swpanel

SEGURIDAD 360 · SOC · NGFW

# Informe de Seguridad 360
# swpanel.com

Lo que el cortafuegos NGFW ha detectado y bloqueado en swpanel.com (203.0.113.10) del 13 de septiembre al 12 de octubre de 2026.

• 47 de 58 amenazas bloqueadas · 24 críticas

| CLIENTE | SERVICIO | PERIODO |
|---|---|---|
| SWPanel Demo, S.L. | swpanel.com · 203.0.113.10 | 13-09-2026 a 12-10-2026 · 30 días |
| **DOCUMENTO** | **FECHA DE EMISIÓN** | **SENSIBILIDAD** |
| SW-S36-EJEMPLO-2026 | 16-10-2026 | Bloquea desde gravedad media |

# Contenido del informe

Cuadro de mando 2

01 Introducción del consultor 3

02 Amenazas 8
- Por gravedad, tipo y aplicación 9
- Las más repetidas, origen y destino 10
- Qué ha cambiado: los últimos 6 meses 11

03 Accesos y archivos 12
- Autenticación y archivos sospechosos 13

04 Qué hacer 14
- Las más graves primero 15

05 Detalle por host 17
- Host 203.0.113.10 18
- Qué es cada amenaza 20

06 Seguridad 360 23
- Diagnóstico de Seguridad 360 24
- SOC: hallazgos abiertos 26
- Accesos y cambios sensibles 27
- Bloqueo por países 28
- Bloqueo de bots 30
- Análisis de código 31
- WAF adaptativo 32
- Qué se ha hecho en el periodo 33
- Qué hemos hecho por ti 34
- Recursos y disponibilidad cruzados con la seguridad 35
- Riesgos pendientes y qué decidir 36
- Plan del próximo mes 38

07 Conclusiones del análisis 40

Glosario 43

Anexo: cómputo de IA 45

Informe NGFW de swpanel.com generado por SWPanel

# Cuadro de mando




## 81 % CON BLOQUEO

De los eventos detectados con acción de bloqueo, del 13-09-2026 al 12-10-2026

swpanel.com · 203.0.113.10 · bloquea desde gravedad media

11 de gravedad baja solo se registraron, como pide la sensibilidad.

• 24 críticas, todas bloqueadas

| 58 | 47 | 11 | 1 | 0 |
|---|---|---|---|---|
| AMENAZAS DETECTADAS | BLOQUEADAS | REGISTRADAS | INTENTO DE ACCESO ILEGÍTIMO | ARCHIVOS SOSPECHOSOS |

## Por gravedad



• Crítica **24** • Alta **11** • Media **12** • Baja **11**

## Frente a la media de los clientes

| 58 | 1 | 0 | 1 |
|---|---|---|---|
| amenazas por host<br>Media: 944,7 | intento de intrusión<br>Media: 659,9 | archivos sospechosos<br>Media: 70,3 | aplicación en la red<br>Media: 1,2 |
| **93,9 % menos** | **99,8 % menos** | **Ninguno** | **18,9 % menos** |

## Lo que te conviene hacer

**CRÍTICA**

24 amenazas críticas, todas bloqueadas. Casi todas son de tipo «Ejecución de código». Mantén el servidor y sus programas actualizados.

**REVISAR**

11 amenazas solo se registraron. Son de gravedad baja y la sensibilidad bloquea desde gravedad media. Si quieres bloquearlas también, baja la sensibilidad en el panel.

1 intento(s) de fuerza bruta (WordPress Login Brute Force Attempt). Si usas WordPress, limita los intentos de acceso.

Informe NGFW de swpanel.com generado por SWPanel

01

# Introducción del consultor

Tu situación en un minuto, lo que hemos analizado y lo que merece tu atención.

Informe NGFW de swpanel.com generado por SWPanel

# Introducción del consultor

IA Escrito por el Asistente IA de seguridad de SWPanel

## El panel ha detectado actividad sospechosa, pero con una configuración que prioriza la seguridad y evita acciones drásticas sin más información.

ATENCIÓN

**Tu situación en un minuto**

Se han detectado 58 intentos de ataque, de los cuales 47 fueron bloqueados. Es necesario revisar si el software del servidor es vulnerable a algunos de estos ataques.

**1.** Verificar si el servidor está usando versiones afectadas de PHP, Apache Shiro o phpunit.

**2.** Revisar los logs de Cloudflare y de WordPress para asegurarnos de que no hubo actividad sospechosa detrás del ataque bloqueado.

