DGTIC Dirección General de Cómputo y de Tecnologías de Información y Comunicación

Actualización de portales de la CSI/UNAM-CERT

Integrantes:

Ayala Sanjuan Luis Antonio

Barragán Ramírez Luis David

Cerón Rodríguez Lezly Dialid

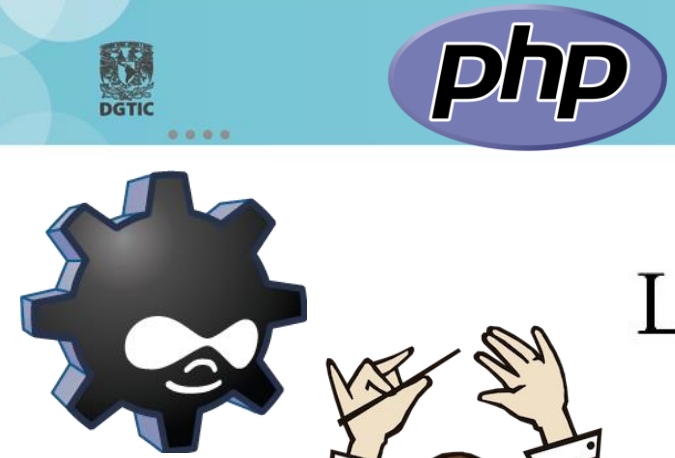
Descripción

Entender el funcionamiento actual de la infraestructura web con la que actualmente cuenta la CSI/UNAM-CERT. Realizar la migración de infraestructura Web de las versiones actuales a versiones posteriores para el CMS Drupal.

Instalar y configurar el funcionamiento y seguridad de la misma infraestructura para los CMS con los que actualmente funcionan los sitios web de la CSI.

Objetivos

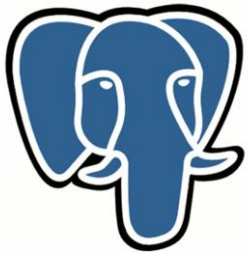
- Migración de plataforma Web de la CSI/UNAM-CERT a una versión posterior de CMS Drupal utilizando scripts para automatizar.
- Hardening del servidor en donde se aloja el nueva plataforma Web.
- Desarrollo de script para reparar el histórico alojado en CSI/UNAM-CERT



LOGWATCH

GitLab

Drupal™



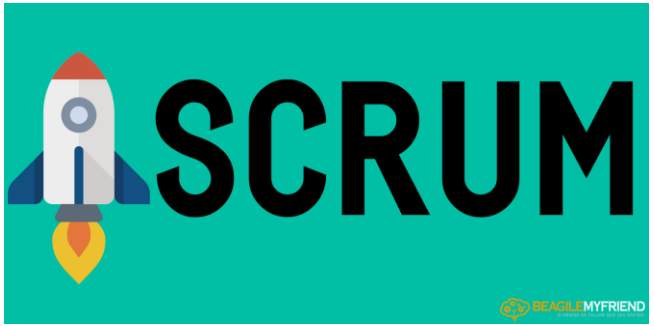
LogCheck

PostgreSQL

FAIL2BAN

Metodología de desarrollo

- Para el desarrollo del proyecto se utilizó la metodología ágil **SCRUM** por su enfoque en la realización de tareas en periodos cortos de tiempo y su flexibilidad en la adaptación de cambios.
- Se llevó a cabo un análisis del planteamiento proporcionado por el líder del proyecto y se recopilaron los requerimientos del proyecto.
- Con esta información se dividió el proyecto en tareas menores, las cuales se fueron realizando en periodos de 5 días a las semana; cada fin de semana se midió el incremento del avance obtenido.



Hardening

- Políticas de contraseña
- Políticas de Sudo
- Cuotas de disco
- Configuración de SSH
- Prevención de intrusos
- Análisis de registros del sistema
- Firewall
- WAF

Políticas de contraseña

- Cambio de contraseña cada 6 meses
- Longitud de 12 caracteres
- Con caracteres alfanuméricos y no alfanuméricos
- Solo se puede repetir dos veces un carácter de forma consecutiva
- No debe de tener el nombre del usuario

Políticas de Sudo

- Cada usuario sólo podrá ejecutar programas con privilegios de otro usuario que se especifiquen en el sudoers.

```
# Especificacion de privilegios de usuarios
ADMINS ALL = WEBCMDS,REDCMDS,/usr/bin/systemctl,EDITCMDS,TEXTCMDS
OPS ALL = REDCMDS
BDS ALL = (postgres:postgres) /usr/bin/psql, /usr/bin/pg_*
```

Cuotas de disco

Las cuotas de disco permiten limitar el espacio de almacenamiento que puede utilizar un usuario en el sistema.

