by the project's maintainer.
↓ [tar.gz \(103.53 KB\)](#) | [zip \(112.94 KB\)](#)

Development version: [7.x-1.x-dev](#) updated 5 Oct 2019 at 18:33 UTC
Testing result: [PHP 5.3 & MySQL 5.5, D7 31 pass](#) [all results](#)

2.6. REVISAR EL REGISTRO RECIENTE DE MENSAJES

Revisar periódicamente el registro de mensajes de Drupal para identificar actividades sospechosas como intentos de inicio de sesión, errores de PHP, envío de formularios y otros datos importantes.

[Inicio](#) » [Administración](#) » [Informes](#)

El módulo Database Logging registra un log de sucesos del sistema en la base de datos de Drupal. Vigile su sitio o depure problemas de página.

Type	Severity
access denied	Emergencia
CAPTCHA	Alerta
cron	Crítico
page not found	Error
php	Advertencia
smtp	Aviso
user	Info
webform	Depurar

TYPE	DATE	MESSAGE	USER
⚠ access denied	- 10:45	Path: /user/register?element_parents=account/mail/%...	Anónimo (no verificado)
⚠ access denied	- 00:14	Path: /node/add. Drupal\Core\Http\Exception\...	Anónimo (no verificado)
⚠ access denied	- 19:05	Path: /es/publicaciones/guia-de-implementacion-de-...	Anónimo (no verificado)
⚠ access denied	- 14:44	Path: /user/register. Drupal\Core\Http\Exception\...	Anónimo (no verificado)
⚠ access denied	- 16:56	Path: /es/publicaciones/guia-de-implementacion-de-...	Anónimo (no verificado)
⚠ access denied	- 15:36	Path: /es/publicaciones/guia-de-implementacion-de-...	Anónimo (no verificado)
⚠ access denied	- 06:43	Path: /es/publicaciones/guia-de-implementacion-de-...	Anónimo (no verificado)
⚠ access denied	- 20:01	Path: /admin/. Drupal\Core\Http\Exception\...	Anónimo (no verificado)

2.7. MÓDULO LOGIN SECURITY

El módulo Login Security permite configurar la forma en la que los usuarios se autentican en el sitio.

- Instalar el módulo login security (https://www.drupal.org/project/login_security) y habilitarlo simultáneamente con el módulo Ban que viene de forma predeterminada con el core de Drupal.
- Configurar en ajustes generales el número de intentos de inicio de sesión fallidos por usuario, host y también la detección de ataques.

Login Security ☆

Inicio » Administración » Configuración » Usuarios

▼ AJUSTES GENERALES

Tiempo de seguimiento

hora(s)

The time window to check for security violations: the time in hours the login information is kept to compute the login a

User

failed attempts

Enter the number of login failures a user is allowed.

After this amount is reached, the user will be blocked, no matter the host attempting to log in. Use this option carefully.

The user blocking protection will not disappear and should be removed manually from the [user management](#) interface

Soft host

failed attempts

Enter the number of login failures a host is allowed.

After this amount is reached, the host will not be able to submit the log in form again, but can still browse the site con

This protection is effective during the time indicated at tracking time option.

Servidor

failed attempts

Enter the number of login failures a host is allowed.

After this number is reached, the host will be blocked, no matter the username attempting to log in.

The host blocking protection will not disappear automatically and should be removed manually from the [access rules](#) s

Attack detection

failed attempts

Enter the number of login failures before creating a warning log entry about this suspicious activity.

If the number of invalid login events currently being tracked reach this number, and ongoing attack is detected.

- Configurar notificaciones al correo electrónico, se recomienda deshabilitar los mensajes de error al iniciar sesión, avisar al usuario el número de intentos de inicio de sesión que le restan, mostrar la fecha y hora de último acceso.