**3.** Revisar si el servidor tiene instalado Apache Shiro o OpenSSL, que son mencionados en las alertas.

Informe NGFW de swpanel.com generado por SWPanel

### Lo que he analizado

He revisado el informe del último mes de la protección de tu servicio, que incluye las amenazas detectadas y las conexiones rechazadas por el firewall de SW Hosting.

En este periodo, el sistema ha bloqueado 47 intentos de ataque y ha registrado otros 11 sin bloquear, porque no alcanzaban el umbral de sensibilidad 'media'.

Lo que más llama la atención es que el 70% de los intentos de ataque vinieron desde Estados Unidos, y que se detectó un intento de ataque a WordPress desde un IP de Cloudflare.

Esto no significa que tu sitio esté en peligro, pero sí que hay actividad que merece atención y verificación.

Tu Asistente IA de seguridad de SWPanel

### ¿Debo preocuparme?

No es momento de alarmarse, pero sí de actuar con cuidado. El firewall ha actuado según su configuración y ha bloqueado lo que consideró necesario. Ahora es momento de revisar si esos bloqueos son relevantes para tu servicio.

# Introducción del consultor

## Qué cubre este informe y qué no

Este informe muestra únicamente las amenazas detectadas y las conexiones rechazadas por el firewall. No incluye el tráfico normal ni lo que ocurre dentro del servidor.

Informe NGFW de swpanel.com generado por SWPanel

# Lo que he encontrado y por qué importa

Cada hallazgo con lo que hemos visto, en qué nos basamos, qué significa para tu servicio, qué falta por comprobar, qué te recomendamos y cómo sabremos que está resuelto.

IMPACTO BAJO

**Ataque a WordPress desde un IP de Cloudflare**

**Qué hemos observado:** Un intento de ataque de fuerza bruta a WordPress fue bloqueado. El IP desde el que vino está asociado a Cloudflare, que actúa como intermediario.

**En qué nos basamos:** Registro del firewall de SW Hosting: WordPress Login Brute Force Attempt against swpanel.com, desde IP 198.51.100.21 (CLOUDFLARE PROXY).

**Qué significa:** Alguien intentó adivinar las contraseñas de WordPress desde un servicio de red común. No sabemos si el ataque era real o si era un usuario legítimo que coincidió con el patrón de ataque.

**Qué falta comprobar:** No se puede determinar si el ataque fue real o falso positivo, ni si el usuario del Cloudflare era malicioso o no.

**Qué recomendamos:** Revisa los logs de WordPress y de Cloudflare para ver si hubo actividad sospechosa detrás de ese IP.

**Cómo lo verificaremos:** Si no hay actividad sospechosa en los logs de WordPress ni en los de Cloudflare, no hay problema.

IMPACTO MEDIO

**Vulnerabilidad en phpunit aplicable al servidor**

**Qué hemos observado:** Se detectó un intento de ataque relacionado con una vulnerabilidad en phpunit, que sí parece aplicable al servidor.

**En qué nos basamos:** Registro del firewall de SW Hosting: phpunit Remote Code Execution Vulnerability, severity critical, block, 4 veces.

**Qué significa:** Alguien intentó aprovechar una vulnerabilidad en phpunit, que está instalado en el servidor. Si el servidor usa una versión afectada, podría ser vulnerable.

**Qué falta comprobar:** No se conoce la versión exacta de phpunit instalada en el servidor.

**Qué recomendamos:** Verifica si la versión de phpunit instalada en el servidor está afectada por esta vulnerabilidad y actualízala si es necesario.

**Cómo lo verificaremos:** Si la versión de phpunit es actual y no está afectada, el problema se resuelve.

Informe NGFW de swpanel.com generado por SWPanel

# Lo que he encontrado y por qué importa

**IMPACTO BAJO**

**Varios intentos de ataque a Apache Shiro y OpenSSL**

**Qué hemos observado:** Se detectaron intentos de ataque a Apache Shiro y OpenSSL, que no se pueden verificar por falta de inventario de software.

**En qué nos basamos:** Registros del firewall de SW Hosting: Apache Shiro Improper Authentication Vulnerability y OpenSSL SSL_check_chain NULL Pointer Dereference Vulnerability.

**Qué significa:** Alguien intentó aprovechar estas vulnerabilidades, pero no sabemos si el servidor las tiene instaladas o si son relevantes para él.

