



Aprende de los
ataques para hacer
tu WordPress más
seguro

Córdoba, 13 de mayo de 2017

Miguel Ángel Arroyo - @miguel_arroyo76

NUEVA **2017** EDICIÓN

VI Córdoba

WordPress

meetup



✕ ★★★ **PARA DESARROLLADORES,
CREATIVOS Y CURIOSOS** ★★★

12-13 DE MAYO DE 2017

VIERNES 12: 17-21 HORAS / SÁBADO 13: 10-14 HORAS
FACULTAD DE CIENCIAS DEL TRABAJO

2017.wpcordoba.org

#whoami

IS Auditor – SVT Cloud Security Services

Hack&Beers founder

Hacking Solidario co-founder

Twitter: @miguel_arroyo76

Blog: www.hacking-etico.com



WordPress Meetup Córdoba 2017
VI EDICIÓN



El arte de la guerra es un libro sobre tácticas y estrategias militares, escrito por Sun Tzu, un famoso estratega militar chino.

Sun
Tzu's
THE
ART
OF
WAR

孫子兵法



WordPress Meetup Córdoba 2017
VI EDICIÓN

El arte de la guerra: Tu WordPress VS Tus Atacantes




WordPress Meetup Córdoba 2017
VI EDICIÓN

Estrategia de seguridad para WordPress basada en algunas de las mejores frases de Sun Tzu en el Arte de la Guerra.



WordPress Meetup Córdoba 2017
VI EDICIÓN

1. Uno puede conocer la condición de todo un ejército por el comportamiento de un simple hombre.



intitle:phpinfo site:es

Todo Imágenes Shopping Vídeos Libros Más Configuración Herramientas

Aproximadamente 141 resultados (0,26 segundos)

[Crear un archivo phpinfo | Blog Unelink](#)
blog.unelink.es/wiki/php/crear-un-archivo-phpinfo/ ▼
3 jun. 2011 - Existe una función en php llamada phpinfo(). Dicha función imprime toda la configuración de su archivo php.ini formateada y nos permite ...

[donde esta el phpinfo - PHP - Foro de soporte - miarroba ES](#)
soporte.miarroba.es/17451/10734331-donde-esta-el-phpinfo/ ▼
29 jun. 2012 - que tal una simple pregunta el phpinfo siempre tan util por que esta deshabilitado o tal vez no doy como encontrarlo ...

[phpinfo\(\) - Cruz Roja](#)
www.cruzroja.es/info?a%5B%5D=phpinfo ▼ Traducir esta página
System, SunOS iasrv1 5.10 Generic_147440-01 sun4v. Build Date, Jul 13 2005 01:42:58. Configure Command, './configure' ...

PHP Version 5.1.6 

System	Linux Isiweb.Isi.us.es 2.6.18-400.1.1.el5 #1 SMP Sun Dec 14 06:01:17 EST 2014 x86_64
Build Date	Oct 28 2014 09:20:15
Configure Command	./configure '--build=x86_64-redhat-linux-gnu' '--host=x86_64-redhat-linux-gnu' '--target=x86_64-redhat-linux-gnu' '--program-prefix=' '--prefix=/usr' '--exec-prefix=/usr' '--bindir=/usr/bin' '--sbindir=/usr/sbin' '--sysconfdir=/etc' '--datadir=/usr/share' '--includedir=/usr/include' '--libdir=/usr/lib64' '--libexecdir=/usr/libexec' '--localstatedir=/var' '--sharedstatedir=/usr/com' '--mandir=/usr/share/man' '--infodir=/usr/share/info' '--cache-file=../config.cache' '--with-libdir=lib64' '--with-config-file-path=/etc' '--with-config-file-scandir=/etc/php.d' '--disable-debug' '--with-pic' '--disable-rpath' '--without-pear' '--with-bz2' '--with-curl' '--with-exec-dir=/usr/bin' '--with-freetype-dir=/usr' '--with-png-dir=/usr' '--enable-gd-native-ttf' '--without-gd' '--with-gettext' '--with-gmp' '--with-iconv' '--with-jpeg-dir=/usr' '--with-openssl' '--with-png' '--with-pspell' '--with-ldap-dir=/usr' '--with-pcre-regex=/usr' '--with-zlib' '--with-layout=GNU' '--enable-exif' '--enable-ftp' '--enable-magic-quotes' '--enable-sockets' '--enable-sysvsem' '--enable-sysvshm' '--enable-sysvmsg' '--enable-track-vars' '--enable-trans-sid' '--enable-yp' '--enable-wddx' '--with-kerberos' '--enable-ucd-snmp-hack' '--with-unixODBC=shared,/usr' '--enable-memory-limit' '--enable-shmop' '--enable-calendar' '--enable-dbx' '--enable-dio' '--with-mime-magic=/usr/share/file/magic.mime' '--without-sqlite' '--with-libxml-dir=/usr' '--with-xml' '--with-system-tdata' '--with-apxs2=/usr/sbin/apxs' '--without-mysql' '--without-gd' '--without-odbc' '--disable-dom' '--disable-dba' '--without-unixODBC' '--disable-pdo' '--disable-xmlreader' '--disable-xmlwriter'
Server API	Apache 2.0 Handler