▼ NOTIFICACIÓN

- Desactivar el mensaje de error de fallo al iniciar sesión
 Prevents the display of login error messages.
 A user attempting to login will not be aware if the account exists, an invalid user name or password has been submitte
- Avisar al usuario del número de intentos de identificación que le quedan
 The user is notified about the number of remaining login attempts before the account gets blocked.
 Security tip: If you enable this option, try to not disclose as much of your login policies as possible in the message sho
- Muestra la fecha/hora de la última entrada
 When a user successfully logs in, a message will display the last time he logged into the site.
- Muestra la fecha/hora del último acceso
 When a user successfully logs in, a message will display the last site access with this account.

▼ EMAIL FOR ONGOING ATTACK DETECTION

Para

Provide a comma-separated list of emails for who should receive an email message when an ongoing attack is detecte

Asunto

Body

2.8. MÓDULO SECURITY KIT

Security Kit permite proteger el sitio web de una amplia variedad de ataques como Cross-Site Scripting, Cross-Site Request Forgery, Clickjacking. Para aplicar este módulo se recomienda probar primero en el ambiente de pruebas.

- Instalar el módulo security kit (<https://www.drupal.org/project/seckit>) y habilitarlo.



The screenshot shows the 'Security Kit' configuration page in Drupal. At the top, there is a breadcrumb trail: 'Inicio » Administración » Configuración » Sistema'. Below this, a descriptive paragraph states: 'This module provides your website with various options to mitigate risks of common web application vulnerability issue leading to an easy exploitation of an old Internet Explorer MIME sniffer HTML injection vulnerability. Note'. The main content area is a list of expandable configuration sections:

- ▼ **CROSS-SITE SCRIPTING**
 Configure levels and various techniques of protection from cross-site scripting attacks
 - ▶ **CONTENT SECURITY POLICY**
 - ▶ **X-XSS-PROTECTION HEADER**
- ▶ **CROSS-SITE REQUEST FORGERY**
- ▶ **CLICKJACKING**

- Configurar las opciones del módulo para mitigar riesgos de seguridad.

Si se desea ampliar las opciones de configuración de seguridad, se recomienda consultar los siguientes recursos:

- <https://developer.mozilla.org/es/docs/Web/HTTP/CSP>
- https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html
- <https://developer.mozilla.org/es/docs/Web/HTTP/Headers/X-Frame-Options>
- <https://developer.mozilla.org/es/docs/Web/HTTP/Headers/Strict-Transport-Security>

3. CONTROL DE CAMBIOS.

Versión	Fecha	Descripción de las modificaciones
1	12/01/2021	Versión nueva del Documento.

ANEXO 4

1. INTRODUCCIÓN

Wordpress es un sistema de gestión de contenido (CMS, Content Management System), que permite crear sitios web, su popularidad ha logrado que resulte muy atractivo para los “ciberatacantes”, con el fin de explotar vulnerabilidad

2. ASEGURANDO WORDPRESS

Para mitigar el riesgo de ataques a Wordpress, recomendamos las siguientes buenas prácticas de seguridad.

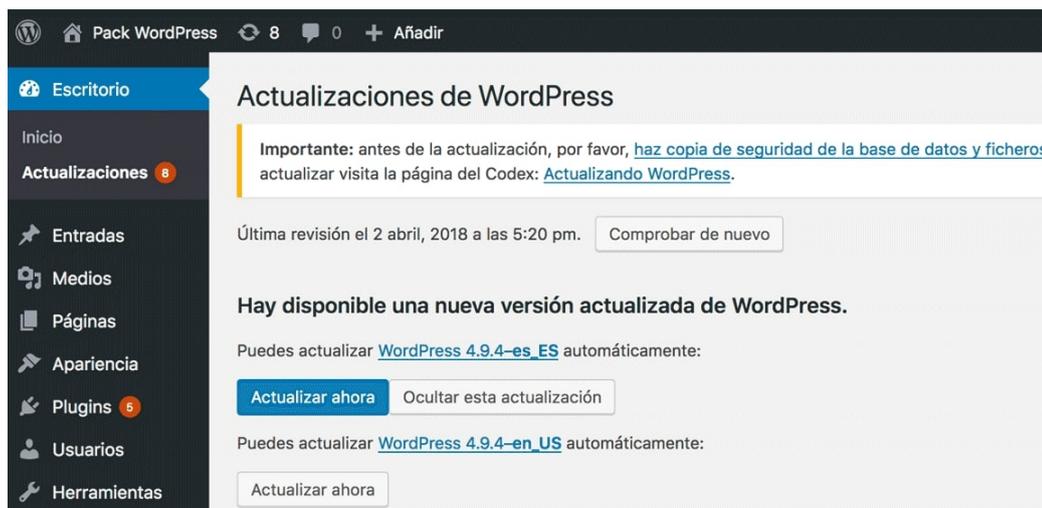
2.1. CONFIGURAR EL CONTROL DE ACCESO DE USUARIOS