**Qué falta comprobar:** No se puede confirmar si Apache Shiro o OpenSSL están instalados en el servidor.

**Qué recomendamos:** Revisa si el servidor tiene instalado Apache Shiro o OpenSSL y si están actualizados.

**Cómo lo verificaremos:** Si no están instalados o si están actualizados, no hay riesgo.

Informe NGFW de swpanel.com generado por SWPanel

02

# Amenazas

Qué ha llegado, de qué gravedad y tipo, por qué aplicación y desde dónde.

Informe NGFW de swpanel.com generado por SWPanel

# Amenazas del periodo

**IA** **El consultor opina**

La mayoría de las amenazas detectadas son intentos de ejecución de código o de acceso no autorizado. El firewall las bloqueó o las registró según su nivel de gravedad.

El NGFW ha detectado 58 amenazas en el periodo. Ha bloqueado las 47 de gravedad media, alta o crítica y ha registrado sin bloquear las 11 de gravedad baja.

• 47 bloqueadas • 11 registradas

## Por gravedad



• Crítica **24** • Alta **11** • Media **12** • Baja **11**

## Por tipo

| Tipo | Gravedades | Bloqueadas | Registradas | Total |
|---|---|---|---|---|
| Ejecución de código | • Crítica • Baja | **23** | **5** | 28 |
| Filtrado de información | • Alta • Media • Baja | **19** | **1** | 20 |
| Anomalía de protocolo | • Baja | **0** | **5** | 5 |
| Denegación de servicio | • Alta | **4** | **0** | 4 |
| Fuerza bruta | • Crítica | **1** | **0** | 1 |
| Total | | 47 | 11 | 58 |

## Por aplicación

| Aplicación | Bloqueadas | Registradas | Total | Del total |
|---|---|---|---|---|
| web-browsing | **37** | **5** | 42 | **72 %** |
| ftp | **0** | **6** | 6 | **10 %** |
| soap | **5** | **0** | 5 | **8,6 %** |
| ssl | **4** | **0** | 4 | **6,9 %** |
| portmapper | **1** | **0** | 1 | **1,7 %** |

Informe NGFW de swpanel.com generado por SWPanel

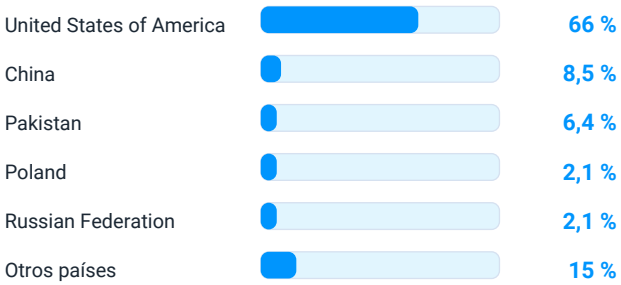
# Las más repetidas, origen y destino

## Las 10 más repetidas

| Amenaza | Tipo | Gravedad | Intentos | Acción |
|---|---|---|---|---|
| **HTTP /etc/passwd Access Attempt**<br>ID 35107 · web-browsing | **Filtrado de información** | • Alta | 7 | • Bloqueada |
| **Apache Shiro Improper Authentication Vulnerability**<br>ID 58590 · web-browsing | **Ejecución de código** | • Crítica | 6 | • Bloqueada |
| **HTTP Directory Traversal Request Attempt**<br>ID 30844 · web-browsing | **Filtrado de información** | • Media | 6 | • Bloqueada |
| **D-Link DSL Soap Authorization Remote Command Execution Vulnerability**<br>ID 58483 · soap | **Ejecución de código** | • Crítica | 5 | • Bloqueada |
| **FTP Protocol Evasion Application Detection**<br>ID 39826 · ftp | **Anomalía de protocolo** | • Baja | 5 | • Registrada |
| **phpunit Remote Code Execution Vulnerability**<br>ID 55852 · web-browsing | **Ejecución de código** | • Crítica | 4 | • Bloqueada |
| **Netgear DGN Device Remote Command Execution Vulnerability**<br>ID 40741 · web-browsing | **Ejecución de código** | • Crítica | 4 | • Bloqueada |
| **OpenSSL SSL_check_chain NULL Pointer Dereference Vulnerability**<br>ID 58033 · ssl | **Denegación de servicio** | • Alta | 4 | • Bloqueada |
| **ZGrab Application Layer Scanner Detection**<br>ID 57955 · web-browsing | **Filtrado de información** | • Media | 4 | • Bloqueada |
| **GPON Home Routers Remote Code Execution Vulnerability**<br>ID 37264 · web-browsing | **Ejecución de código** | • Crítica | 3 | • Bloqueada |