Programas utilizados:

quota

```
root@csi-server2:/home/user# grep -v "#" /etc/fstab
UUID=28fff170-cc7d-4504-b175-5f9ccd091361 /               ext4    errors=remount-ro 0       1
UUID=133449b1-f337-4a06-9033-03936d38b61e /home           ext4    defaults,nosuid,nodev,usrquota,grpquota  0     2
UUID=1cd43652-9fb1-4b76-b3ca-b065edd1a8ed /tmp            ext4    defaults,nosuid,noexec,nodev  0  2
UUID=cf13fd40-0251-45fe-8dc3-1573248fae3d /var            ext4    defaults,nosuid,nodev   0     2
UUID=cb701b4b-9ea0-4fe1-bb6a-7f1591d5b86e none            swap    sw              0       0
/dev/sr0        /media/cdrom0   udf,iso9660 user,noauto     0       0
root@csi-server2:/home/user#
```

Configuración de SSH

/etc/ssh/sshd_config

```
#LoginGraceTime 2m
PermitRootLogin no
#StrictModes yes
```

```
ClientAliveInterval 600
ClientAliveCountMax 3
#UseDNS no
#PidFile /var/run/sshd.pid
MaxStartups 3:5:8
```

Prevención de intrusos

[Fail2Ban] sshd: banned [redacted] from Revisiones

Fail2Ban <reportes_sistemas@cert.unam.mx>
Sun 9/26/2021 5:04 PM

To: Luis David Barragan Ramirez

Hi,

The IP [redacted] has just been banned by Fail2Ban after
5 attempts against sshd.

Here is more information about [redacted]:

```
#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2021, American Registry for Internet Numbers, Ltd.
#


NetRange:       [redacted] - [redacted]
CIDR:           [redacted]
```

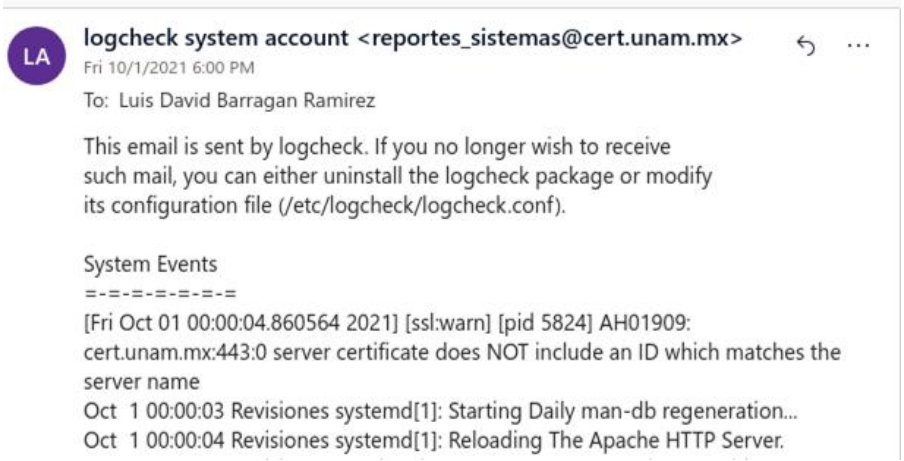
Análisis de registros del sistema

/etc/logcheck/logcheck.conf

/usr/share/logwatch/default.conf/logwatch.conf

LogCheck

LOGWATCH



LA

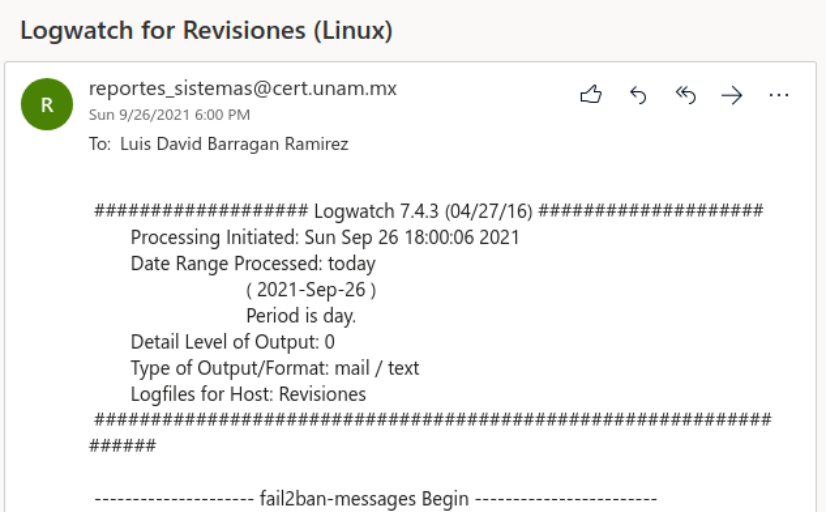
logcheck system account <reportes_sistemas@cert.unam.mx>

Fri 10/1/2021 6:00 PM

To: Luis David Barragan Ramirez

This email is sent by logcheck. If you no longer wish to receive
such mail, you can either uninstall the logcheck package or modify
its configuration file (/etc/logcheck/logcheck.conf).

