



**Seguridad en Sistemas y  
Respuesta a Incidentes**

---

# **CMSInstaller**

***Documentación***

Proyecto elaborado por:

**Diana Guadalupe Tadeo Guillén y Rafael Alejandro Vallejo Fernández**



## TABLA DE CONTENIDO

---

Introducción.....	3
1. Requisitos.....	5
2. Información general de la aplicación .....	7
3. Funcionamiento general de la aplicación	10
4. Referencias .....	15

# INTRODUCCIÓN

---

Este proyecto fue desarrollado para permitir a usuarios instalar de forma automática un CMS con las configuraciones generadas a partir de las preferencias del usuario. Los CMS's disponibles son los más conocidos y usados de código abierto y específicamente usados en servidores Linux.

## Objetivo Principal:

Generar un instalador de CMS seguro con los datos que se obtengan a partir del llenado de un formulario en una aplicación web que permita instalar todo lo necesario para el funcionamiento de este CMS.

## Otros objetivos:

- Instalar lo necesario para la implementación de un CMS de forma automática. Esto puede incluir, el servidor web, el manejador de base de datos y otras dependencias.
- Configurar el sistema en donde se instalará este CMS para permitir conexiones seguras en el entorno de producción.
- Agregar configuraciones para que la instalación se pueda realizar de forma remota.
- Generar toda la documentación para el uso del instalador.
- Instalar configuraciones extras en el CMS para mayor seguridad de este más allá del servidor en donde se encuentra.
- Generar las bitácoras necesarias para mantener el monitoreo constante de cómo se está llevando a cabo el proceso de instalación y configuración.

Entre los principales requerimientos se encuentran:

1. Elaborar una interfaz web se usuario que permita seleccionar las características del sistema operativo y lo que el usuario requiera para la configuración del sitio del CMS. Permitir la descarga de un script que llevará a cabo la instalación completa en el sistema operativo seleccionado.
2. La ejecución del script debe generar una bitácora que contenga la descripción de las intalaciones y configuraciones que se van realizando.
3. El script debe contener la configuración de seguridad necesaria (Hardening)
4. Generar respaldos para la Base de Datos, el servicio web, firewall y WAF.

## 5. Documentación.

Este proyecto fue realizado como proyecto final del Plan de Becarios de Seguridad de la información de UNAM-CERT.

# 1. REQUISITOS

---

Los requisitos necesarios para poder utilizar el CMSInstaller son los siguientes.

## Requisitos Generales para que funcione la aplicación:

- Para la aplicación web, se debe tener instalado el sistema operativo Debian 10
- Para la aplicación web, se debe contar con al menos 10mb de espacio en disco.
- Para la ejecución de los scripts es necesario tener instalado como sistema operativo Debian 9 /10 o CentOS 6/7.
- Una conexión a internet estable.
- Al menos 512MB de memoria RAM.
- Tener Git instalado.
- Tener políticas sudo (opcional si se puede ejecutar como root).

## Requisitos específicos de acuerdo a la instalación

Se aclara que estos son requisitos de Hardware, ya que el requisito de software ya se encuentra en los requisitos generales o se instalarán en el proceso.

- **PostgreSQL**
  - Arquitectura de 64 bits
  - 2 GB de memoria RAM
  - Dual CPU/Core
  - RAID 1
- **MySQL**
  - CPU: Intel Core o Xeon 3GHz (o Dual Core 2GHz) o iguales a AMD CPU
  - Core singl
  - 4 GB de memoria RAM
  - Graphic Accelerators: nVidia o ATI con soporte OpenGL 1.5 o superiores
  - Display Resolution: 1280×1024 es recomendada, 1024×768 es la mínima.
- **Apache**
  - Linux kernel versión 2.6 o superior, glibc2 versión 2.5 o superior
  - 256 MB de memoria RAM (512 MB recomendado)
  - 400 Mbytes de espacio en disco

- X-Server con resolución de 1024 x 768 o superior resolution y al menos 256 colores

- **Nginx:**

- 2 CPU cores
- 4 GB en memoria RAM
- 2x1 GbE NIC
- 500 GB De espacio en disco duro

- **Drupal:**

- 2 GHz Dual-core
- Arquitectura 64-bit
- 4 GB de Memoria RAM
- 120 GB espacio en disco

- **Joomla** (No hay especificación oficial, pero la recomendada):

- 4 GB de Memoria RAM
- 100 GB espacio en disco
- 2 CPU cores

- **WordPress** (No hay especificación oficial, pero la recomendada):

- 4 GB de Memoria RAM
- 100 GB espacio en disco
- 2 CPU cores

- **OJS** (No hay especificación oficial, pero la recomendada):

- 4 GB de Memoria RAM
- 100 GB espacio en disco
- 2 CPU cores

- **Moodle**

- 5GB mínimo (con un 200MB para el código de Moodle)
- Procesador 1GHz, (recomendado 2GHz dual core o superior).
- 512MB mínimo de memoria RAM (8GB recomendada en entornos de producción grandes).