- Ingresar al panel de administración de usuarios del sitio web: [https://\[mi-dominio.gob.bo\]/wp-admin/users.php](https://[mi-dominio.gob.bo]/wp-admin/users.php) y eliminar a los usuarios administradores que no se usan actualmente:



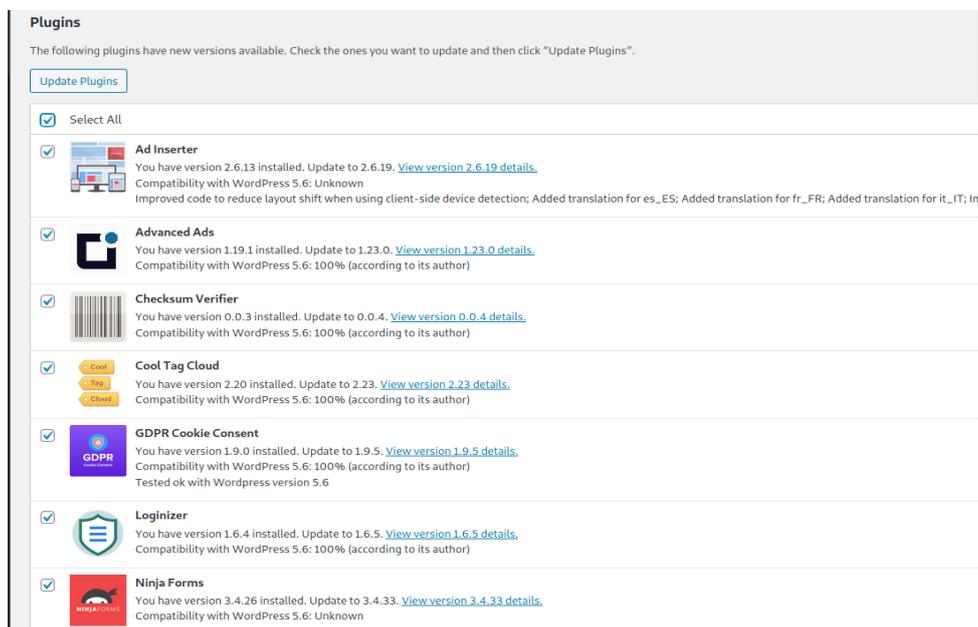
2.2. ACTUALIZAR EL CORE DE WORDPRESS:

- Ingresar a su sitio web [https://\[mi-dominio.gob.bo\]/wp-admin/update-core.php](https://[mi-dominio.gob.bo]/wp-admin/update-core.php) y hacer click en el botón “Actualizar ahora”.



2.3. ACTUALIZAR LOS PLUGINS DE WORDPRESS

- Previamente instalar y activar el plugin WP-Rollback (<https://es.wordpress.org/plugins/wp-rollback/>) que será útil en caso que la actualización de algún plugin no sea exitosa.
- Realizar un backup de la base de datos.
- Ingresar al sitio [https://\[mi-dominio.gob.bo\]/wp-admin/update-core.php](https://[mi-dominio.gob.bo]/wp-admin/update-core.php) y seleccionar todos los plugins y presionar el botón “Actualizar plugins”.



