WORDCAMP BILBAO mayo 2017

Plugins de seguridad, tiburones, gatitos y elefantes.

WordCamp BILBAO 2017

Security Hell Conference

netkia

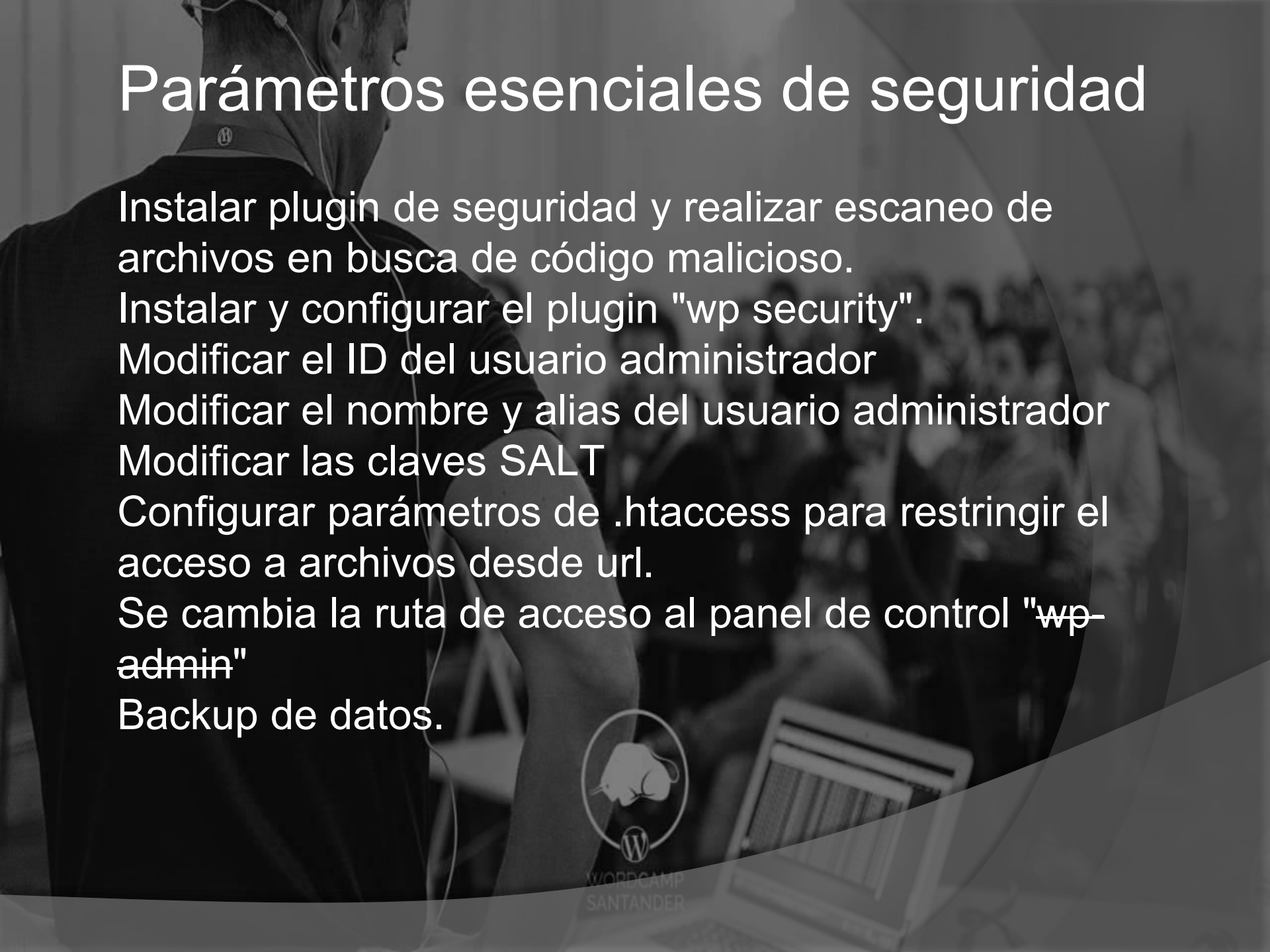
Tomás Sierra

Parámetros esenciales de seguridad

Backup preventivo
Actualización de plugins y tema.
Modificar prefijos de la base de datos.
Modificar permisos en archivos y directorios.
Fortificar archivos críticos.
Indexar directorios para impedir listado de archivos.
Deshabilitar el editor de archivos del BackEnd.
Deshabilitar y desinstalar plugins inactivos.