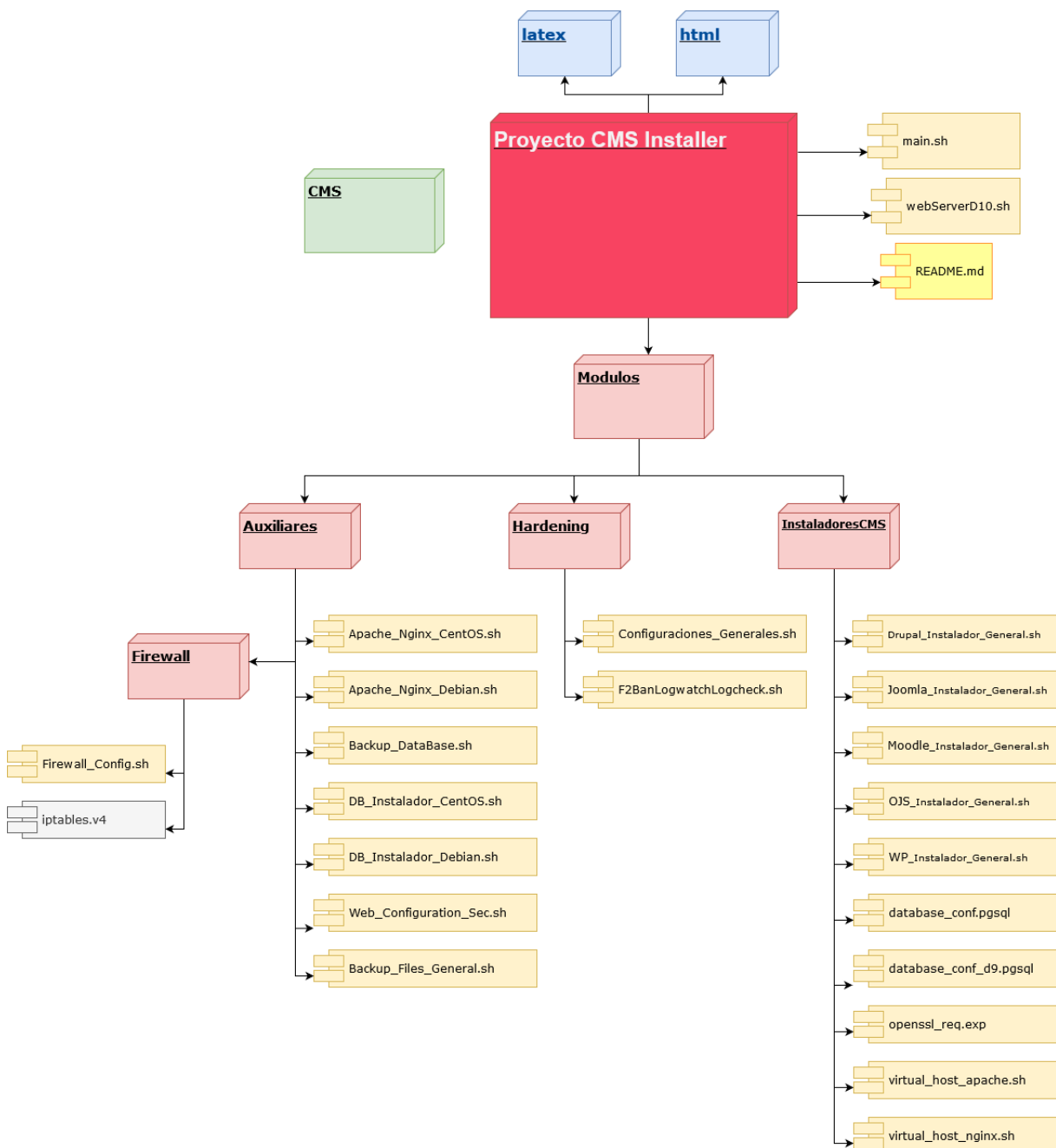
Estos requerimientos se pueden consultar en sus respectivos sitios, los cuales se anexan en la sección de **Referencias** de este documento.

## 2. INFORMACIÓN GENERAL DE LA APLICACIÓN

### Estructura del proyecto en Github

- En el siguiente diagrama se encuentra cómo se encuentran estructurados los módulos y archivos que se encuentran dentro del proyecto en Github.