System Events
=-=-=-=-=-=-=-=
[Fri Oct 01 00:00:04.860564 2021] [ssl:warn] [pid 5824] AH01909:
cert.unam.mx:443:0 server certificate does NOT include an ID which matches the
server name
Oct 1 00:00:03 Revisiones systemd[1]: Starting Daily man-db regeneration...
Oct 1 00:00:04 Revisiones systemd[1]: Reloading The Apache HTTP Server.



Logwatch for Revisiones (Linux)

R

reportes_sistemas@cert.unam.mx

Sun 9/26/2021 6:00 PM

To: Luis David Barragan Ramirez

########## Logwatch 7.4.3 (04/27/16) ##########
Processing Initiated: Sun Sep 26 18:00:06 2021
Date Range Processed: today
(2021-Sep-26)
Period is day.
Detail Level of Output: 0
Type of Output/Format: mail / text
Logfiles for Host: Revisiones
##########
######

---------- fail2ban-messages Begin ----------

Firewall

Crearon políticas restrictivas, las cuales fueron las siguientes:

- Permitir el acceso a ssh
- Puerto 80 accesible
- Permitir el acceso al servicio de resolver dominios(DNS)
- Permitir el acceso a los repositorio del sistema
- Permitir el acceso al servidor de correos
- Permitir el acceso al servicio de sincronización del tiempo NTP

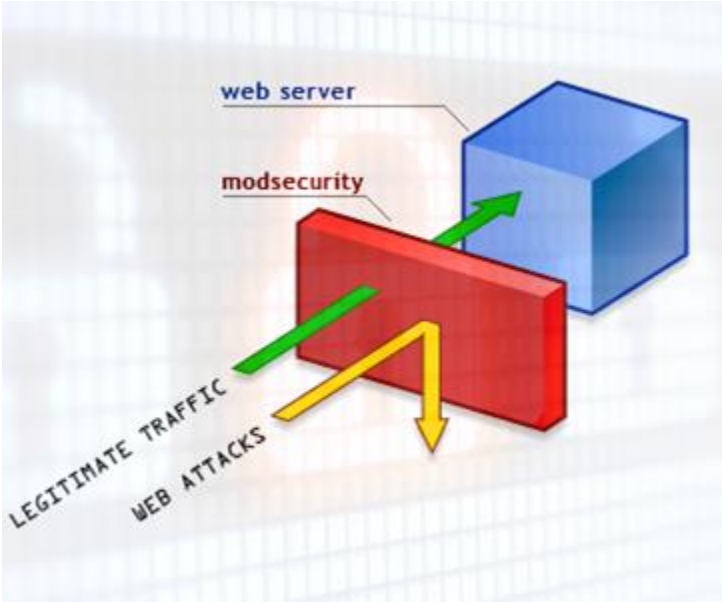
WAF

```
root@debian:~# sudo apt install libapache2-mod-security2
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
  liblua5.1-0 modsecurity-crs
```

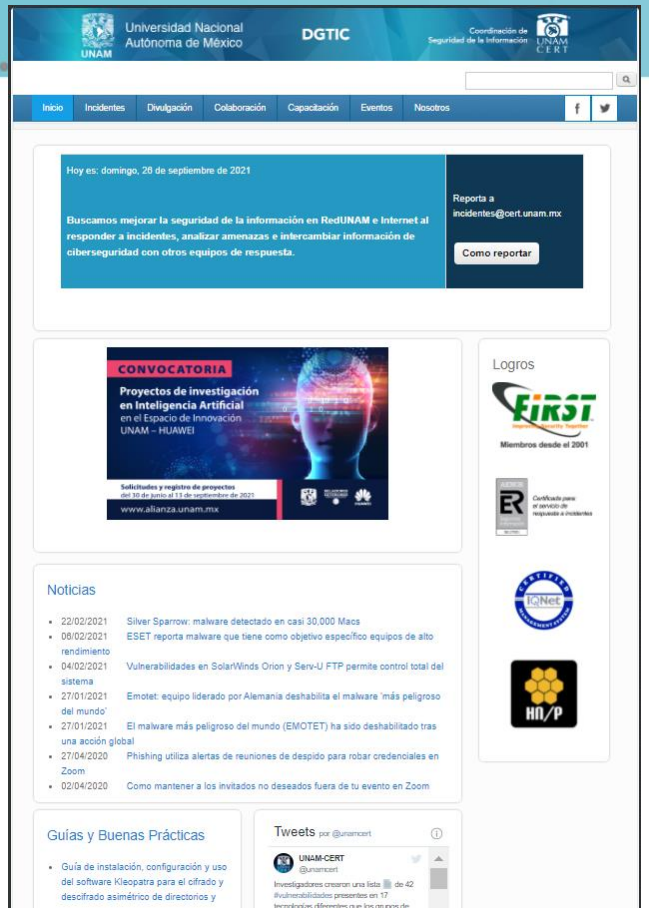
Archivo Modsecurity.conf
SecRuleEngine DetectionOnly > SecRuleEngine On