2. El que es prudente y está a la espera de un enemigo que no lo es, será victorioso.

```
C:\Users\Miguel>ping www.wpcordoba.org
```

```
Haciendo ping a wpcordoba.org [192.254.189.65] con 32 bytes de datos:  
Respuesta desde 192.254.189.65: bytes=32 tiempo=218ms TTL=50
```



ip:192.254.189.65

Web Imágenes Vídeos Mapas Noticias

6.720 RESULTADOS Fecha Idioma Región

Luis Serrano Pallarés - Ingeniero Técnico Agrícola en Córdoba
luiserranopallares.com
Luis Serrano Pallarés - Ingeniero Técnico Agrícola Córdoba - Topografía, peritaciones y valoraciones - Córdoba

Personaliza WordPress - Información, tutoriales, themes ...
personalizawp.com
Información, tutoriales, themes, plugins y todo sobre WordPress y WooCommerce

Farmacia de la Espartería
farmaciadelaesparteria.es
Farmacia de la Espartería, ubicada en Córdoba junto a la plaza de la corredera

Sun-Dance.org - Aotearoa Traducir esta página
www.sun-dance.org
Leonard Crow Dog (Kangi Shunka Manitou), Sundance elder/chief of the Paradise grounds in Rosebud, South Dakota, USA received and acknowledged a jar of Manuka ...

Programa – WordPress Meetup Córdoba 2017
2017.wpcordoba.org/programa
Sign up with your email address to be the first to know about new products, VIP offers, blog features & more.

WordPress Meetup Córdoba 2017

VI EDICIÓN

3. *Maniobrar con un ejército es ventajoso. Maniobrar con una multitud indisciplinada, es peligroso.*



Jetpack by WordPress.com

WordfenceTM
Securing your **WordPress** website

Better WP Security is now
iThemes Security

More than 30 ways to protect your site from attacks.