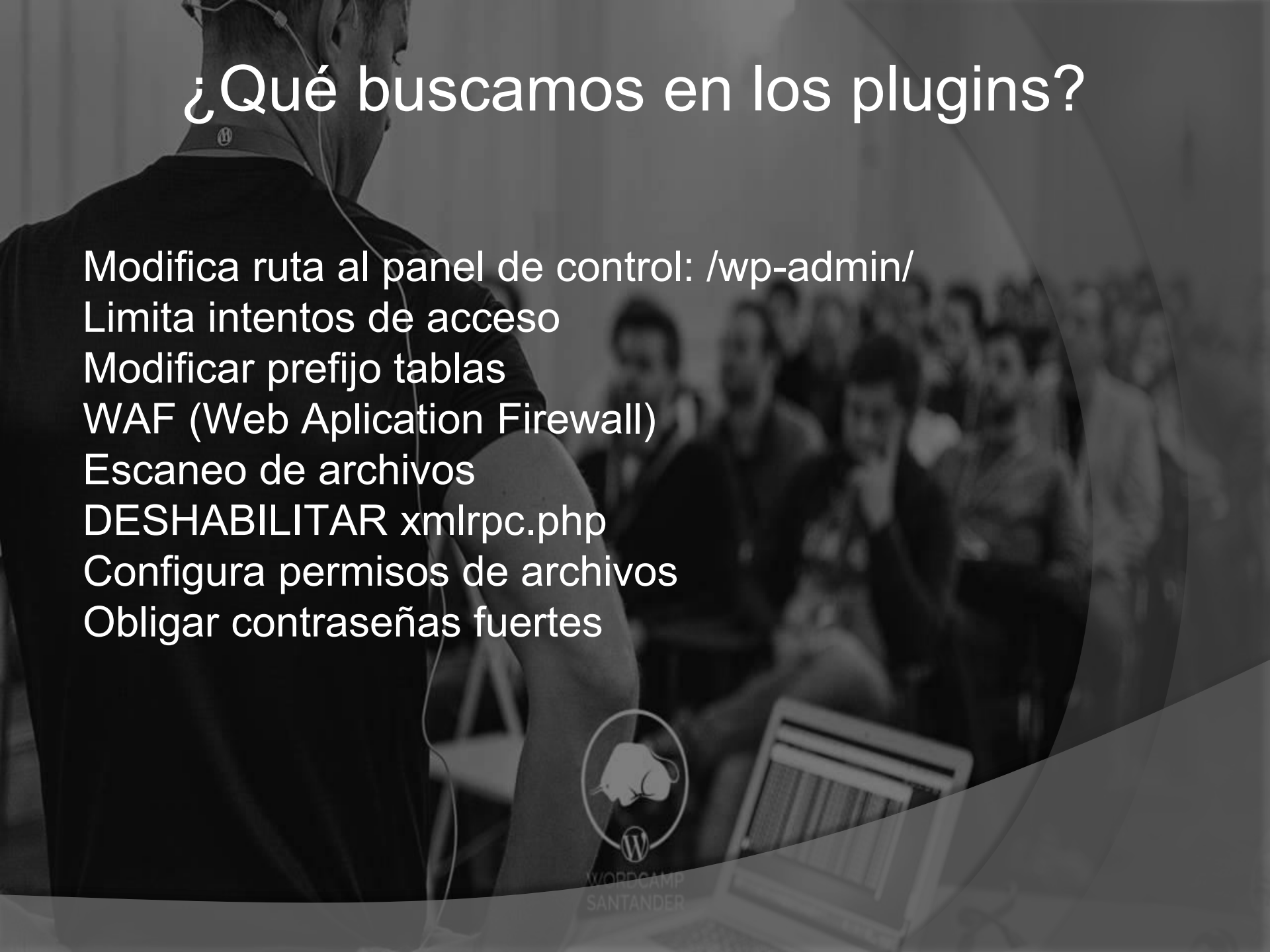
Parámetros esenciales de seguridad

Instalar plugin de seguridad y realizar escaneo de archivos en busca de código malicioso.
Instalar y configurar el plugin "wp security".
Modificar el ID del usuario administrador
Modificar el nombre y alias del usuario administrador
Modificar las claves SALT
Configurar parámetros de .htaccess para restringir el acceso a archivos desde url.
Se cambia la ruta de acceso al panel de control "~~wp-admin~~"
Backup de datos.