OWASP ModSecurity Core Rule Set
wget https://github.com/coreruleset/coreruleset/archive/v3.3.0.zip
mv modsecurity/

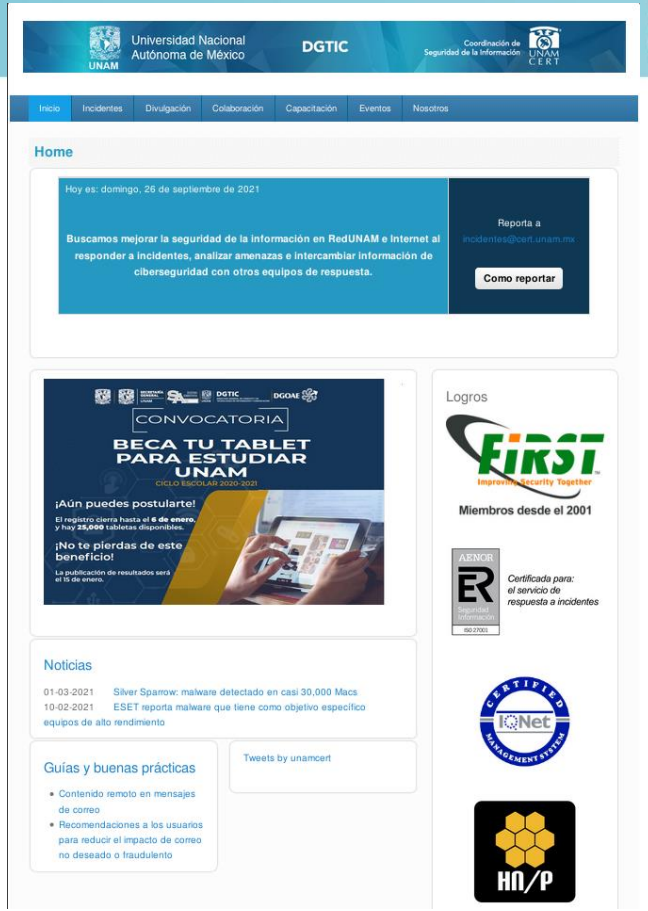
Apache2
Archivo security2.conf
IncludeOptional modsecurity/rules/.*.conf
IncludeOptional /usr/share/modsecurity-crs/*.load