WordPress Meetup Córdoba 2017
VI EDICIÓN

4. Si conoces al enemigo y a ti mismo, no debes temer el resultado a un ciento de batallas.




```
207.46.13.240 - - [09/Apr/2017:13:36:29 +0000] "GET /robots.txt HTTP/1.0" 200 67 "-" "Mozilla/5.0 (cor
207.46.13.240 - - [09/Apr/2017:13:36:30 +0000] "GET /robots.txt HTTP/1.0" 200 67 "-" "Mozilla/5.0 (cor
207.46.13.240 - - [09/Apr/2017:13:36:28 +0000] "GET /robots.txt HTTP/1.0" 200 67 "-" "Mozilla/5.0 (cor
207.46.13.240 - - [09/Apr/2017:13:36:32 +0000] "GET /robots.txt HTTP/1.0" 200 67 "-" "Mozilla/5.0 (cor
163.172.150.74 - - [09/Apr/2017:13:36:30 +0000] "POST /wp-cron.php?doing_wp_cron=1491744990.4251799583
/wp-cron.php?doing_wp_cron=1491744990.4251799583435058593750" "WordPress/4.6.4; http://[redacted]
45.58.117.234 - - [09/Apr/2017:13:41:22 +0000] "GET / HTTP/1.0" 200 45167 "http://[redacted]
like Gecko) Chrome/39.0.2171.95 Safari/537.36 OPR/26.0.1656.60"
104.168.68.171 - - [09/Apr/2017:13:41:27 +0000] "GET /wp-login.php?action=register HTTP/1.0" 404 39196
6.2; Win64; x64) Presto/2.12.388 Version/12.17"
104.168.68.171 - - [09/Apr/2017:13:41:30 +0000] "GET /wp-login.php?action=register HTTP/1.0" 404 39196
"Opera/9.80 (Windows NT 6.2; Win64; x64) Presto/2.12.388 Version/12.17"
104.168.68.171 - - [09/Apr/2017:13:41:38 +0000] "POST /-/-/-/-/-/-/-/-/-/-/- HTTP/1.0" 404 39317 "http://
"Opera/9.80 (Windows NT 6.2; Win64; x64) Presto/2.12.388 Version/12.17"
104.168.68.171 - - [09/Apr/2017:13:41:43 +0000] "POST /-/-/-/-/-/-/-/-/-/-/- HTTP/1.0" 404 39317 "http://
"Opera/9.80 (Windows NT 6.2; Win64; x64) Presto/2.12.388 Version/12.17"
104.168.68.171 - - [09/Apr/2017:13:41:47 +0000] "POST /-/-/-/-/-/-/-/-/-/-/- HTTP/1.0" 404 39317 "http://
"Opera/9.80 (Windows NT 6.2; Win64; x64) Presto/2.12.388 Version/12.17"
104.168.68.171 - - [09/Apr/2017:13:41:51 +0000] "POST /-/-/-/-/-/-/-/-/-/-/- HTTP/1.0" 404 39317 "http://
"Opera/9.80 (Windows NT 6.2; Win64; x64) Presto/2.12.388 Version/12.17"
207.46.13.180 - - [09/Apr/2017:14:14:01 +0000] "GET /login HTTP/1.0" 200 47313 "-" "msnbot-media/1.1
207.46.13.180 - - [09/Apr/2017:14:32:39 +0000] "GET / HTTP/1.0" 200 45167 "-" "Mozilla/5.0 (compatible
66.249.83.139 - - [09/Apr/2017:22:13:29 +0000] "GET / HTTP/1.0" 200 45167 "-" "Mozilla/5.0 (X11; Linux
Chrome/49.0.2623.75 Safari/537.36 Google Favicon"
```

WordPress Meetup Córdoba 2017

VI EDICIÓN

5. No hay más de cinco notas musicales, sin embargo, las combinaciones de éstas cinco dan como resultado más melodías de las que pueden escucharse.

183.60.244.37




```
[Fri Apr 15 16:27:21 2016] [error] [client 183.60.244.37] File does not exist
[Fri Apr 15 16:27:21 2016] [error] [client 183.60.244.37] File does not exist
[Fri Apr 15 16:27:22 2016] [error] [client 183.60.244.37] File does not exist
[Fri Apr 15 16:27:22 2016] [error] [client 183.60.244.37] File does not exist
[Fri Apr 15 16:27:23 2016] [error] [client 183.60.244.37] File does not exist
[Fri Apr 15 16:27:23 2016] [error] [client 183.60.244.37] File does not exist
[Fri Apr 15 16:27:23 2016] [error] [client 183.60.244.37] File does not exist
[Fri Apr 15 16:27:23 2016] [error] [client 183.60.244.37] File does not exist
[Fri Apr 15 16:27:24 2016] [error] [client 183.60.244.37] File does not exist
[Fri Apr 15 16:27:24 2016] [error] [client 183.60.244.37] File does not exist
[Fri Apr 15 16:27:24 2016] [error] [client 183.60.244.37] File does not exist
[Fri Apr 15 16:27:25 2016] [error] [client 183.60.244.37] File does not exist
```