¿Qué buscamos en los plugins?

Modifica ruta al panel de control: /wp-admin/
Limita intentos de acceso
Modificar prefijo tablas
WAF (Web Aplication Firewall)
Escaneo de archivos
DESHABILITAR xmlrpc.php
Configura permisos de archivos
Obligar contraseñas fuertes



Parámetros esenciales de seguridad

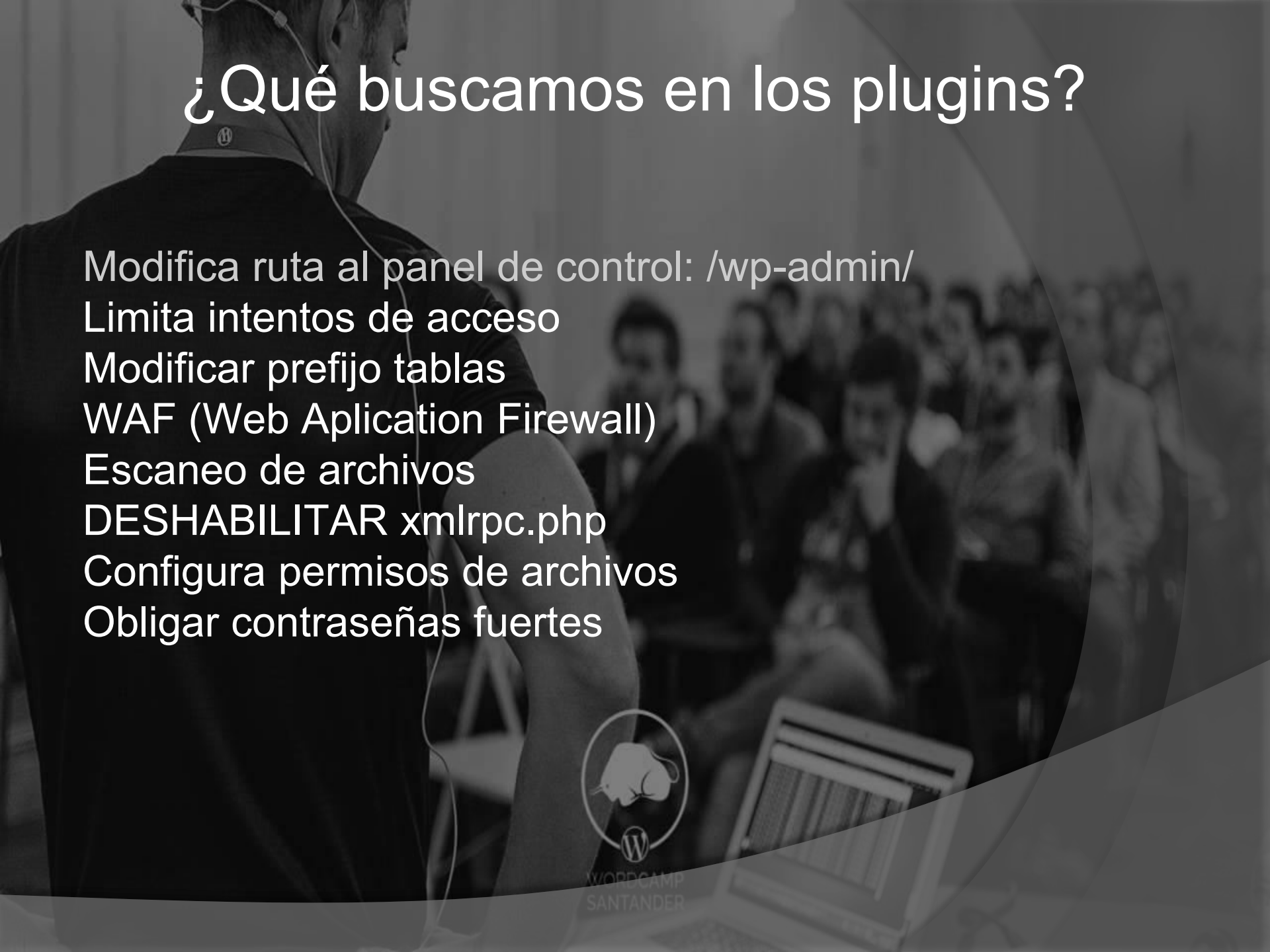
Esconder la ruta de acceso al panel de control

