



MY WORDPRESS IN PARANOID MODE

Chema Alonso (@chemaalonso)

<https://www.elevenpaths.com>

<http://www.elladodelmal.com>

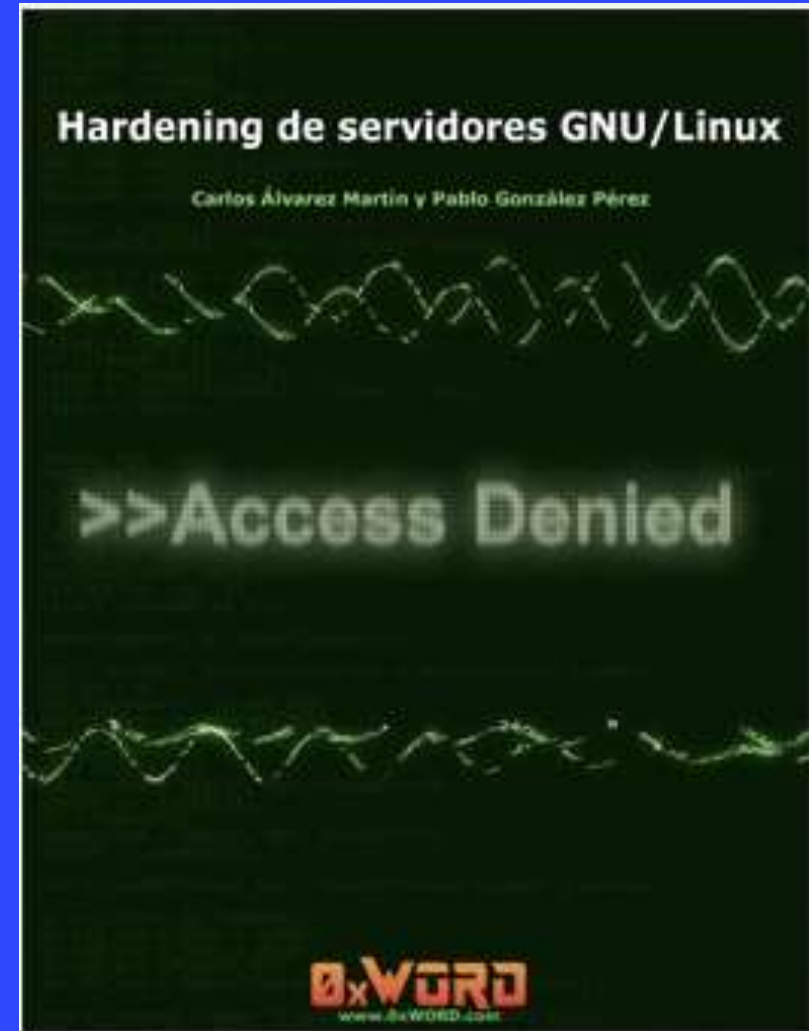
(SOME) WORDPRESS RISKS

- My plugin has a Code Injection Bug
- Someone stole an identity
- My WordPress is under Attack!!



HARDEN IT!

- **Harden OS**
 - (GNU/Linux Hardening)
- **Harden DB**
 - (MySQL Hardenig)
- **Harden WordPress**
 - (Main & Plugins)
- **Harden Users**
 - (Awarness & Tools)