<https://github.com/DianaTadeo/CMSInstaller>



- **html:** Carpeta que contiene la documentación en formato html de las funciones de cada archivo
- **latex:** Carpeta que contiene la documentación en formato latex (para generar PDF) de las funciones de cada archivo
- **main.sh:** Script principal que invoca el resto de los scripts de acuerdo a la configuración escogida en el formulario. Tiene las condiciones necesarias y no necesita ser modificado ni pasarle ningún argumento.
- **webServerD10.sh:** Script que permite realizar la instalación automática del servidor web con el formulario que permite generar los paquetes de descarga.
- **CMS:** Carpeta que contiene los archivos para el contenido del servidor web (Frontend y Backend).
- **README.md:** Archivo que explica la forma de ejecución de CMSInstaller.
- **Modulos:** Subcarpeta que contiene todos los scripts necesarios para instalaciones y configuraciones.
- **Hardening:** Subcarpeta que contiene los scripts necesarios para las configuraciones de seguridad necesarias para mayor seguridad en el sistema donde se instalará el CMS.
- **Auxiliares:** Subcarpeta que contiene los scripts necesarios para instalar y configurar la base de datos y algunos complementos para poder instalar posteriormente el CMS.
- **InstaladorCMS:** Subcarpeta que contiene los scripts necesarios para la instalación del CMS escogido de acuerdo a las especificaciones en el formulario.

Para más información sobre el propósito de cada script, es necesario revisar la documentación de estos localizada en **html** y **latex** o en los respectivos scripts.

## Especificaciones

- **Ubicación del repositorio:**  
<https://github.com/DianaTadeo/CMSInstaller>
- **Peso de la aplicación web (Formulario de creación): 1.65MB**
- **Peso de la documentación: 439KB**
- **Peso del un instalador: 439KB**
- **Permisos de ejecución: root / instalación con sudo**



- **Genera varios archivos de acuerdo a las dependencias instaladas, por lo tanto, el mínimo de espacio recomendado es de 30GB.**
- **Se realizan configuraciones de *Firewall*, por lo cual, se debe de revisar las reglas que se generaron después de la ejecución.**

### 3. FUNCIONAMIENTO GENERAL DE LA APLICACIÓN

---

La aplicación funciona a partir del montaje de la aplicación web (Formulario). En este se deben ingresar los datos que se piden para poder generar el instalador adecuado, por lo tanto, la aplicación se encuentra conformado por dos partes. La primera que es montaje de la aplicación web en algún servidor; y la segunda, que corresponde al instalador descargado en un archivo comprimido.

#### ¿Cómo monto la aplicación web?

Para instalar el sitio web en un servidor Debian 10, debe descargarse el script "webServerD10.sh" que está en el repositorio <https://github.com/DianaTadeo/CMSInstaller..>

- Primero se instala wget para descargar el script:

```
sudo apt install wget -y
```

- Realizar descarga de script:

```
wget https://raw.githubusercontent.com/DianaTadeo/CMSInstaller/master/webServerD10.sh
```

- Dar permisos de ejecución al script:

```
chmod +x webServerD10.sh
```

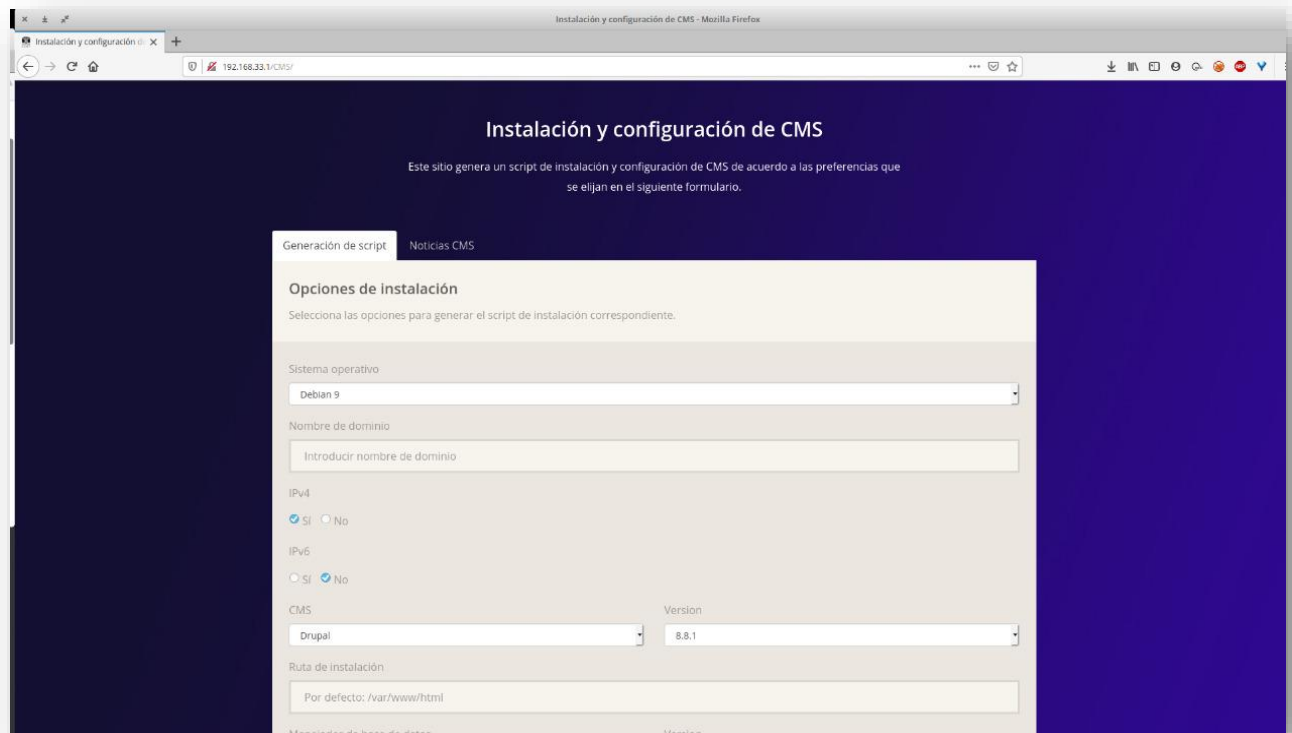
- Se ejecuta el script y se siguen las indicaciones que se van mostrando durante la ejecución.

```
sudo ./webServerD10.sh
```