http://www.miweb.com/wp-admin

http://www.miweb.com/paneldegestion

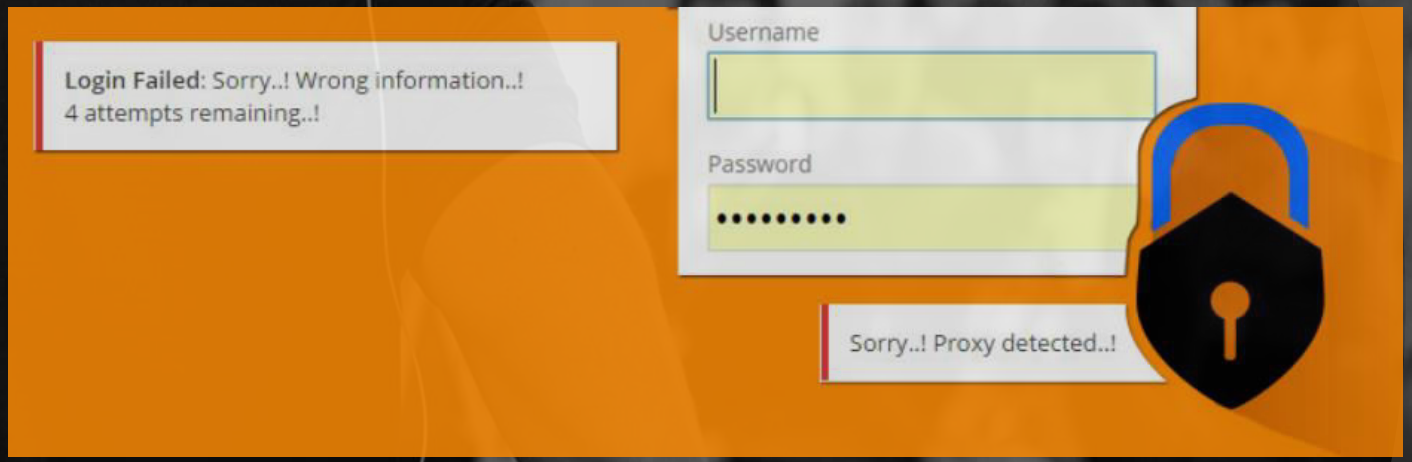
¿Qué buscamos en los plugins?

Modifica ruta al panel de control: /wp-admin/
Limita intentos de acceso
Modificar prefijo tablas
WAF (Web Aplication Firewall)
Escaneo de archivos
DESHABILITAR xmlrpc.php
Configura permisos de archivos
Obligar contraseñas fuertes



Parámetros esenciales de seguridad

Limitar el número de intentos de acceso al panel de control.