Sitio Original

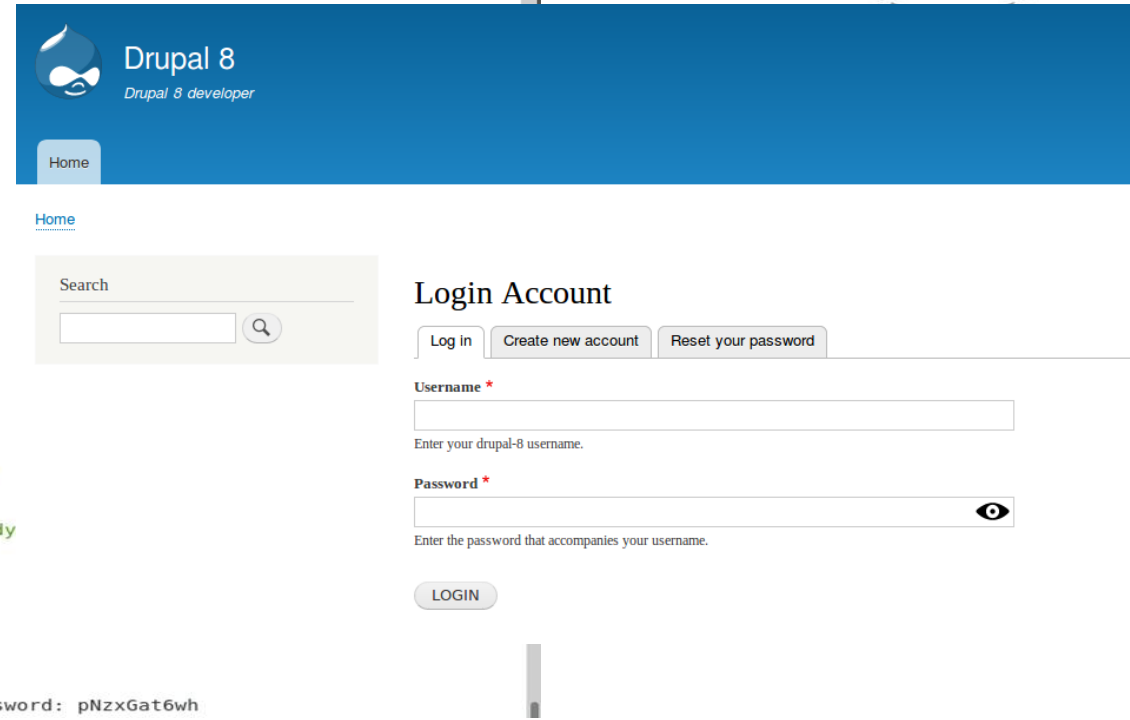


Sitio Réplica



Instalación de CMS Drupal 8

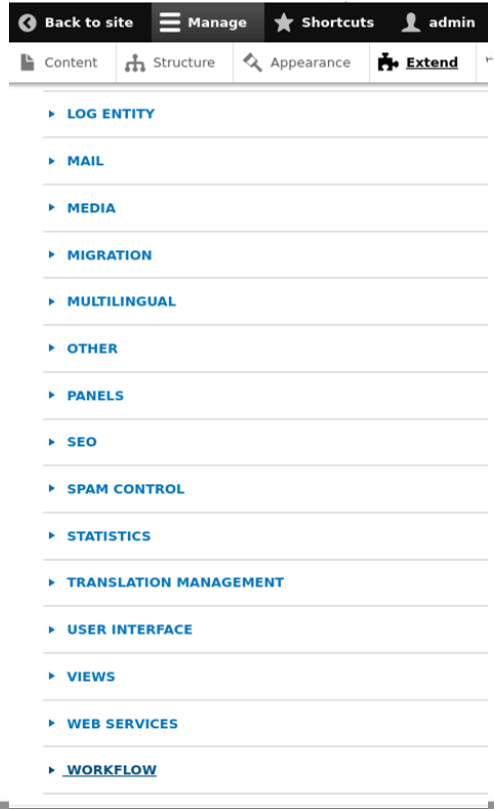
```
root@debian: ~
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
root@debian:~# ./InstalacionDrupal8.sh
Instalacion de Drupal 8
Actualizacion de Linux
Instalacion dependencias
Instalacion de composer
Instalador verificado
All settings correct for using Composer
Downloading...
30 packages you are using are looking for funding.
Use the `composer fund` command to find out more!
Instalacion de Drupal 8

 You are about to:
 * Create a sites/default/settings.php file
 * DROP all tables in your 'drupal81' database.

 // Do you want to continue?: yes.

 [notice] Starting Drupal installation. This takes a while.
 [notice] Performed install task: install_select_language
 [notice] Performed install task: install_select_profile
 [notice] Performed install task: install_load_profile
 [notice] Performed install task: install_verify_requirements
 [notice] Performed install task: install_settings_form
 [notice] Performed install task: install_write_profile
 [notice] Performed install task: install_verify_database_ready
 [notice] Performed install task: install_base_system
 [notice] Performed install task: install_bootstrap_full
 [notice] Performed install task: install_profile_modules
 [notice] Performed install task: install_profile_themes
 [notice] Performed install task: install_install_profile
 [notice] Performed install task: install_configure_form
 [notice] Cron run completed.
 [notice] Performed install task: install_finished
 [success] Installation complete.  User name: admin  User password: pNzxGat6wh
```



root@debian: ~

Archivo Editar Ver Buscar Terminal Ayuda

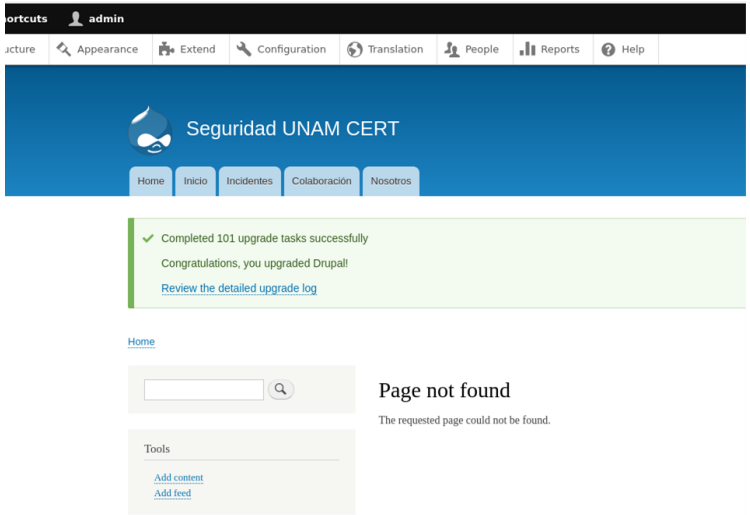
```
root@debian:~# ./InstalacionModulos.sh
Permisos
No composer.json in current directory, do you want to use the one at /var/www/drupal8? [Y,n]? y
Do not run Composer as root/super user! See https://getcomposer.org/root for details
Continue as root/super user [yes]?
Using version ^6.4 for phpmailer/phpmailer
./composer.json has been updated
Running composer update phpmailer/phpmailer
Loading composer repositories with package information
Updating dependencies
Lock file operations: 1 install, 0 updates, 0 removals
  - Locking phpmailer/phpmailer (v6.4.0)
Writing lock file
Installing dependencies from lock file (including require-dev)
Package operations: 1 install, 0 updates, 0 removals
  - Downloading phpmailer/phpmailer (v6.4.0)
  - Installing phpmailer/phpmailer (v6.4.0): Extracting archive
3 package suggestions were added by new dependencies, use `composer suggest` to see details.
Generating autoload files
29 packages you are using are looking for funding.
Use the `composer fund` command to find out more!
Modulos de migracion
migrate_upgrade was not found.                                          [warning]
The following projects provide some or all of the extensions not found: [ok]
migrate_upgrade
Would you like to download them? (y/n): y
Project migrate_upgrade (8.x-3.2) downloaded to                         [success]
/var/www/drupal8/web//modules/migrate_upgrade.
The following projects have unmet dependencies:                         [ok]
migrate_upgrade requires migrate_plus
Would you like to download them? (y/n): y
Project migrate_plus (8.x-5.1) downloaded to /var/www/drupal8/web//modules/migrate_plus.  [success]
Project migrate_plus contains 6 modules: migrate_example_setup, migrate_example, migrate_json_example, m
igrate_example_advanced_setup, migrate_example_advanced, migrate_plus.
The following extensions will be enabled: migrate_upgrade, migrate_plus, migrate_drupal, migrate
Do you really want to continue? (y/n): y
```