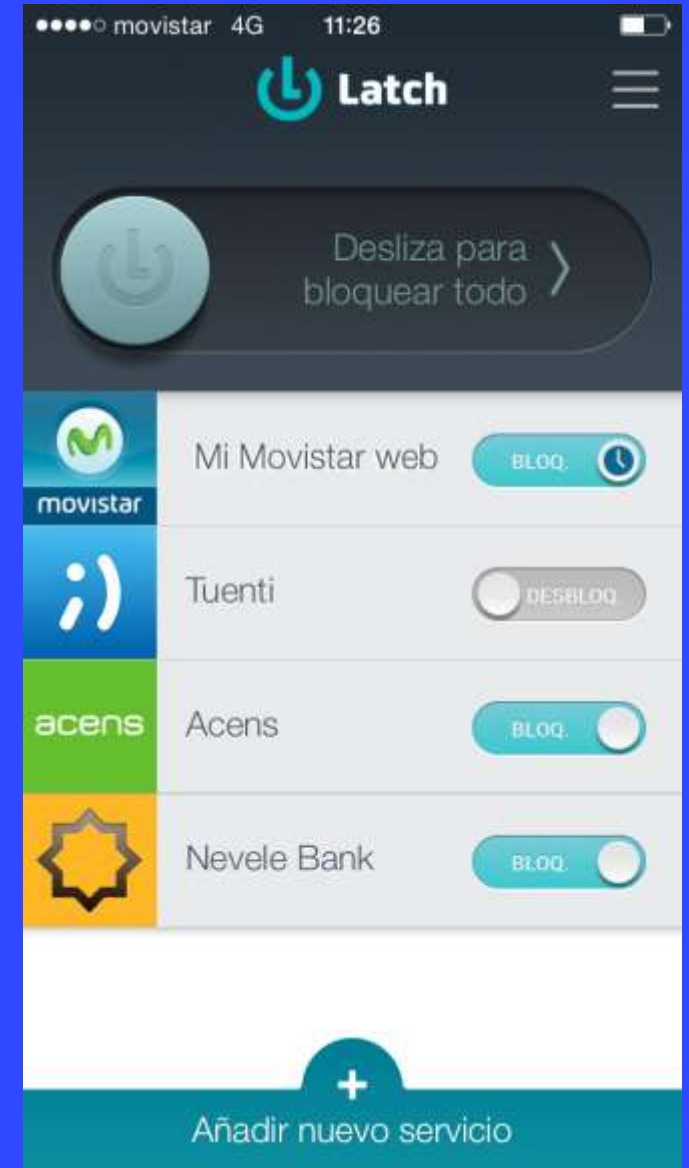


www.Oxword.com

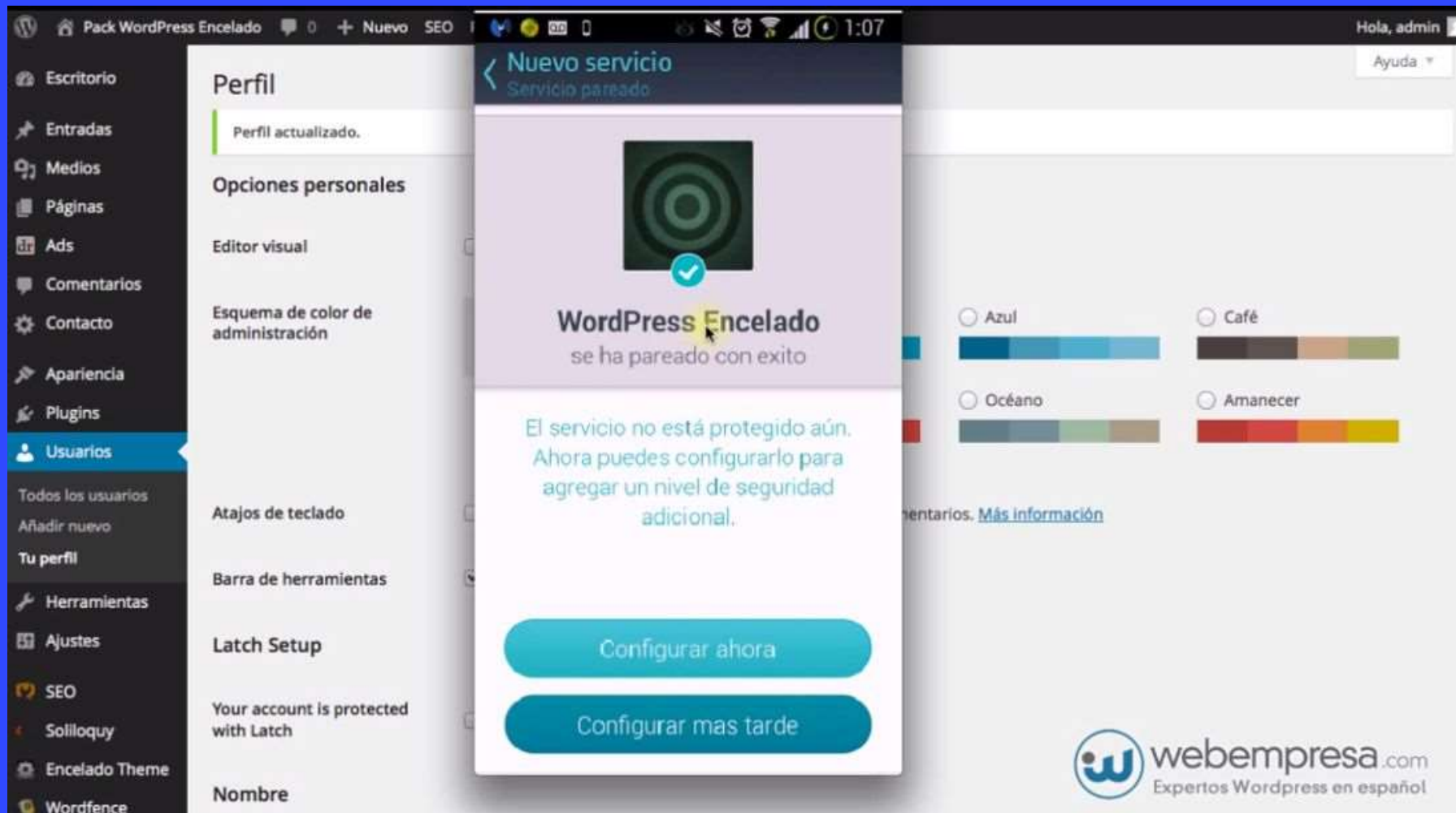
PUT A LATCH ON IT!