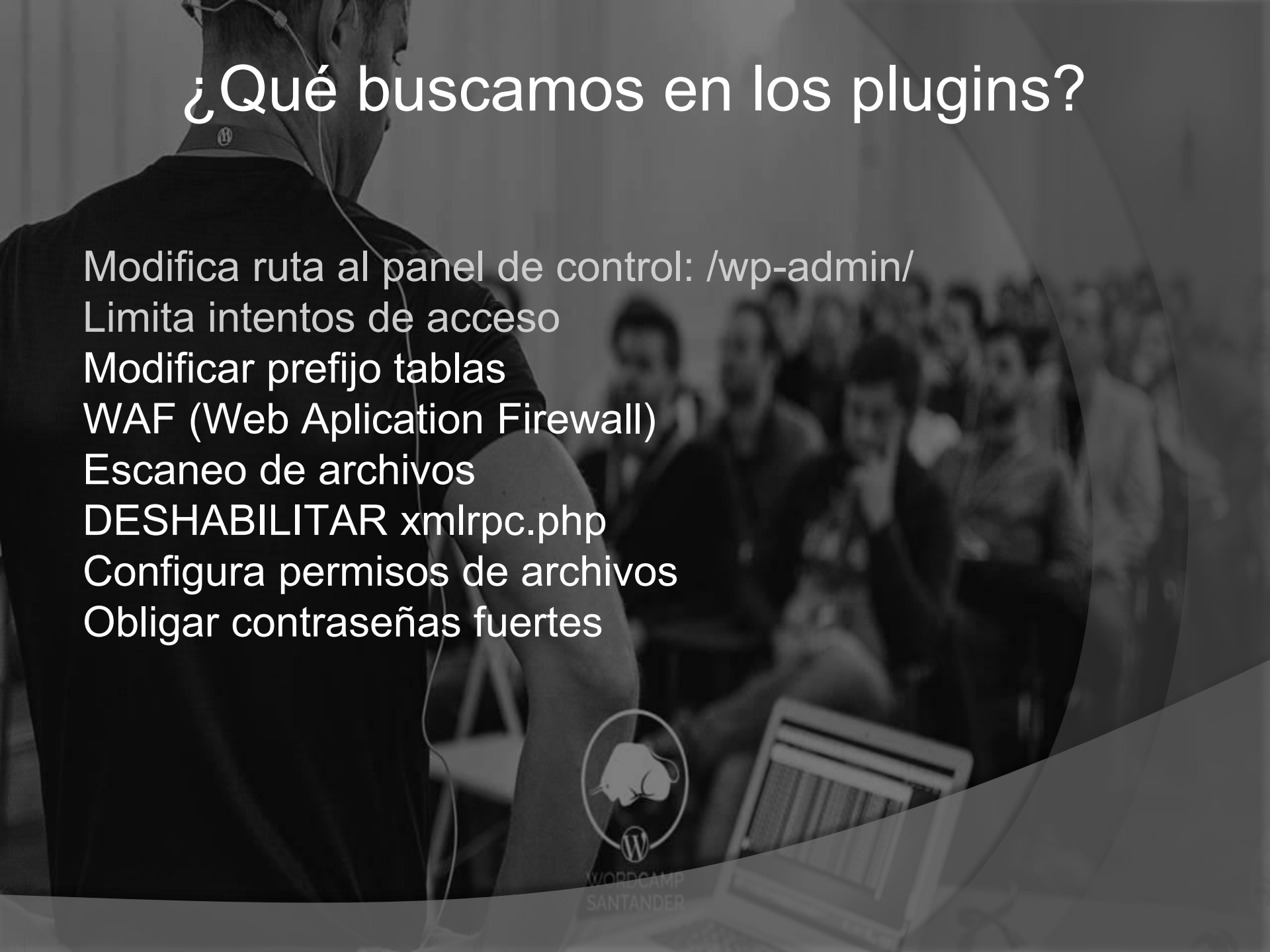
Plugins:

Limit login attemps...

Wordfence, Sucuri, All In One WP Security & Firewall...

¿Qué buscamos en los plugins?

Modifica ruta al panel de control: /wp-admin/
Limita intentos de acceso
Modificar prefijo tablas
WAF (Web Aplication Firewall)
Escaneo de archivos
DESHABILITAR xmlrpc.php
Configura permisos de archivos
Obligar contraseñas fuertes