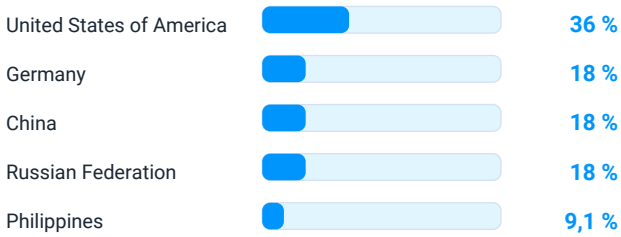
## Origen de las bloqueadas

47 amenazas, por país




## Origen de las registradas

11 amenazas, por país




Informe NGFW de swpanel.com generado por SWPanel

# Las más repetidas, origen y destino (continuación)

## Destino

Las 58 amenazas fueron a swpanel.com (203.0.113.10), el único servicio de este informe.

## Qué ha cambiado: los últimos 6 meses

| Mes | Eventos | Con bloqueo | Registrados | Críticos | Altos | Fuerza bruta |
|---|---|---|---|---|---|---|
| **mayo 2026** | **0** | 0 | 0 | 0 | 0 | 0 |
| **junio 2026** | **0** | 0 | 0 | 0 | 0 | 0 |
| **julio 2026** | **22** | 11 | 11 | 11 | 0 | 0 |
| **agosto 2026** | **51** | 35 | 16 | 24 | 1 | 0 |
| **septiembre 2026** | **92** | 77 | 15 | 38 | 16 | 1 |
| **octubre 2026** | **0** | 0 | 0 | 0 | 0 | 0 |

Meses naturales; el último, hasta el final del periodo de este informe. Comparar con tu propio historial dice más que cualquier media.

Informe NGFW de swpanel.com generado por SWPanel

03

# Accesos y archivos

Intentos de entrar a la fuerza y archivos sospechosos.

Informe NGFW de swpanel.com generado por SWPanel

# Accesos y archivos sospechosos

**IA** **El consultor opina**

Se detectó un solo intento de ataque de fuerza bruta a WordPress. No se registraron conexiones SSH ni archivos sospechosos.

## Intentos de acceso por fuerza bruta

El NGFW ha bloqueado 1 intento(s) de entrar a la fuerza, frente a 660 de media por host en el resto de clientes. Muchos de estos ataques son automáticos y se lanzan contra cualquier equipo conectado a internet: con el sistema al día, las aplicaciones bien configuradas y contraseñas seguras no suponen un riesgo real.

| Amenaza | Servicio | IP de origen | Intentos | Acción |
|---|---|---|---|---|
| **WordPress Login Brute Force Attempt**<br>ID 40044 | **swpanel.com** | **198.51.100.21**<br>Cloudflare (proxy) | 1 | • Bloqueada |

## Sesiones SSH

Nadie ha llegado a la pantalla de login de SSH en el periodo.

## Archivos sospechosos

No se ha detectado ningún archivo sospechoso: ni bloqueado ni registrado. La media de los clientes es de 70 por host.

Informe NGFW de swpanel.com generado por SWPanel

04

# Qué hacer

Qué es cada tipo de amenaza detectada y cómo protegerte, por orden de lo que te juegas.

QUÉ HACER

# Cómo protegerte

Solo los tipos que se han detectado en este periodo, de más a menos grave.

### **Ejecución de código** · 28 intentos

• Crítica • Baja

Intentos de que el servidor ejecute órdenes del atacante. Un exploit o un ransomware entran en esta categoría y pueden comprometer todo el sistema. Llegaron a swpanel.com por soap, web-browsing; 8 amenaza(s) distinta(s).

QUÉ HACER

Filtra las amenazas en capa 7, instala un antivirus y mantén el servidor y sus programas actualizados.

### **Fuerza bruta** · 1 intentos

• Crítica

Probar muchos usuarios y contraseñas seguidos hasta acertar. Llegaron a swpanel.com por web-browsing; 1 amenaza(s) distinta(s).

QUÉ HACER

Contraseñas seguras y bloqueo automático de las IPs que fallan varias veces seguidas, tanto en el cortafuegos como en el acceso a la aplicación.