Plugins

The following plugins have new versions available. Check the ones you want to update and then click "Update Plugins".

[Update Plugins](#)

- Select All
- Ad Inserter**
You have version 2.6.13 installed. Update to 2.6.19. [View version 2.6.19 details.](#)
Compatibility with WordPress 5.6: Unknown
Improved code to reduce layout shift when using client-side device detection; Added translation for es_ES; Added translation for fr_FR; Added translation for it_IT; In
- Advanced Ads**
You have version 1.19.1 installed. Update to 1.23.0. [View version 1.23.0 details.](#)
Compatibility with WordPress 5.6: 100% (according to its author)
- Checksum Verifier**
You have version 0.0.3 installed. Update to 0.0.4. [View version 0.0.4 details.](#)
Compatibility with WordPress 5.6: 100% (according to its author)
- Cool Tag Cloud**
You have version 2.20 installed. Update to 2.23. [View version 2.23 details.](#)
Compatibility with WordPress 5.6: 100% (according to its author)
- GDPR Cookie Consent**
You have version 1.9.0 installed. Update to 1.9.5. [View version 1.9.5 details.](#)
Compatibility with WordPress 5.6: 100% (according to its author)
Tested ok with Wordpress version 5.6
- Loginizer**
You have version 1.6.4 installed. Update to 1.6.5. [View version 1.6.5 details.](#)
Compatibility with WordPress 5.6: 100% (according to its author)
- Ninja Forms**
You have version 3.4.26 installed. Update to 3.4.33. [View version 3.4.33 details.](#)
Compatibility with WordPress 5.6: Unknown

- En caso de existir un error durante el proceso de actualización, realizar un ROLLBACK ([https://\[mi-dominio.gob.bo\]/wp-admin/plugins.php](https://[mi-dominio.gob.bo]/wp-admin/plugins.php)).

Bulk actions ▼ Apply	
<input type="checkbox"/> Plugin	Description
<input type="checkbox"/> Ad Inserter Activate Delete Rollback	Ad management w Version 2.6.19 By
<input type="checkbox"/> Advanced Ads Add-Ons Support Deactivate Rollback	Manage and optimi Version 1.23.1 By
<input type="checkbox"/> Auto Post Scheduler Settings Deactivate Rollback	Publishes posts or Version 1.82 By S
<input type="checkbox"/> Checksum Verifier Deactivate Rollback	Verifies MD5 check Version 0.0.4 By
<input type="checkbox"/> Cool Tag Cloud Deactivate Rollback	A simple, yet very t Version 2.23 By W

2.4. HABILITAR ACTUALIZACIONES DE SEGURIDAD AUTOMÁTICAS

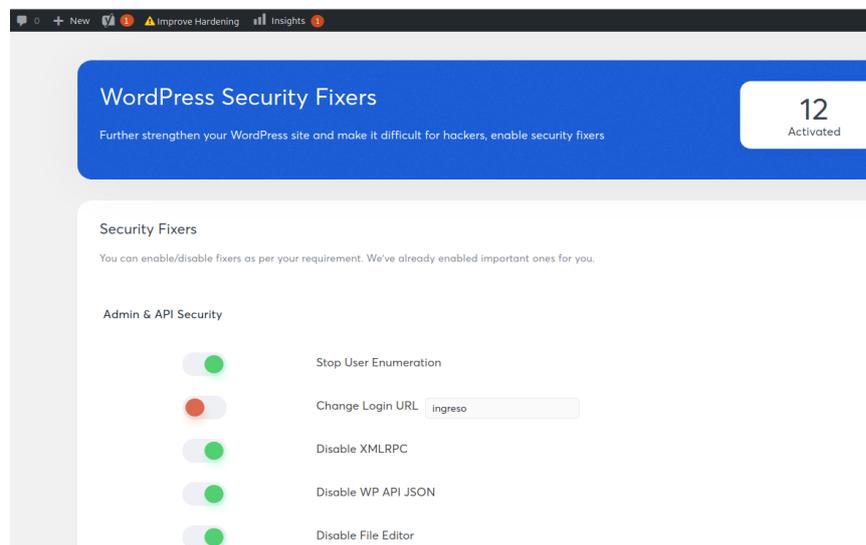
- Ingresar al panel de administración [https://\[mi-dominio.gob.bo\]/wp-admin/plugins.php](https://[mi-dominio.gob.bo]/wp-admin/plugins.php) y seleccionar todos los plugins.
- Seleccionar la acción “habilitar actualizaciones automáticas” y ejecutar “Aplicar”.