Parámetros esenciales de seguridad

Modificar prefijos de la bbdd

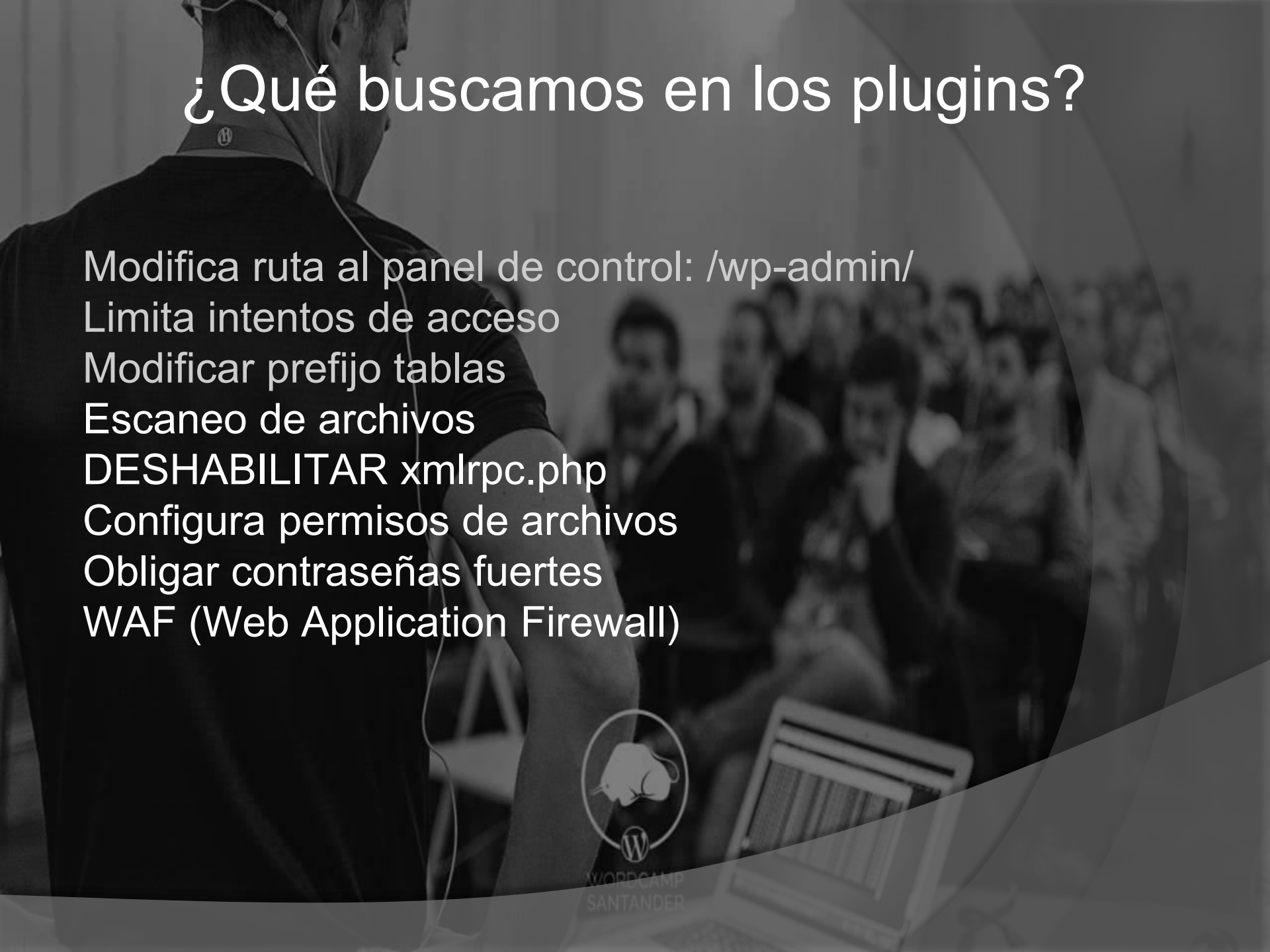
Modificar el prefijo por defecto **wp_**
por algo como **lsdjdujm_**

Plugins como:

Sucuri
Acunetix WP Security
Ithemes Security...

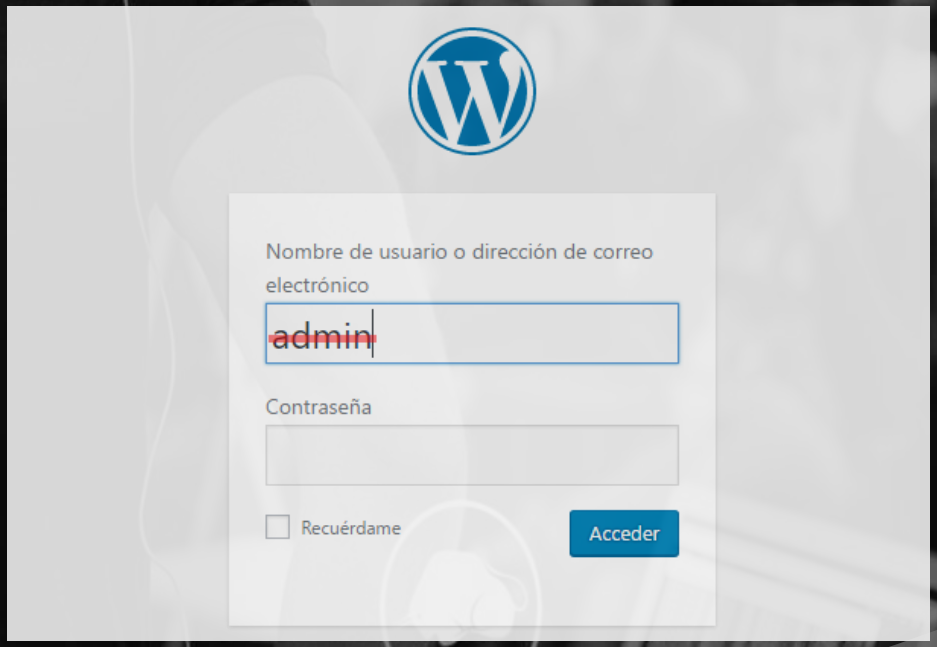
¿Qué buscamos en los plugins?