**NOTA: es necesario tener acceso a una cuenta de Google**

#### ¿Cómo funciona CMSInstaller?

Se debe de ingresar en el navegador en donde fue montada la aplicación web (Formulario). Una vez dentro aparecerán las opciones que se deben de elegir. Todas las opciones deben de ser llenadas correspondientemente para poder generar un instalador adecuado.

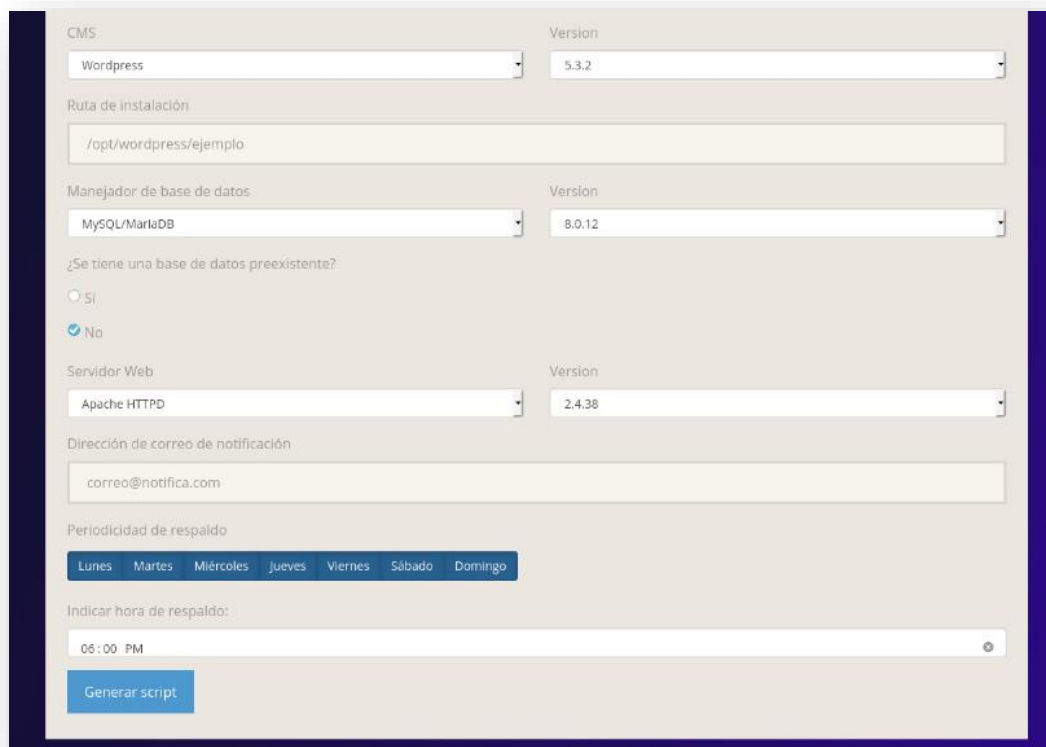


**Fig 1. Aplicación Web de CMSInstaller con la que se genera el instalador.**

Primero se piden las especificaciones del sistema operativo y otros extras.