WordPress Meetup Córdoba 2017
VI EDICIÓN

6. Nunca interrumpas a tu enemigo cuando está cometiendo un error.



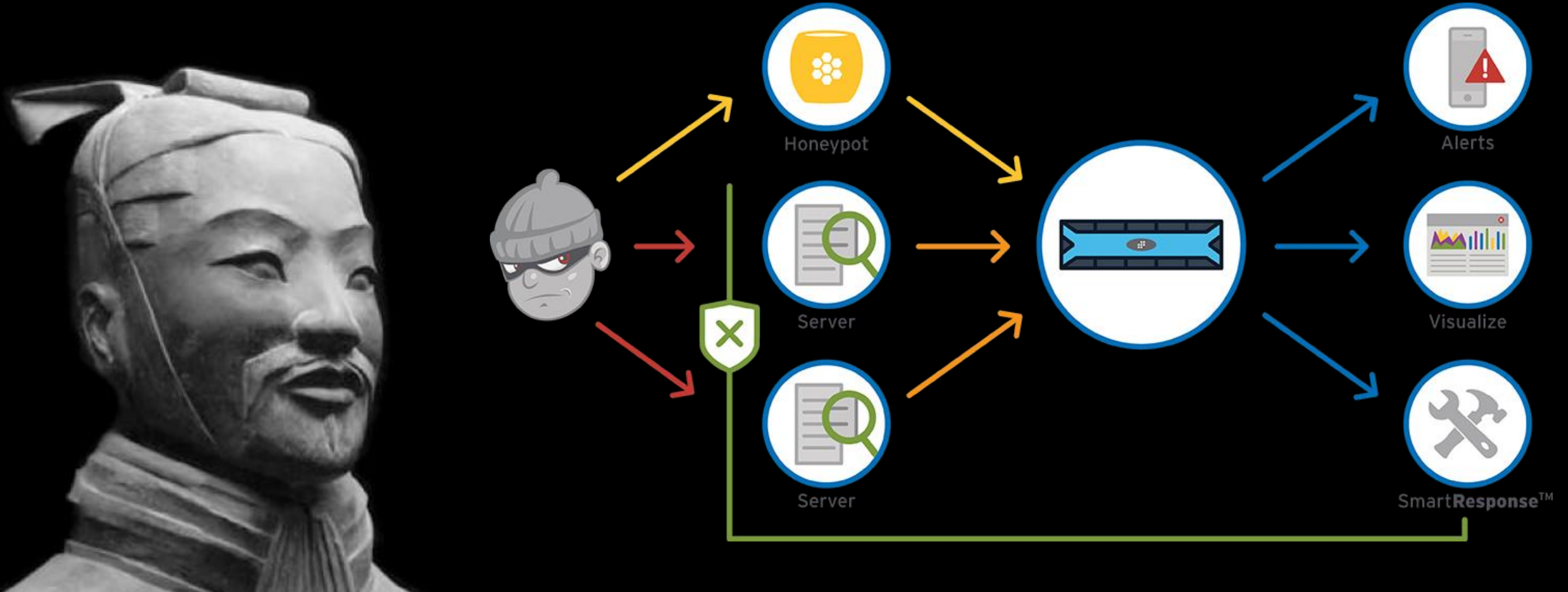
```
[Fri Feb 10 16:30:08 2017] [error] [client 195.154.194.116] File does not exist: /usr/www/ /blog
[Fri Feb 10 16:30:08 2017] [error] [client 195.154.194.116] File does not exist: /usr/www/ /blog
[Fri Feb 10 16:30:08 2017] [error] [client 195.154.194.116] File does not exist: /usr/www/ /wordpress
[Fri Feb 10 16:30:08 2017] [error] [client 195.154.194.116] File does not exist: /usr/www/ /wp
[Fri Feb 10 16:30:09 2017] [error] [client 195.154.194.116] File does not exist: /usr/www/ /administrator
[Fri Feb 10 16:30:09 2017] [error] [client 195.154.194.116] File does not exist: /usr/www/ /blog
[Fri Feb 10 16:30:09 2017] [error] [client 195.154.194.116] File does not exist: /usr/www/ /blog
[Fri Feb 10 16:30:09 2017] [error] [client 195.154.194.116] File does not exist: /usr/www/ joomla
[Fri Feb 10 16:30:09 2017] [error] [client 195.154.194.116] File does not exist: /usr/www/ joomla
[Fri Feb 10 16:30:10 2017] [error] [client 195.154.194.116] File does not exist: /usr/www/ /bitrix
```

```
[Sat Nov 26 14:56:04 2016] [error] [client 178.162.205.5] File does not exist: /usr/www/ /downloader,
[Sat Nov 26 17:48:28 2016] [error] [client 106.185.44.224] File does not exist: /usr/www/ /favicon.ico,
[Sat Nov 26 18:34:53 2016] [error] [client 45.32.10.93] File does not exist: /usr/www/ /favicon.ico, re
[Sat Nov 26 19:20:16 2016] [error] [client 111.12.97.52] File does not exist: /usr/www/ /favicon.ico,
[Sat Nov 26 20:05:39 2016] [error] [client 60.249.100.237] File does not exist: /usr/www/ /favicon.ico,
[Sat Nov 26 20:07:19 2016] [error] [client 43.250.8.30] File does not exist: /usr/www/ /favicon.ico, re
```