Modifica ruta al panel de control: /wp-admin/
Limita intentos de acceso
Modificar prefijo tablas
Escaneo de archivos
DESHABILITAR xmlrpc.php
Configura permisos de archivos
Obligar contraseñas fuertes
WAF (Web Application Firewall)



Parámetros esenciales de seguridad

No usar usuario “admin”



Parámetros esenciales de seguridad

Modificar la ID del usuario administrador

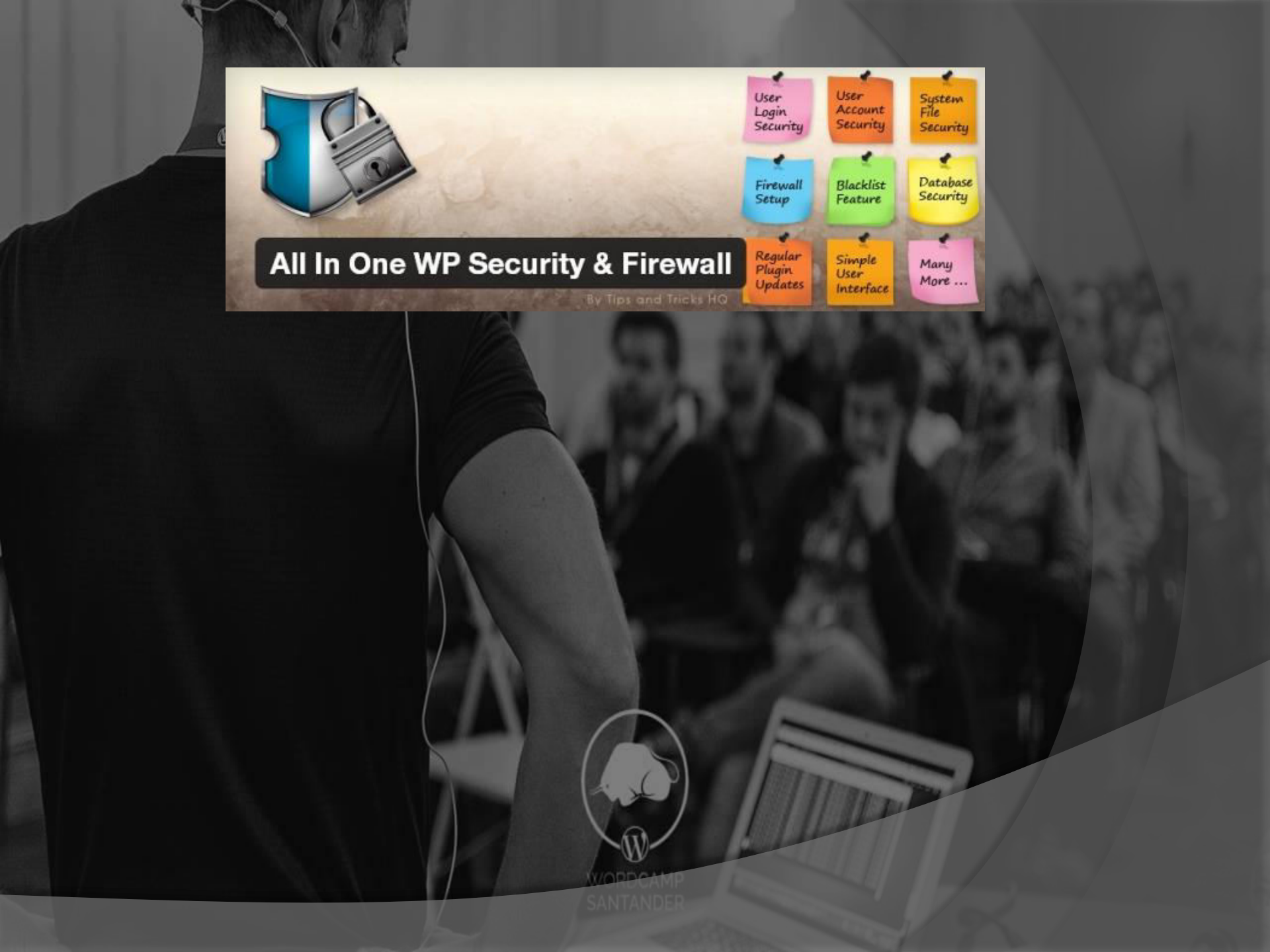
dymweb.es/?autor=1

dymweb.es/author/admin/

Wordfence™
acunetix
Better WP Security is now
iThemes Security
sucuri
Real People. Real Security.
WORDCAMP SANTANDER