Plugins Add New	
All (18) Active (18) Update Available (11) Auto-updates Enabled (1) Auto-updates Disabled (17)	
Enable Auto-updates ▼ Apply	
<input checked="" type="checkbox"/> Plugin	Description
<input checked="" type="checkbox"/> Ad Inserter Settings Deactivate	Ad management with many advanced advertising features to insert ads at optimal positions Version 2.6.13 By Igor Funa View details Safe mode
🔔 There is a new version of Ad Inserter available. View version 2.6.19 details or update now .	
<input checked="" type="checkbox"/> Advanced Ads Add-Ons Support Deactivate	Manage and optimize your ads in WordPress Version 1.19.1 By Thomas Maier, Advanced Ads GmbH View details
🔔 There is a new version of Advanced Ads available. View version 1.23.0 details or update now .	
<input checked="" type="checkbox"/> Auto Post Scheduler Settings Deactivate	Publishes posts or recycles old posts at specified time intervals automatically. Version 1.82 By Super Blog Me View details

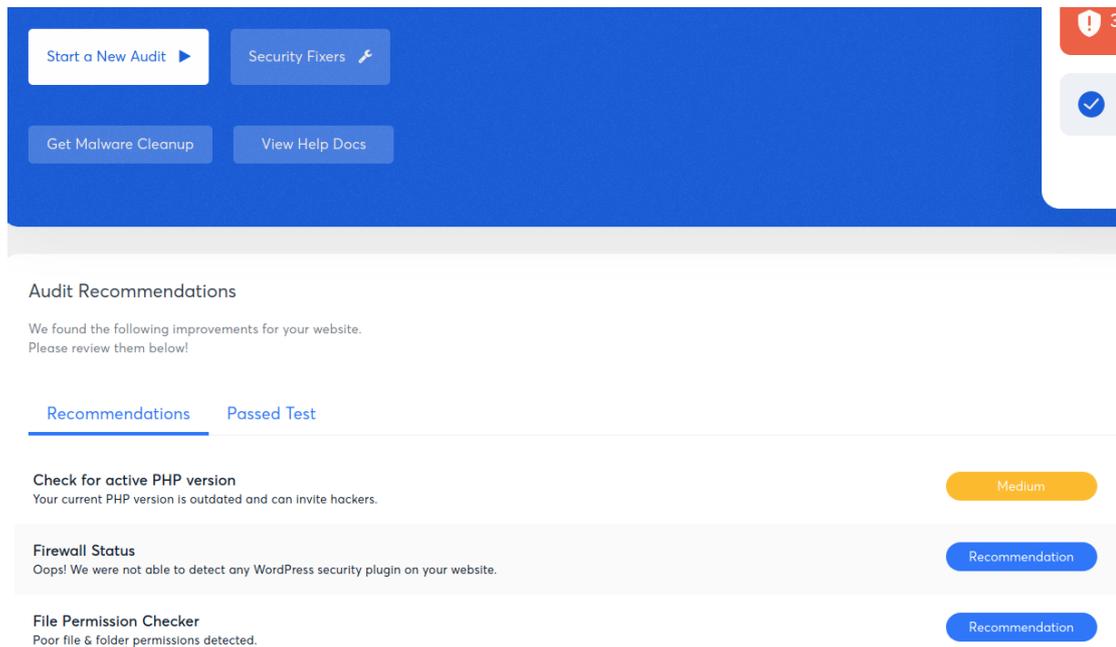
- Borrar los themes no usados mediante la URL [https://\[mi-dominio.gob.bo\]/wp-admin/themes.php](https://[mi-dominio.gob.bo]/wp-admin/themes.php)