Latch



1) HARDEN WORDPRESS USERS

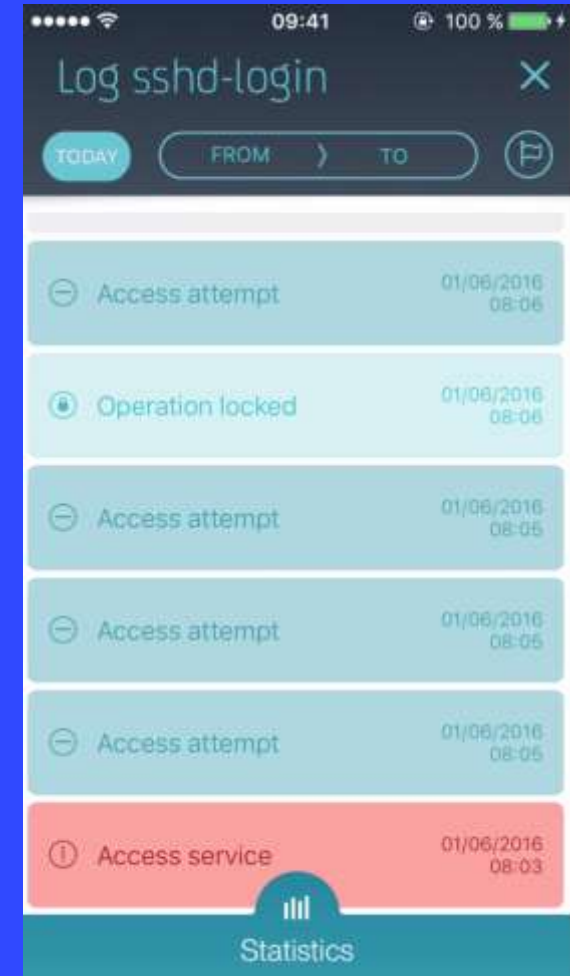
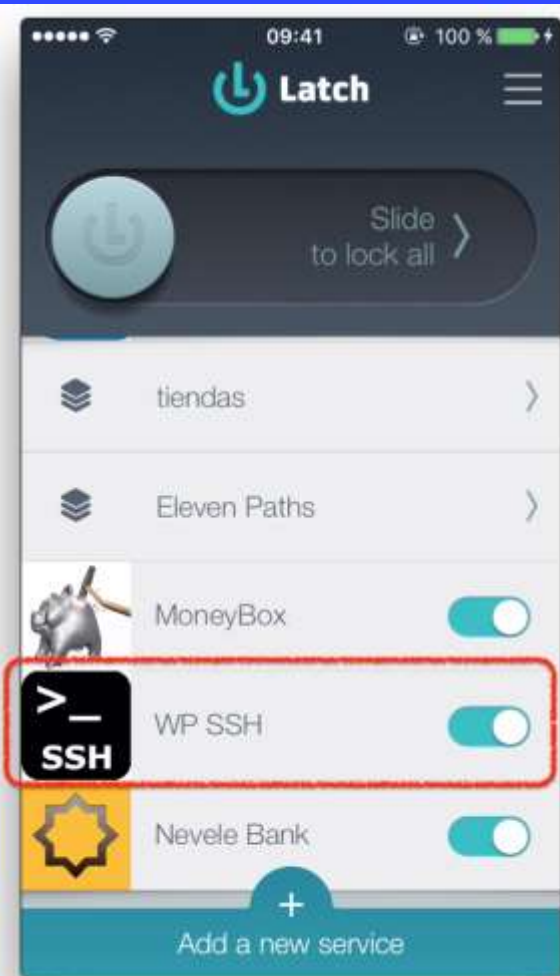