### **Filtrado de información** · 20 intentos

• Alta • Media • Baja

Intentos de sacar información interna del servidor: ficheros de configuración, contraseñas o datos personales. Llegaron a swpanel.com por ftp, portmapper, web-browsing; 6 amenaza(s) distinta(s).

QUÉ HACER

Que la información sensible no se pueda leer desde fuera: cifra los ficheros que la contienen y da permisos solo a los grupos de usuarios que la necesitan.

### **Denegación de servicio** · 4 intentos

• Alta

Intentos de dejar un servicio sin respuesta, saturándolo o haciéndolo fallar. Llegaron a swpanel.com por ssl; 1 amenaza(s) distinta(s).

QUÉ HACER

Usa cortafuegos de capa 3 y de capa 7 para detectar y cortar las conexiones repetidas, y mantén actualizados los programas expuestos.

Informe NGFW de swpanel.com generado por SWPanel

QUÉ HACER

# Cómo protegerte (continuación)

**Anomalía de protocolo** · 5 intentos • Baja

Tráfico que no se comporta como el protocolo que dice ser, normalmente para pasar desapercibido. Llegaron a swpanel.com por ftp; 1 amenaza(s) distinta(s).

QUÉ HACER

Cierra los puertos que no uses y deja que el NGFW identifique la aplicación antes de dejarla pasar: lo que no se reconoce, mejor bloquearlo.

Informe NGFW de swpanel.com generado por SWPanel

05

# Detalle por host

Cada amenaza recibida por cada servicio, con su referencia.

Informe NGFW de swpanel.com generado por SWPanel

# Host 203.0.113.10

**IA** El consultor opina

No se detectaron hosts comprometidos ni actividad interna sospechosa. El firewall solo rechazó conexiones que no cumplían con su política.

swpanel.com ha recibido 58 amenazas de 17 tipos distintos, de más a menos grave.

| ID | Amenaza | Gravedad | Intentos | Acción |
|---|---|---|---|---|
| 58590 | **Apache Shiro Improper Authentication Vulnerability** Ejecución de código · web-browsing | • Crítica | 6 | • Bloqueada |
| 58483 | **D-Link DSL Soap Authorization Remote Command Execution Vulnerability** Ejecución de código · soap | • Crítica | 5 | • Bloqueada |
| 55852 | **phpunit Remote Code Execution Vulnerability** Ejecución de código · web-browsing | • Crítica | 4 | • Bloqueada |
| 40741 | **Netgear DGN Device Remote Command Execution Vulnerability** Ejecución de código · web-browsing | • Crítica | 4 | • Bloqueada |
| 37264 | **GPON Home Routers Remote Code Execution Vulnerability** Ejecución de código · web-browsing | • Crítica | 3 | • Bloqueada |
| 54617 | **Mirai and Reaper Exploitation Traffic** Ejecución de código · web-browsing | • Crítica | 1 | • Bloqueada |
| 40044 | **WordPress Login Brute Force Attempt** Fuerza bruta · web-browsing | • Crítica | 1 | • Bloqueada |
| 35107 | **HTTP /etc/passwd Access Attempt** Filtrado de información · web-browsing | • Alta | 7 | • Bloqueada |
| 58033 | **OpenSSL SSL_check_chain NULL Pointer Dereference Vulnerability** Denegación de servicio · ssl | • Alta | 4 | • Bloqueada |
| 30844 | **HTTP Directory Traversal Request Attempt** Filtrado de información · web-browsing | • Media | 6 | • Bloqueada |
| 57955 | **ZGrab Application Layer Scanner Detection** Filtrado de información · web-browsing | • Media | 4 | • Bloqueada |
| 32796 | **RPC Portmapper DUMP Request Detected** Filtrado de información · portmapper | • Media | 1 | • Bloqueada |
| 34804 | **PHP CGI Query String Parameter Handling Information Disclosure Vulnerability** Filtrado de información · web-browsing | • Media | 1 | • Bloqueada |
| 39826 | **FTP Protocol Evasion Application Detection** Anomalía de protocolo · ftp | • Baja | 5 | • Registrada |

Informe NGFW de swpanel.com generado por SWPanel

# Host 203.0.113.10 (continuación)

| ID | Amenaza | Gravedad | Intentos | Acción |
|---|---|---|---|---|
| 58098 | **Possible HTTP Malicious Payload Detection** Ejecución de código · web-browsing | • Baja | 3 | • Registrada |
| 54469 | **Suspicious File Downloading Detection** Ejecución de código · web-browsing | • Baja | 2 | • Registrada |
| 40391 | **Application Identification Evasion Attempt Through Malformed FTP Traffic** Filtrado de información · ftp | • Baja | 1 | • Registrada |