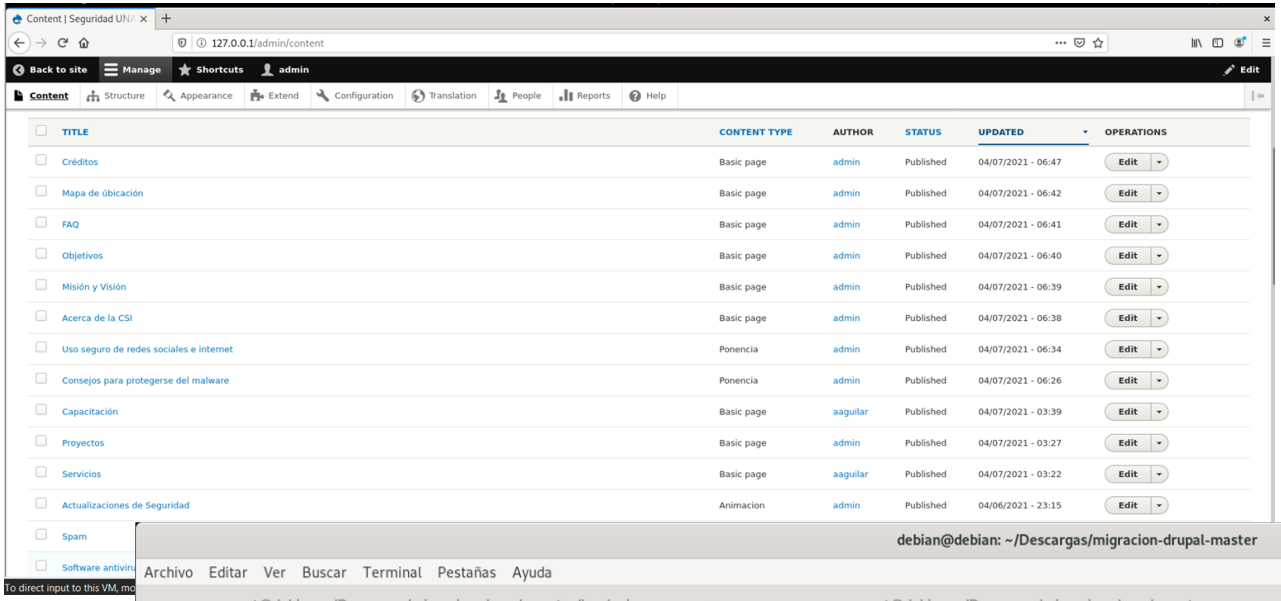


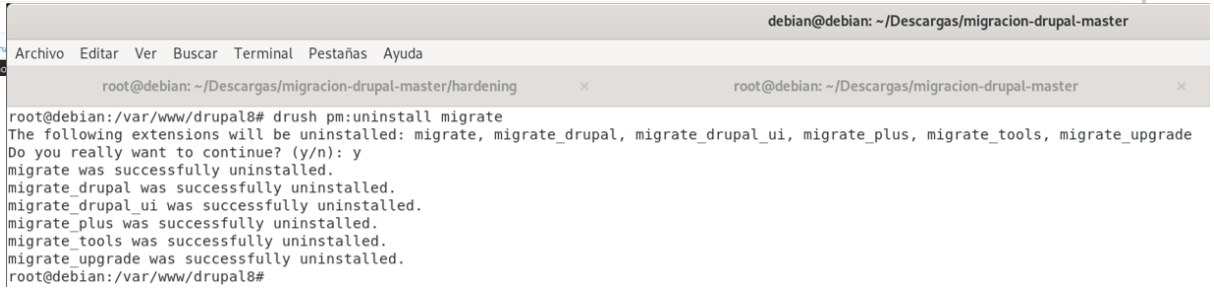
Proceso de migración de Drupal 7 a Drupal 8