**Fig 2. Primera parte del llenado del formulario.**

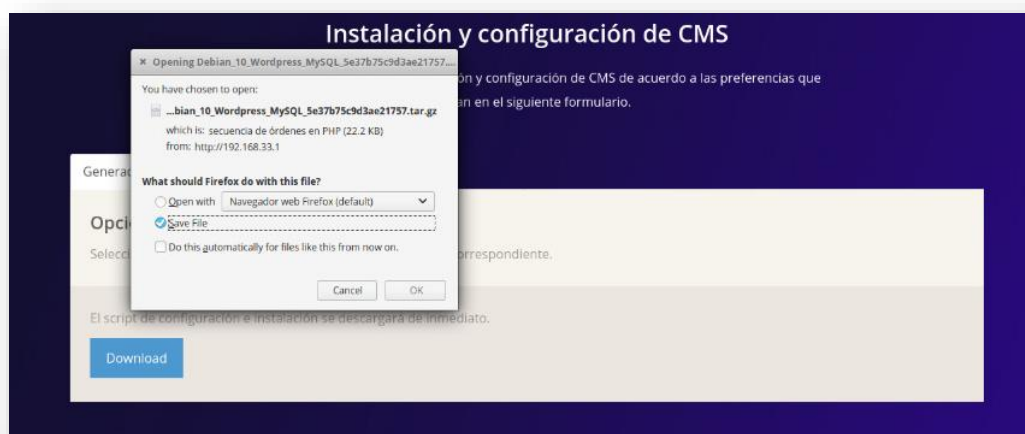
Posteriormente, las especificaciones que queremos para instalar el CMS y los respaldos.



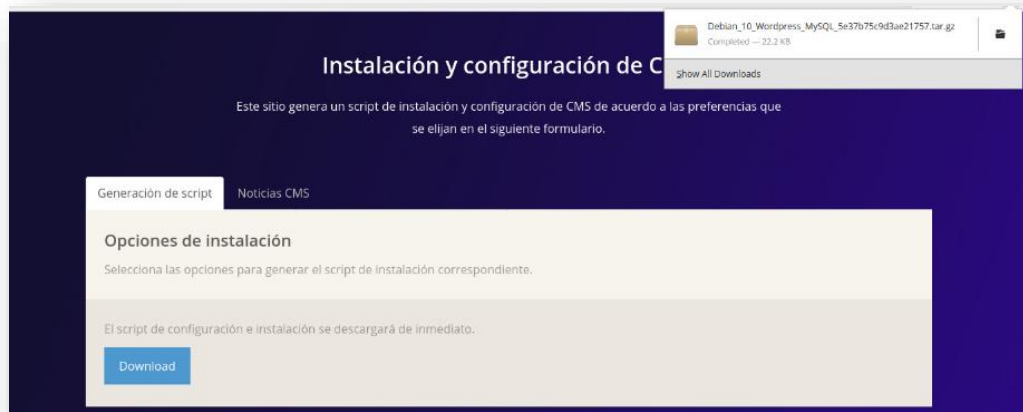
The image shows a web-based configuration form for installing a CMS. The form includes several sections with dropdown menus and input fields. The 'CMS' section has 'Wordpress' selected. The 'Version' section has '5.3.2' selected. The 'Ruta de instalación' section has '/opt/wordpress/ejemplo' entered. The 'Manejador de base de datos' section has 'MySQL/MariaDB' selected. The 'Version' section has '8.0.12' selected. The '¿Se tiene una base de datos preexistente?' section has 'No' selected. The 'Servidor Web' section has 'Apache HTTPD' selected. The 'Version' section has '2.4.38' selected. The 'Dirección de correo de notificación' section has 'correo@notifica.com' entered. The 'Periodicidad de respaldo' section has 'Lunes' selected. The 'Indicar hora de respaldo:' section has '06:00 PM' selected. A 'Generar script' button is at the bottom.

**Fig 3. Segunda parte del llenado de formulario.**

Una vez que se ha terminado de llenar el formulario, se debe dar clic en el botón de [“Generar Script”](#) el cual se encuentra en la parte inferior del formulario. Posteriormente se te redirigirá a la ventana que indica que el script ha sido generado y se te mostrará la opción para descargarlo.