Informe NGFW de swpanel.com generado por SWPanel

# Qué es cada amenaza

ID 58590 · Ejecución de código • Crítica

### Apache Shiro Improper Authentication Vulnerability

Apache Shiro es vulnerable a una autenticación inadecuada al procesar ciertas solicitudes HTTP elaboradas. La vulnerabilidad se debe a la falta de comprobaciones adecuadas en las solicitudes HTTP, lo que lleva a una vulnerabilidad de autenticación inadecuada explotable.

Intentos **6** Bloqueada CVE-2020-11989 Ref. **lists.apache.org**

ID 58483 · Ejecución de código • Crítica

### D-Link DSL Soap Authorization Remote Command Execution Vulnerability

Dlink DSL es vulnerable a la inyección de comandos al procesar ciertas solicitudes HTTP elaboradas. La vulnerabilidad se debe a la falta de comprobaciones adecuadas en las solicitudes HTTP, lo que lleva a una inyección de comandos explotable.

Intentos **5** Bloqueada CVE-2018-19986 Ref. **github.com**

ID 55852 · Ejecución de código • Crítica

### phpunit Remote Code Execution Vulnerability

phpunit es vulnerable a la ejecución de código remoto al procesar ciertas solicitudes HTTP elaboradas. La vulnerabilidad se debe a la falta de comprobaciones adecuadas en las solicitudes HTTP, lo que lleva a una ejecución de código remoto explotable.

Intentos **4** Bloqueada CVE-2017-9841 Ref. **phpunit.vulnbusters.com**

ID 40741 · Ejecución de código • Crítica

### Netgear DGN Device Remote Command Execution Vulnerability

Los dispositivos Netgear DGN son propensos a una vulnerabilidad de ejecución de código remoto al analizar ciertas solicitudes HTTP elaboradas. La vulnerabilidad se debe a la falta de comprobaciones de privilegios en la solicitud, lo que lleva a una vulnerabilidad de ejecución de código remoto exp...

Intentos **4** Bloqueada Ref. **seclists.org**

ID 37264 · Ejecución de código • Crítica

### GPON Home Routers Remote Code Execution Vulnerability

Los routers de hogar GPON son propensos a una vulnerabilidad de ejecución de código remoto al analizar ciertas solicitudes HTTP elaboradas. La vulnerabilidad se debe a la falta de comprobaciones adecuadas en las solicitudes HTTP, lo que lleva a una vulnerabilidad de ejecución de código remoto exp...

Intentos **3** Bloqueada CVE-2018-10561 Ref. **blog.netlab.360.com**

ID 54617 · Ejecución de código • Crítica

### Mirai and Reaper Exploitation Traffic

Esta firma detecta intentos de explotación de los malware Mirai y Reaper. La detección de este tráfico indica un intento de explotar diversas vulnerabilidades de dispositivos IoT, incluyendo: la vulnerabilidad de inyección de comandos del sistema operativo en D-Link DSL-2750B, la vulnerabilidad d...

Intentos **1** Bloqueada

Informe NGFW de swpanel.com generado por SWPanel

# Qué es cada amenaza (continuación)

ID 40044 · Fuerza bruta • Crítica

### WordPress Login Brute Force Attempt

Este evento indica que alguien está utilizando un ataque de fuerza bruta para acceder a WordPress wp-login.php.

Intentos **1** Bloqueada

ID 35107 · Filtrado de información • Alta

### HTTP /etc/passwd Access Attempt

Se ha detectado un intento de acceso al archivo /etc/passwd al analizar ciertas solicitudes HTTP elaboradas. Un ataque exitoso podría permitir a un atacante acceder a información sensible que podría facilitar otros ataques.

Intentos **7** Bloqueada

ID 58033 · Denegación de servicio • Alta

### OpenSSL SSL_check_chain NULL Pointer Dereference Vulnerability

OpenSSL es vulnerable a un error de referencia de puntero NULL al procesar ciertas solicitudes SSL elaboradas. La vulnerabilidad se debe a la falta de comprobaciones adecuadas en las solicitudes SSL, lo que lleva a una vulnerabilidad de referencia de puntero NULL explotable.