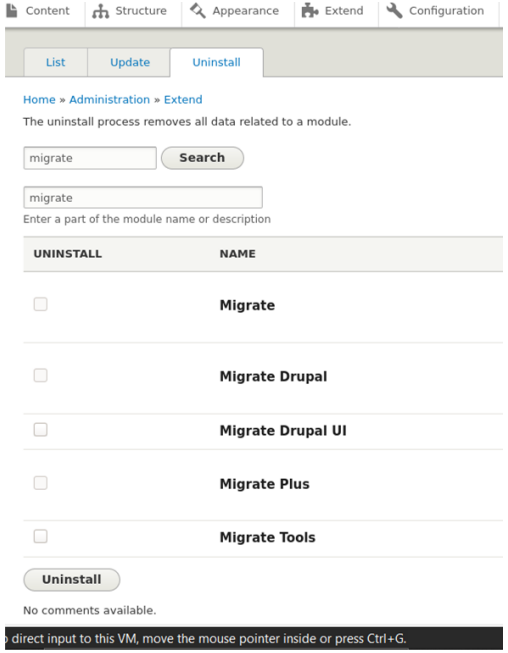
```bash
#!/bin/bash
#variables
ruta="/var/www/drupal7.11"
db="d7"
ip="10.0.0.1"
pas="hola123.,"
name="luis"
echo "Modulos de migracion"
#Habilita los módulos de migración
sudo vendor/bin/drush en migrate_upgrade -y >> archivo.log 2>error.log
sudo vendor/bin/drush en migrate_plus -y >> archivo.log 2>error.log
sudo vendor/bin/drush en migrate_tools -y >> archivo.log 2>error.log
#Conexión para comenzar la migración
sudo vendor/bin/drush migrate-upgrade --legacy-db-url=pgsql://$name:$pas@$ip/$db --legacy-root=http://$ip
#Ver estado de la migración
sudo vendor/bin/drush ms
#Migrar todo el contenido
sudo vendor/bin/drush migrate-import --all
sudo vendor/bin/drush migrate:import upgrade_d7_user_role
sudo vendor/bin/drush migrate:import upgrade_d7_user
#Ver el contenido migrado
sudo vendor/bin/drush ms
```

```
echo "Modulos de migracion"
vendor/bin/drush en migrate_upgrade -y
vendor/bin/drush en migrate_plus -y
vendor/bin/drush en migrate_tools -y
```




Content | Seguridad UNA
127.0.0.1/admin/content
Back to site
Manage
Shortcuts
admin
Edit
Content
Structure
Appearance
Extend
Configuration
Translation
People
Reports
Help
TITLE
CONTENT TYPE
AUTHOR
STATUS
UPDATED
OPERATIONS
Créditos
Basic page
admin
Published
04/07/2021 - 06:47
Edit
Mapa de úbicación
Basic page
admin
Published
04/07/2021 - 06:42
Edit
FAQ
Basic page
admin
Published
04/07/2021 - 06:41
Edit
Objetivos
Basic page
admin
Published
04/07/2021 - 06:40
Edit
Misión y Visión
Basic page
admin
Published
04/07/2021 - 06:39
Edit
Acerca de la CSI
Basic page
admin
Published
04/07/2021 - 06:38
Edit
Uso seguro de redes sociales e internet
Ponencia
admin
Published
04/07/2021 - 06:34
Edit
Consejos para protegerse del malware
Ponencia
admin
Published
04/07/2021 - 06:26
Edit
Capacitación
Basic page
aaguilar
Published
04/07/2021 - 03:39
Edit
Proyectos
Basic page
admin
Published
04/07/2021 - 03:27
Edit
Servicios
Basic page
aaguilar
Published
04/07/2021 - 03:22
Edit
Actualizaciones de Seguridad
Animacion
admin
Published
04/06/2021 - 23:15
Edit
Spam
Software antiviru
To direct input to this VM, mo


debian@debian: ~/Descargas/migracion-drupal-master
Archivo Editar Ver Buscar Terminal Pestañas Ayuda
root@debian: ~/Descargas/migracion-drupal-master/hardening
root@debian: ~/Descargas/migracion-drupal-master
root@debian:/var/www/drupal8# drush pm:uninstall migrate
The following extensions will be uninstalled: migrate, migrate_drupal, migrate_drupal_ui, migrate_plus, migrate_tools, migrate_upgrade
Do you really want to continue? (y/n): y
migrate was successfully uninstalled.
migrate_drupal was successfully uninstalled.
migrate_drupal_ui was successfully uninstalled.
migrate_plus was successfully uninstalled.
migrate_tools was successfully uninstalled.
migrate_upgrade was successfully uninstalled.
root@debian:/var/www/drupal8#