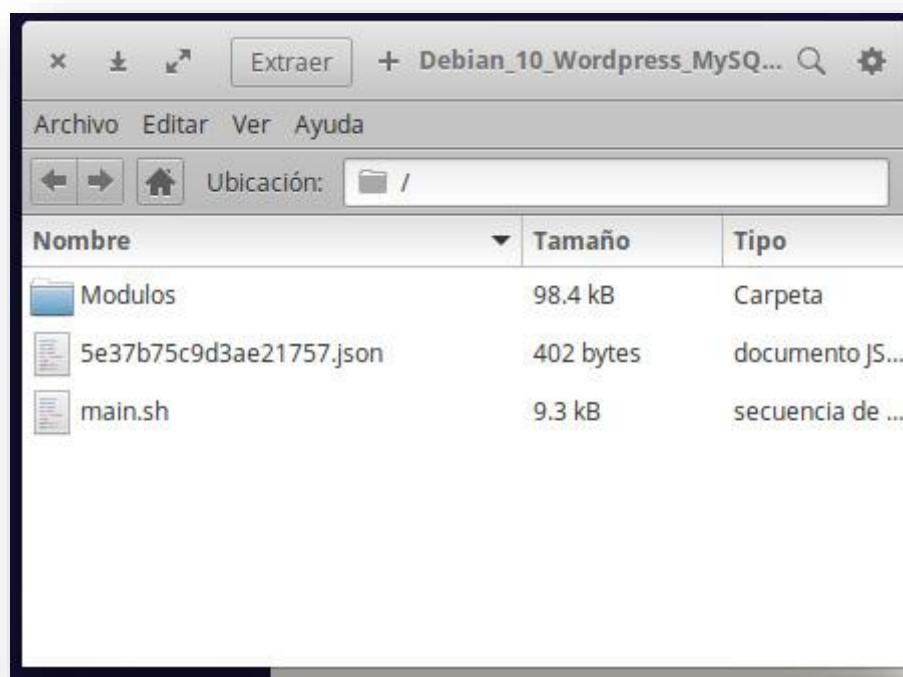
**Fig 4. Pestaña de descarga y confirmación de descarga del script generado.**



**Fig 4. Descarga del script realizada.**

Ya que se ha realizado la descarga, se puede revisar la carpeta donde fue descargado y se encontrará un archivo comprimido tar.gz cuyo nombre parte de las especificaciones en el formulario. Al descomprimirlo, se mostrarán los Módulos para la instalación, el archivo main.sh y un archivo json con todas las especificaciones generadas a partir del formulario y necesarias para la ejecución del script.

**AVISO: Si se borra este archivo json, se perderán todas las configuraciones para poder ejecutar el script.**



**Fig 4. Contendio del archivo tar descargado.**

Una vez obtenido este, es necesario ejecutar el archivo main.sh con permisos sudo, o en su defecto, con permisos root.

Primero volverlo ejecutable y luego ejecutarlo en consola.

```
$ chmod +x main.sh
```

```
$ sudo ./main.sh
```

**AVISO: Es necesario estar atento a la instalación pues se pide ingresar datos de entrada constantemente como contraseñas, confirmaciones, etc.**

Una vez terminada la instalación se debe ingresar a la url que se ingresó en el formulario para poder ingresar al sitio del CMS instalado. Ya no es necesario ingresar configuraciones, solo el usuario y su contraseña para iniciar sesión.

### Posibles paquetes instalados:

- PostgreSQL
- MySQL/MariaDB
- Apache
- Nginx
- PHP (En sus versiones más recientes)
- Wget
- Curl
- Iptables
- Fail2Ban
- Logwatch
- Logcheck
- ModSecurity (OWASP rules)
- Openssl
- Composer
- Drush
- Wp-cli
- Joomla!tools
- Tools para dpkg y yum
- Jq
- Expect