<http://www.slideshare.net/elevenpaths/instalacin-de-latch-en-word-press>

2) HARDEN OS: GNU/LINUX SSH



```
Chemas-MacBook-Pro:~ Chema$ ssh chema@[REDACTED].95
chema@[REDACTED].95's password:
Permission denied, please try again.
chema@[REDACTED].95's password: [REDACTED]
```



3) WORDPRESS IN PARANOID MODE (LATCHING MYSQL DB)

- Create triggers in critical tables of Wordpress
 - This triggers allow or deny 3 actions:
 - Insert
 - Update
 - Delete
 - Trigger verify Latch to carry out an action:
 - Latch ON = Action
 - Latch OFF = Blocked




CREATE LATH APP (LATCH DEVELOPER AREA)

Mis aplicaciones

[Inicio](#) > [Mis aplicaciones](#)

[Editar](#)



[Directrices de imágenes](#) ?

Ni...do

Nombre

ID de aplicación ?

Secreto

2º factor OTP

Bloquear tras consultar

Operaciones

<https://latch.elevenpaths.com>

INSTALL WPM

(./INSTALL.SH <APPID> <SECRET>)

```
pgonzalez@pg-usrv01:~/latchBD$ ./install.sh J3HgQDAvF4[REDACTED] QeMJ8iBtUpCefj[REDACTED]
```



WPM

Wordpress in Paranoid Mode with Latch
Chema Alonso & Pablo González @elevenpaths

Go to Install? ENTER...

STEP 1: PAIRING MYSQL & LATCH

(GIVE ME TOKEN => PAIRING)

Go to Install? ENTER...

Step 1: Pairing with Latch

Give me token:8xqbh2

Pairing...

Account ID: frrUxzjysk JrNVLmwMet2WYZ



STEP 2&3: CREATING OPERATIONS (RELAX AND ENJOY)

```
Step 2: Creating Ruby files for Latch operations
=====

Copying comment_template.rb to comment.rb
Copying post_template.rb to post.rb
Copying users_template.rb to users.rb
```



```
Step 3: Create Operations
=====

Creating ReadOnly Operation...
MsZQL [redacted]

Creating Edition Operation...
Tk3V4 [redacted]

Creating Administration Operation
xpDDJ2 [redacted]
```