Content
Structure
Appearance
Extend
Configuration
List
Update
Uninstall
Home » Administration » Extend
The uninstall process removes all data related to a module.
migrate
Search
migrate
Enter a part of the module name or description
UNINSTALL
NAME
Migrate
Migrate Drupal
Migrate Drupal UI
Migrate Plus
Migrate Tools
Uninstall
No comments available.
direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Contenido no migrado

Vistas:

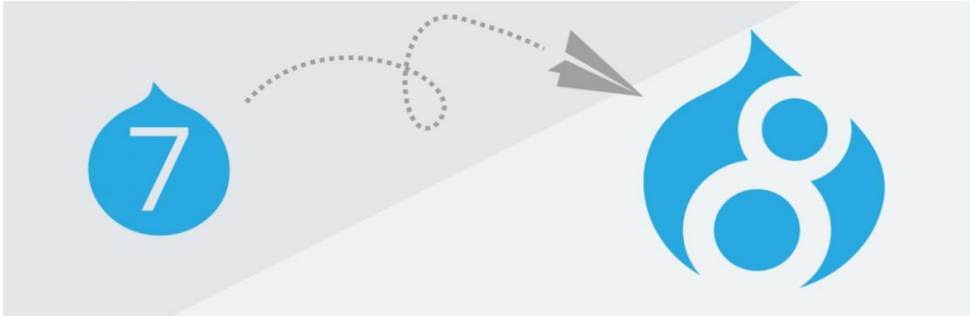
- animaciones-show
- archive
- boletines
- coloquios
- cómics
- consejos
- diccionario
- documentos
- infografías
- noticias
- pentest
- personajes
- presentaciones
- vulnerabilidades

Paneles:

- Estadísticas
- Noticias
- Vulnerabilidades
- Capacitación
- Animaciones
- Consejo de Seguridad UNAM-CERT
- Cómic
- Becarios

Otros:

- Campos de Menú Principal
- Tema del sitio web
- Creación de usuarios



Histórico

```
Python3 cambioextencion.py ./historico
```

```
root@debian: ~
Archivo  Editar  Ver  Buscar  Terminal  Pestañas  Ayuda
root@debian: ~/Descargas
./Descargas/historico/descarga.dsc-arch=3342
Archivos actualizados: 8/12071
```

```
Archivo  Editar  Ver  Buscar  Terminal  Pestañas  Ayuda
root@debian: ~/Descargas/migracion-drupal-master
/home/debian/Descargas/historico/descarga.dsc-arch=3035
Archivos actualizados: 10720/10723
Elapsed time: 3.0103070647 horas
Tiene correo nuevo en /var/mail/root
root@debian:~/Descargas/migracion-drupal-master#
```

seguridad.unam.mx/historico/noticia/index.html-noti=3226

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">
<html>
<head>
        <title>Usuarios de Skype afectados por ransomware en anuncios maliciosos | Noticias - CSI -</title>
        <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
        <meta http-equiv="X-UA-Compatible" content="IE=edge" >
        <meta http-equiv="Vary" content="Accept-Encoding">
        <meta property="fb:admins" content="572144752"/>
        <meta property="fb:app_id" content="217582688303467"/>
        <meta property="og:type" content="appsunamcert:comment">
        <link rel="shortcut icon" href="/historico/vistas/img/icon/dsc.ico">
        <link rel="alternate" type="application/rss+xml" href="/historico/xml.dsc-arch=noticias_dsc" title="Noticias de Seguridad en Computo">
        <link rel="alternate" type="application/rss+xml" href="/historico/xml.dsc-arch=vulne_dsc" title="Vulnerabilidades de Seguridad en Computo">
        <link rel="alternate" type="application/rss+xml" href="../xml.dsc-arch=bol_unam-cert" title="Boletines de Seguridad en Computo, UNAM-CERT">
    <link rel="alternate" type="application/rss+xml" href="../xml.dsc-arch=documentos_dsc" title="Documentos publicados por la CSI/UNAM-CERT">
                <link href="/historico/vistas/css/all/layoutDSC.css" rel="stylesheet" type="text/css" media="screen">
        <!--[if IE]>
                <link href="/vistas/css/all/ie_fix.css" rel="stylesheet" type="text/css" media="screen">
        <![endif]-->

        <!--[if lte IE 6]>
                <link href="/historico/vistas/css/all/ie6_main.css" rel="stylesheet" type="text/css" media="screen">
        <![endif]-->

        <!--[if IE 7]>
        <style type="text/css">
        #submenu li             {width:130px;padding:0;display:inline;}
        </style>
        <![endif]-->
                        <script src="/historico/vistas/js/jquery.min.js" type="text/javascript"></script>              <script src="/historico/vistas/js/anuncios.js"
type="text/javascript"></script>
</head>
```

Problemas presentados

- Migración
- Enlaces Rotos
- Migración de imágenes
- Migración de contenidos
- Tema principal
- Compatibilidad Módulos
- Módulos LDAP Y SMTP

Conclusión

Gracias por su atención