## 4. REFERENCIAS

---

- <https://www.debian.org/News/2019/20190706>
- <https://www.debian.org/News/2017/20170617>
- <https://httpd.apache.org/>
- <https://www.postgresql.org/>
- <https://github.com/joomlatools/joomlatools-console>
- <https://www.mysql.com/>
- <https://wordpress.org/>
- <https://www.drupal.org/>
- <https://pkp.sfu.ca/ojs/>
- <https://www.joomla.org/>
- <https://moodle.org/>
- <https://wp-cli.org/>
- [https://docs.moodle.org/19/en/Installing Moodle using command line](https://docs.moodle.org/19/en/Installing_Moodle_using_command_line)
- [https://www.owasp.org/index.php/OWASP Backend Security Project SQLServer Hardeni](https://www.owasp.org/index.php/OWASP_Backend_Security_Project_SQLServer_Hardeni)  
[ng](#)
- <https://sites.google.com/site/linuxscooter/linux/aministration/yum-apt>
- <https://stackoverflow.com/questions/44044449/facing-issue-while-installing-jq-in-centos>
- <https://drushcommands.com/drush-8x/core/site-install/>
- <http://docs.drush.org/en/master/install/>
- <https://drupal.stackexchange.com/questions/282857/recommended-drush-version-to-use-and-install-for-ubuntu-19-with-php-7-2-and-run>
- <https://drushcommands.com/drush-8x/core/site-install/>
- <http://docs.drush.org/en/master/install/>
- <https://www.zyxware.com/articles/3170/solved-drupal-errors-page-not-found-errors-on-all-pages-except-homepage>
- <https://www.valuebound.com/resources/blog/Installing-drupal-with-drush-the-basics>
- <https://www.pluralsight.com/blog/it-ops/linux-hardening-secure-server-checklist>
- <https://www.tecmint.com/linux-server-hardening-security-tips/>
- [https://www.drupal.org/project/captcha\\_webform](https://www.drupal.org/project/captcha_webform)
- <https://drupal.stackexchange.com/questions/263970/change-account-settings-in-db>
- [http://www.joshstaiger.org/archives/2005/07/bash\\_profile\\_vs.html](http://www.joshstaiger.org/archives/2005/07/bash_profile_vs.html)
- <https://drushcommands.com/drush-7x/role/role-add-perm/>
- <https://www.acquia.com/blog/leverage-drush-7-drupal-8>
- <https://pkp.sfu.ca/ojs/docs/userguide/2.3.1/systemAdministrationBackupRestore.html>
- <https://omarcerecedo.wordpress.com/2019/05/20/ojs-open-journal-system/>
- <https://pkp.sfu.ca/ojs/docs/userguide/2.3.3/es/systemAdministrationCaptcha.html>
- <https://github.com/pkp/vagrant/issues>
- <https://stackoverflow.com/questions/26734777/yum-error-cannot-retrieve-metalink-for-repository-epel-please-verify-its-path>
- <https://github.com/drush-ops/drush/issues/1437>

- <https://serverfault.com/questions/433295/what-is-the-right-iptables-rule-to-allow-apt-get-to-download-programs>
- <https://www.thegeekstuff.com/2011/06/iptables-rules-examples/>
- <https://superuser.com/questions/1412054/non-interactive-apt-upgrade>
- <https://content-security-policy.com/>
- <https://geekflare.com/http-header-implementation/>
- <https://blog.sucuri.net/2018/04/content-security-policy.html>
- <https://geekflare.com/http-header-implementation/#X-Permitted-Cross-Domain-Policies>
- <https://likegeeks.com/es/comando-expect/>
- <https://scotthelme.co.uk/hpkp-http-public-key-pinning/>
- <https://geekflare.com/10-best-practices-to-secure-and-harden-your-apache-web-server/>
- <https://forum.joomla.org/viewtopic.php?t=789045>
- <https://kubik-rubik.de/downloads/ecc-easycalccheck-plus/joomla-3>
- <https://github.com/osolgithub/OSOLCaptcha4Joomla3>
- <http://www.outsource-online.net/osol-captcha-for-joomla.html#Download>
- <https://stelfox.net/blog/2016/02/better-practices-with-sudo/>
- <https://github.com/fcaviggia/hardening-script-el6/blob/master/config/sudoers>
- <https://stackoverflow.com/questions/19487365/how-do-i-force-redirect-all-404s-or-every-page-whether-invalid-or-not-to-the>
- <https://stackoverflow.com/questions/43346297/convert-apache-command-to-nginx-filesmatch>
- <https://comomolatodo.com/2019/06/12/modsecurity-con-nginx-en-buster/>
- <https://stackoverflow.com/questions/57415360/configure-error-the-http-xsdt-module-requires-the-libxml2-libxslt-libraries>
- <https://github.com/SpiderLabs/ModSecurity/issues/1941>
- <https://github.com/SpiderLabs/ModSecurity-nginx/issues/117>
- <https://www.nginx.com/blog/compiling-and-installing-modsecurity-for-open-source-nginx/>
- <https://stackoverflow.com/questions/17196230/bash-print-each-input-string-in-a-new-line>
- <https://guides.wp-bullet.com/nginx-redirect-404-errors-to-homepage-wordpress/>
- [https://medium.com/@shoaibhassan\\_/install-wordpress-with-postgresql-using-apache-in-5-min-a26078d496fb](https://medium.com/@shoaibhassan_/install-wordpress-with-postgresql-using-apache-in-5-min-a26078d496fb)
- <https://www.smashingmagazine.com/2014/05/proper-wordpress-filesystem-permissions-ownerships/>
- <https://www.nginx.com/resources/wiki/start/topics/recipes/drupal/>
- <https://coolpandaca.wordpress.com/2012/12/07/migrate-ojs-to-nginx-from-apache/>
- <https://websiteforstudents.com/install-moodle-3-3-2-ubuntu-17-04-17-10-nginx-mariadb-php-support/>
- <https://www.digitalocean.com/community/tools/nginx>
- [https://www.peterbe.com/plog/be-very-careful-with-your-add\\_header-in-nginx](https://www.peterbe.com/plog/be-very-careful-with-your-add_header-in-nginx)
- <https://www.rosehosting.com/blog/how-to-install-joomla-with-nginx-on-ubuntu-18-04/#Step-2-Install-PHP-72-and-Required-PHP-Modules>
- <https://blog.programster.org/debian-9-install-nginx>
- [https://docs.moodle.org/38/en/Security\\_recommendations](https://docs.moodle.org/38/en/Security_recommendations)
- <https://stackoverflow.com/questions/35599883/disable-options-http-on-apache-server>