Intentos **4** Bloqueada CVE-2020-1967 Ref. **openssl.org**

ID 30844 · Filtrado de información • Media

### HTTP Directory Traversal Request Attempt

Se ha descubierto una vulnerabilidad de recorrido de directorios al analizar solicitudes HTTP malformadas. Esta vulnerabilidad se debe a la falta de comprobaciones adecuadas en las solicitudes URI HTTP.

Intentos **6** Bloqueada Ref. **imperva.com**

ID 57955 · Filtrado de información • Media

### ZGrab Application Layer Scanner Detection

Esta firma indica que un atacante está intentando recopilar información sobre la red utilizando el escáner ZGrab.

Intentos **4** Bloqueada

ID 32796 · Filtrado de información • Media

### RPC Portmapper DUMP Request Detected

La mayoría de los servidores Unix pueden obtener información mediante una solicitud normal al puerto de mapeo de puertos.

Intentos **1** Bloqueada

ID 34804 · Filtrado de información • Media

### PHP CGI Query String Parameter Handling Information Disclosure Vulnerability

Las configuraciones basadas en PHP-CGI, como Apache's mod_cgid, contienen una vulnerabilidad al analizar parámetros de cadena de consulta de archivos PHP. En este tipo de configuración, php-cgi recibe una cadena de consulta procesada como argumentos de línea de comandos, lo que permite pasar opci...

Intentos **1** Bloqueada CVE-2012-1823 Ref. **kb.cert.org**

ID 39826 · Anomalía de protocolo • Baja

### FTP Protocol Evasion Application Detection

Esta firma detecta aplicaciones o herramientas que tunnelean el tráfico SSH a través del tráfico FTP.

Intentos **5** Registrada Ref. **room362.com**

Informe NGFW de swpanel.com generado por SWPanel

# Qué es cada amenaza (continuación)

ID 58098 · Ejecución de código • Baja

**Possible HTTP Malicious Payload Detection**

Esta firma detecta una carga útil maliciosa en el tráfico HTTP.

Intentos **3** Registrada Ref. **unit42.paloaltonetworks.com**

ID 54469 · Ejecución de código • Baja

**Suspicious File Downloading Detection**

Esta firma detecta la ejecución de comandos WGET y CURL en parámetros de URL de solicitudes HTTP, lo cual es ampliamente explotado por atacantes para obtener posteriormente una carga útil maliciosa.

Intentos **2** Registrada

ID 40391 · Filtrado de información • Baja

**Application Identification Evasion Attempt Through Malformed FTP Traffic**

La firma detecta un intento de evasión de identificación de aplicaciones que envía tráfico malformado a través del puerto TCP 21.

Intentos **1** Registrada Ref. **jira-hq.paloaltonetworks.local**

Informe NGFW de swpanel.com generado por SWPanel

06

# Seguridad 360

Todas las protecciones de tu servicio: su estado, lo que han visto y lo que queda por resolver.

Informe NGFW de swpanel.com generado por SWPanel

# Diagnóstico de Seguridad 360

IA **Escrito por el Asistente IA de seguridad de SWPanel**

**ATENCIÓN MEDIA**

La actividad de ataque es moderada y se han bloqueado la mayoría de los eventos detectados, pero hay riesgos pendientes que requieren atención, como la falta de SPF y DMARC en el correo.

En los últimos 30 días, el cortafuegos ha detectado 58 eventos de seguridad, de los cuales 47 han sido bloqueados. Esto significa que el 81% de los eventos con riesgo suficiente han sido detenidos antes de que pudieran afectar tu servicio.

La mayor parte de las amenazas detectadas son de tipo ejecución de código o filtración de información, lo que sugiere que tu web es objetivo de intentos de acceso no autorizado o de robo de datos.

Aunque no se han observado accesos SSH ni archivos sospechosos, sí se ha detectado un intento de ataque de fuerza bruta a WordPress desde un IP que parece estar detrás de un proxy de Cloudflare. Esto indica que alguien intentó adivinar credenciales, pero el firewall lo bloqueó.

El nivel de actividad maliciosa es moderado, pero no se pueden descartar amenazas futuras. Es importante mantener actualizados los sistemas y revisar las configuraciones de seguridad.

La información proviene del cortafuegos de SWPanel y de los análisis del SOC. No se han observado accesos SSH ni archivos sospechosos, pero no se dispone de datos completos sobre todas las protecciones.

Informe NGFW de swpanel.com generado por SWPanel

## Estado de cada protección

Lo decide el sistema con lo que puede comprobar: configurado no es lo mismo que funcionando.