Wordfence™
WORDCAMP
SANTANDER

Better WP Security is now
iThemes
Security
WORDCAMP
SANTANDER


All In One WP Security & Firewall
By Tips and Tricks HQ
User Login Security
User Account Security
System File Security
Firewall Setup
Blacklist Feature
Database Security
Regular Plugin Updates
Simple User Interface
Many More ...
WORDCAMP SANTANDER

sucuri
Real People. Real Security.
WORDCAMP
SANTANDER

Removes WordPress Version
Disables PHP Error Reporting
Integrates with WebsiteDefender
Disables Database Error Reporting
Acunetix WP Security
WORDCAMP
SANTANDER

	Wordfence	IThemes Security	All In One WP Security & Firewall	Sucuri	Accunetix wp Security
Descargas	>1.000.000	>800.000	>500.000	>300.000	>100.000
Configuración	Media	Media. ajustes básicos a 1 clic	Fácil pero larga (Sistema de PUNTOS)	Larga y tediosa	SI
Exportar / Importar configuración	SI		SI		---
Permite actualizaciones automáticas					
modifica ruta /wp-admin/	---	SI	SI	SI	---
Limita intentos de acceso	SI	SI	SI	SI	---
Modifica prefijo tablas		SI	SI	SI	SI
WAF	SI		SI	SI (de pago)	---
Escaneo de archivos	SI		SI	SI	SI
DESHABILITAR xmlrpc.php		SI	SI	SI	SI
Desconecta user tras xx minutos de inactividad					---
Permisos de archivos críticos		SI	SI		SI
Desactivar la edición de archivos desde WordPress					
Live Trafic	SI			SI	SI
Copias de seguridad		BBDD	BBDD .htaccess wp-config.php		
CAMBIO DE SALTS		SI		SI	

ShieldSecurity
WORDCAMP
SANTANDER

	Wordfence	IThemes Security	All In One WP Security & Firewall	Sucuri	Shield Security	Accunetix wp Security
Descargas	>1.000.000	>800.000	>500.000	>300.000	>50.000	>100.000
Configuración	Media	Media. ajustes básicos a 1 clic	Fácil pero larga (Sistema de PUNTOS)	Larga y tediosa	Fácil pero larga	SI
Exportar / Importar configuración	SI		SI			---
Permite actualizaciones automáticas					SI	
modifica ruta /wp-admin/		SI	SI	SI	SI	---
Limita intentos de acceso	SI	SI	SI	SI	SI	---
Modifica prefijo tablas		SI	SI	SI		SI
WAF	SI		SI	SI (de pago)	SI	---
Escaneo de archivos	SI		SI	SI	Sólo del Core	SI
DESHABILITAR xmlrpc.php		SI	SI	SI	SI	SI
Desconecta user tras xx minutos de inactividad					SI	---
Permisos de archivos críticos		SI	SI			SI
Desactivar la edición de archivos desde WordPress					SI	
Live Trafic	SI			SI	SI	SI
Copias de seguridad		BBDD	BBDD .htaccess wp-config.php			
CAMBIO DE SALTS		SI		SI		

¡Muy bien!
Entonces la pregunta es…
WORDCAMP
SANTANDER

¿Con cuál te quedarías?

Wordfence™

Better WP Security is now iThemes Security

acunetix

ShieldSecurity

Sucuri
Real People. Real Security.

WORDCAMP SANTANDER

Auditar WordPress Online

WPDOCTOR:

https://www.wpdoctor.es/

Auditar WordPress por consola

WPSCAN:

https://wpscan.org/

¡No digas que no te avisé!

MUCHAS GRACIAS

www.tomassierra.com

@Tomycant

https://www.facebook.com/tomas.profesor.3

WordCamp BILBAO 2017

SHELLCON Security Hell Conference

netkia

Tomás Sierra