STEP 4: COMPILATION & INSTALL

(LIB_MYSQL_UDF.SO)

```
Step 4: Setup lib mysql udf so
```

```
=====
```

```
Leyendo lista de paquetes... Hecho
```

```
Creando árbol de dependencias
```

```
Leyendo la información de estado... Hecho
```

```
Se instalarán los siguientes paquetes NUEVOS:
```

```
  libmysqlclient-dev
```

```
0 actualizados, 1 nuevos se instalarán, 0 para eliminar y 287 no actualizados.
```

```
Se necesita descargar 0 B/999 kB de archivos.
```

```
Se utilizarán 6.337 kB de espacio de disco adicional después de esta operación.
```

```
Seleccionando el paquete libmysqlclient-dev previamente no seleccionado.
```

```
(Leyendo la base de datos ... 188538 ficheros o directorios instalados actualmente.)
```

```
Preparando para desempaquetar .../libmysqlclient-dev_5.6.28-0ubuntu0.15.04.1_amd64.deb ...
```

```
Desempaquetando libmysqlclient-dev (5.6.28-0ubuntu0.15.04.1) ...
```

```
Procesando disparadores para man-db (2.7.0.2-5) ...
```

```
Configurando libmysqlclient-dev (5.6.28-0ubuntu0.15.04.1) ...
```

STEP 5: UNLOAD MYSQL PROFILE

(MYSQL APPARMOR PROFILE BLOCK CODE EXECUTION)

```
Step 5: AppArmor Configuration
```

```
=====
```

```
File /etc/apparmor.d/usr.sbin mysqld not found, skipping...
```

```
Reboot MySQL, if this fail, you need reboot MySQL
```

```
[ ok ] Restarting mysql (via systemctl): mysql.service.
```

```
sudo ln -s /etc/apparmor.d/usr.sbin.mysqld /etc/apparmor.d/disable/  
sudo apparmor_parser -R /etc/apparmor.d/usr.sbin.mysqld  
echo "Reboot MySQL, if this fail, you need reboot MySQL"  
sudo /etc/init.d/mysql restart
```

STEP 6: CREATING MYSQL TRIGGERS

(READ-ONLY, ADMINISTRATION, EDITION)

Step 6: Creating Triggers on MySQL

Enter password:

Success! Triggers on MySQL



< Latch WPM ≡



ReadOnly ☒

Edition ☐

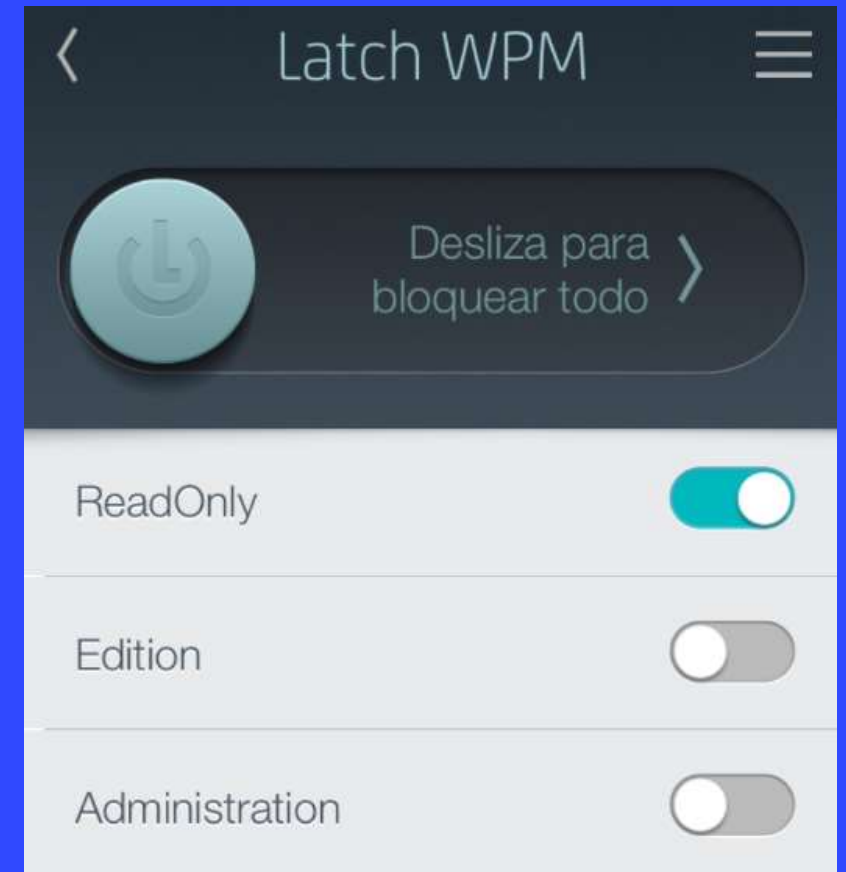
Administration ☐

YOU GOT LATCH IN WPM



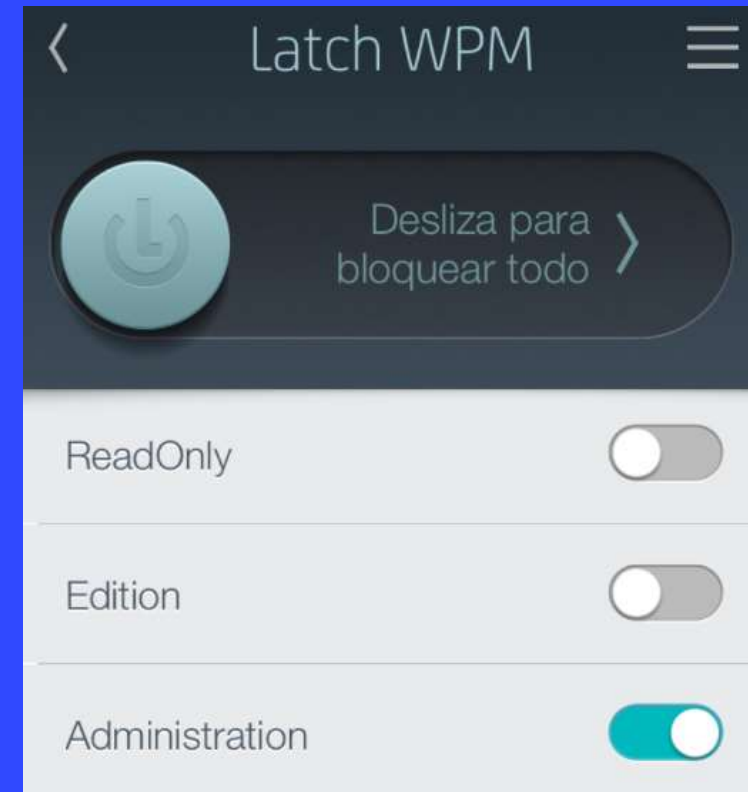
LATCH WPM: READ-ONLY MODE

- **Read-Only Mode:**
 - Nobody can login in WordPress.
 - No one can make changes in MySQL.
- **wp_usermeta Table:**
 - insert, delete and update blocked if 'read-only' operation enabled
 - If 'read-only' mode is deactivated then you can login



LATCH: ADMINISTRATION MODE





- **Protects:**
 - Delete on wp_users
 - Update on wp_users
 - Insert on wp_users
- **SQL Injection Bugs:**
 - No Delete
 - No Update
 - No Insert



LATCH: ADMINISTRATION MODE

All (4) | Administrator (3) | Subscriber (1)

Bulk Actions ▾ Apply Change role to... ▾ Change

<input type="checkbox"/>	Username
<input type="checkbox"/>	 chema
<input type="checkbox"/>	 pablo Edit Delete
<input type="checkbox"/>	 pepe
<input type="checkbox"/>	 wordpress

Delete Users

You have specified this user for deletion:

ID #2: pablo


What should be done with content owned by this user?

☒ Delete all content.

☐ Attribute all content to:

[Confirm Deletion](#)

Intento de acceso ×



**Latch WPM
(Administration)**

Probablemente has intentado acceder al servicio que tienes bloqueado.

Si no fuiste tú y las alertas continúan, recomendamos cambiar tu contraseña y contactar con el proveedor del servicio.

- Trigger on wp_users:
 - Delete Action
 - Verify Latch
 - Abort SQL Operation

QUESTIONS?

- WPM -WordPress in Paranoid Mode

- <https://github.com/elevenpaths>
- <https://community.elevenpaths.com>

- Chema Alonso
- (@chemaalonso)

- <https://www.elevenpaths.com>
- <http://www.elladodelmal.com>