- <https://esencialsistemas.com/subsanar-el-error-de-base-de-datos-en-la-instalacion-de-las-versiones-nuevas-de-moodle-3/>
- <http://develoteca.com/clockpicker-para-campos-de-entrada-con-bootstrap-y-jquery/>
- <https://weareoutman.github.io/clockpicker/>
- <https://www.respocert.com/php/php-forms-best-practices>
- <https://blog.jacobemerick.com/web-development/best-practices-with-forms/>
- <https://www.kaplankomputing.com/blog/tutorials/recaptcha-php-demo-tutorial/>
- [https://www.w3schools.com/bootstrap/bootstrap\\_ref\\_css\\_helpers.asp](https://www.w3schools.com/bootstrap/bootstrap_ref_css_helpers.asp)
- <https://codebaker.in/reset-google-recaptcha-jquery/>
- <http://jonsegador.com/2017/05/configurar-recaptcha-2-0-con-php/>
- <https://www.postgresql.org/download/linux/redhat/>
- <https://stackoverflow.com/questions/23443398/nginx-error-connect-to-php5-fpm-sock-failed-13-permission-denied>
- <https://stackoverflow.com/questions/36149036/find-and-replace-text-in-a-file-between-range-of-lines-using-sed>
- [https://linuxhint.com/bash\\_arithmetic\\_operations/](https://linuxhint.com/bash_arithmetic_operations/)
- <https://docs.moodle.org/38/en/Nginx>
- <https://serverdiary.com/linux/how-to-install-and-configure-nginx-modsecurity-on-centos-7/>
- <https://serverfault.com/questions/739218/how-should-i-add-geoip-module-to-nginx>
- <https://www.theshell.guru/category/centos/>
- <https://www.pakjiddat.pk/articles/view/278/integrating-modsecurity-with-nginx-on-debian-9>
- <https://stackoverflow.com/questions/17845637/how-to-change-vagrant-default-machine-name>
- <http://www.servermom.org/how-to-install-modsecurity-with-owasp-on-apache-server/844/>
- [https://linuxadmin.io/mod\\_security-installation-apache-centos/](https://linuxadmin.io/mod_security-installation-apache-centos/)
- <https://stackoverflow.com/questions/21265191/apache-authtype-not-set-500-error>
- <https://stackoverflow.com/questions/21820715/how-to-install-latest-version-of-git-on-centos-7-x-6-x>
- <https://www.hugeserver.com/kb/install-modsecurity-nginx-centos/>
- <https://gist.github.com/jhguxin/145f3d4c0dafcfb7246b>
- <https://www.php.net/manual/es/function.hash-file.php>
- <https://coderwall.com/p/o2fasq/how-to-download-a-project-subdirectory-from-github>
- <https://www.java-samples.com/showtutorial.php?tutorialid=1511>

## Sobre requerimientos

- [https://www.commandprompt.com/blog/postgresql\\_minimum\\_requirements/](https://www.commandprompt.com/blog/postgresql_minimum_requirements/)
- <http://download.nust.na/pub6/mysql/doc/workbench/en/wb-requirements-hardware.html>
- [https://www.openoffice.org/dev\\_docs/source/sys\\_reqs\\_aoo40.html](https://www.openoffice.org/dev_docs/source/sys_reqs_aoo40.html)
- <https://docs.nginx.com/nginx/technical-specs/>
- [https://www.nginx.com/resources/datasheets/nginx-plus-sizing-guide/?\\_ga=2.236296520.873783903.1580769566-1459463291.1580769566](https://www.nginx.com/resources/datasheets/nginx-plus-sizing-guide/?_ga=2.236296520.873783903.1580769566-1459463291.1580769566)
- <https://www.drupal.org/node/1505394>
- [https://docs.moodle.org/38/en/Installing\\_Moodle#Hardware](https://docs.moodle.org/38/en/Installing_Moodle#Hardware)

CC BY-SA REALIZADO EN 2020  
RECONOCIMIENTO-COMPARTIRIGUAL