WordPress Meetup Córdoba 2017

VI EDICIÓN

7. Si la mitad de sus tropas avanza y la otra mitad retrocede, es que el enemigo piensa atraerte a una trampa.



WordPress Meetup Córdoba 2017
VI EDICIÓN

8. Puedes asegurar la posición de tus defensas si sólo mantienes posiciones que no pueden ser atacadas.



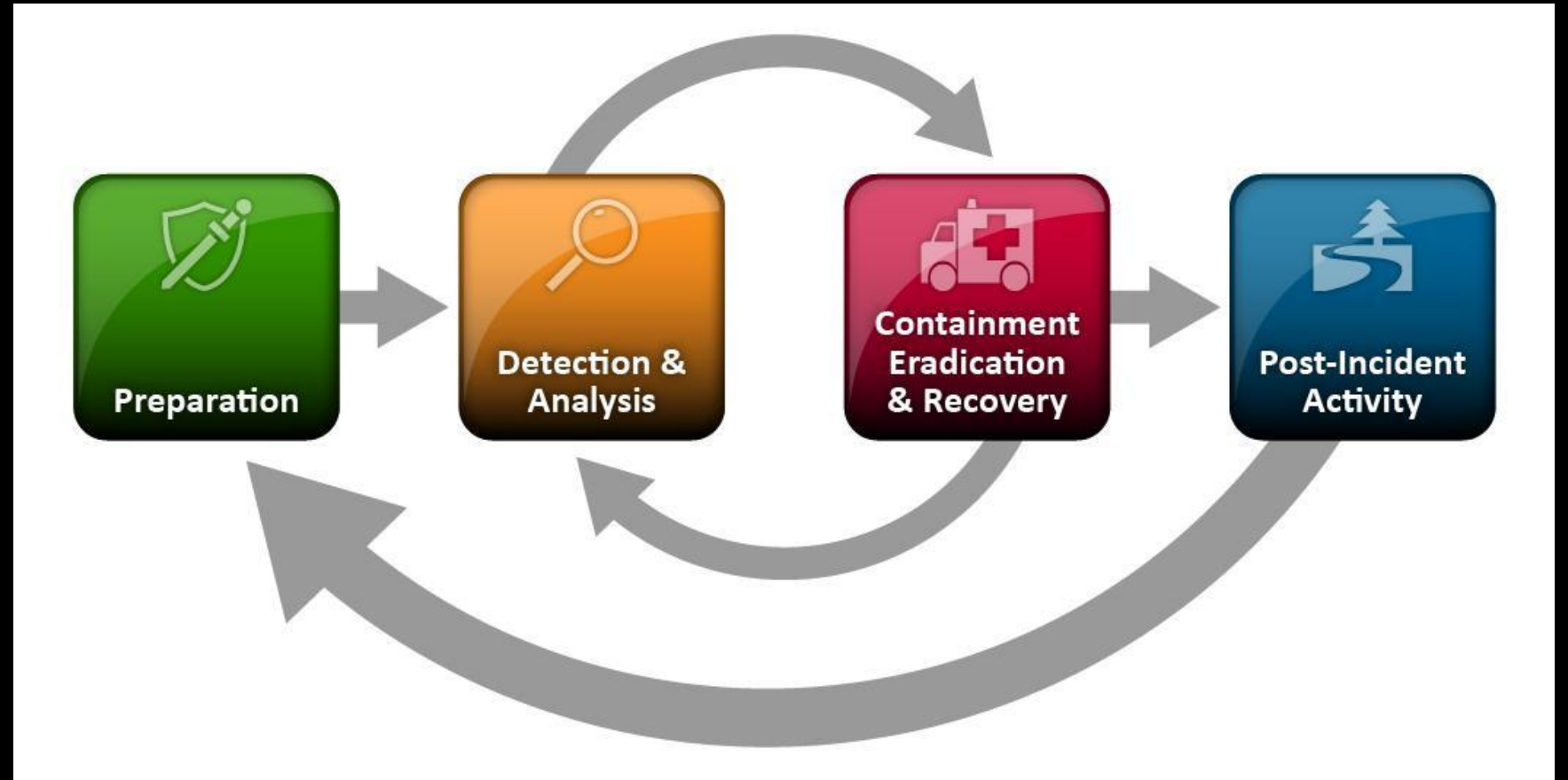
WordPress Meetup Córdoba 2017
VI EDICIÓN

9. Sólo cuando conoces cada detalle de la condición del terreno puedes maniobrar y luchar.



WordPress Meetup Córdoba 2017
VI EDICIÓN

10. La rapidez es la esencia de la guerra.



WordPress Meetup Córdoba 2017
VI EDICIÓN



WordPress Meetup Córdoba 2017

VI EDICIÓN