2.5. INSTALAR PLUGINS DE SEGURIDAD

- Instalar y habilitar el plugin “Logonizer” (<https://wordpress.org/plugins/loginizer/>) para proteger el sitio contra ataques de fuerza bruta.
- Instalar y habilitar el plugin “WP Hardening” (<https://wordpress.org/plugins/wp-security-hardening/>)
- En el panel de “WP hardening” [https://\[mi-dominio.gob.bo\]/wp-admin/admin.php?page=wphwp_harden_fixers](https://[mi-dominio.gob.bo]/wp-admin/admin.php?page=wphwp_harden_fixers) habilitar todas las opciones (12 en total) menos “Change Login URL”:



- En el panel de “WP hardening” [https://\[mi-dominio.gob.bo\]/wp-admin/admin.php?page=wphwp_harden](https://[mi-dominio.gob.bo]/wp-admin/admin.php?page=wphwp_harden) realizar la auditoría de seguridad y corregir todas las observaciones críticas (high), obteniendo como resultado final una pantalla similar a la siguiente:



The screenshot shows a security audit dashboard with a blue header containing buttons for 'Start a New Audit', 'Security Fixers', 'Get Malware Cleanup', and 'View Help Docs'. Below the header, there are tabs for 'Recommendations' and 'Passed Test'. Three recommendations are listed:

- Check for active PHP version**: Your current PHP version is outdated and can invite hackers. (Medium severity)
- Firewall Status**: Oops! We were not able to detect any WordPress security plugin on your website. (Recommendation)
- File Permission Checker**: Poor file & folder permissions detected. (Recommendation)

3. CONTROL DE CAMBIOS.

Versión	Fecha	Descripción de las modificaciones
1	12/01/2021	Versión nueva del Documento.

ANEXO 5

1. INTRODUCCIÓN

En caso de ser afectado por un incidente de seguridad informática como el hackeo del sitio web se deben seguir los siguientes pasos para la contención del incidente.

2. DESARROLLO

- a) No eliminar ningún archivo del servidor ni realizar cambios en la base de datos
- b) Copiar los archivos del sitio web a otra ruta que no sea accesible desde el servidor web. Ej: /home/{usuario}
- c) Restaurar el sitio web con la versión estática (HTML) más reciente generada por la herramienta Httrack. La guía de cómo generar esta copia de respaldo está en el documento “Guía para la administración segura de sitios web” en el punto 6 (COPIA ESTÁTICA DEL SITIO WEB).
- d) Coordinar el envío de los siguientes ítems al CGII.
 - Archivos del sitio web hackeado copiados en el paso b.
 - Backup de la base de datos (si corresponde).
 - Logs del servidor web, ubicados en el siguiente directorio según el sistema operativo del servidor web:
 - **Windows (IIS):** %SystemDrive%\inetpub\logs\LogFiles*
 - **Red Hat/CentOS/Fedora (Apache):** /var/log/httpd/error_log
/var/log/httpd/access_log
 - **Debian/Ubuntu (Apache):** /var/log/apache2/error.log
/var/log/apache2/access.log
 - **Debian/Ubuntu (Nginx):** /var/log/nginx/error.log
/var/log/nginx/access.log
 - **CPANEL:** Metrics --> Raw Access
 - **Windows (Apache)** C:\wamp\logs\access_*.log

C:\xampp\apache\logs.log*

3. CONTROL DE CAMBIOS.

Versión	Fecha	Descripción de las modificaciones
1	12/01/2021	Versión nueva del Documento.