**OPERATIVO Y VERIFICADO**

**Cortafuegos NGFW**

**OPERATIVO Y VERIFICADO**

**SOC: vigilancia y hallazgos**

# Diagnóstico de Seguridad 360

SIN COBERTURA
**Bloqueo de bots**

SIN COBERTURA
**Bloqueo por países**

SIN COBERTURA
**AntiDDoS**

CONFIGURADO, SIN VERIFICAR
**Fail2Ban: bloqueo de quien falla al entrar**

CONFIGURADO, SIN VERIFICAR
**WAF adaptativo**
modo observa: detecta y propone, no bloquea

OPERATIVO Y VERIFICADO
**Accesos SSH**

OPERATIVO Y VERIFICADO
**Análisis de código**

Informe NGFW de swpanel.com generado por SWPanel

# SOC: hallazgos abiertos

**IA** **El consultor opina**

El SOC ha detectado 71 hallazgos abiertos, incluyendo amenazas de alto riesgo como la falta de SPF y DMARC, y direcciones IP con actividad de bots. Se recomienda revisar estas alertas con prioridad.

| 0 | 4 | 13 | 38 |
|---|---|---|---|
| CRÍTICOS | ALTOS | MEDIOS | HALLAZGOS ABIERTOS |

| 2 | 5 | 0 | 23 |
|---|---|---|---|
| NUEVOS EN 7 DÍAS | RESUELTOS EN 7 DÍAS | PICOS EN 30 DÍAS | IPS BLOQUEADAS |

## Los hallazgos más graves

3
**active_check** · SWP01
Falta DMARC | Sin registro _dmarc: el dominio es facilmente suplantable en correos de phishing

3
**ip_reputation** · SWP01
198.51.100.77 | red de bots (spamhaus, riesgo critical) | 41 peticiones

3
**ip_reputation** · SWP01
198.51.100.82 | escaner conocido (abuseipdb, riesgo alto) | 18 peticiones

Informe NGFW de swpanel.com generado por SWPanel

# SOC: hallazgos abiertos

## Accesos y cambios sensibles

**IA** El consultor opina

No se han observado accesos SSH ni intentos de fuerza bruta exitosos. El único intento detectado fue bloqueado por el firewall.

| 1 | 0 | 0 | 248 |
|---|---|---|---|
| ACCESOS SSH | DESDE IPS NO DE ADMINISTRACIÓN | ROOT CON CONTRASEÑA | INTENTOS FALLIDOS |

| 11 | 0 | 0 |
|---|---|---|
| IPS CON FALLOS | USUARIOS NUEVOS | SUDO DE USUARIOS NO ROOT |

Informe NGFW de swpanel.com generado por SWPanel

# Bloqueo por países

**IA** El consultor opina

La mayor parte del tráfico malicioso proviene de Estados Unidos, Alemania y Países Bajos. No se han aplicado bloqueos por países, por lo que se recomienda considerar esta medida para reducir el tráfico de escaneo.

| 8.564 | 8.061 | 10.481 | 0 |
|---|---|---|---|
| PETICIONES DE PERSONAS | DE ROBOTS | DE ESCÁNERES | PAÍSES BLOQUEADOS |

## Actividad por país

| País | Personas | Robots | Escáneres | Bloqueo |
|---|---|---|---|---|
| **United States of America** | 2.517 | 2.887 | 4.855 | — |
| **Spain** | 710 | 1.934 | 1 | — |
| **France** | 961 | 23 | 1.301 | — |
| **Singapore** | 1.273 | 5 | 718 | — |
| **Japan** | 363 | 8 | 961 | — |
| **Korea, Republic of** | 14 | 960 | 22 | — |
| **Belgium** | 366 | 3 | 507 | — |
| **Hong Kong** | 131 | 361 | 225 | — |
| **Lithuania** | 214 | 4 | 477 | — |
| **Canada** | 180 | 96 | 365 | — |
| **India** | 69 | 331 | 214 | — |
| **Brazil** | 177 | 216 | 162 | — |
| **Netherlands** | 187 | 45 | 145 | — |
| **Germany** | 234 | 65 | 65 | — |

Peticiones a tus webs en el periodo, por la ubicación de la IP. Un país bloqueado que sigue recibiendo peticiones después del bloqueo indica que el corte no se aplica.

Informe NGFW de swpanel.com generado por SWPanel

# Bloqueo por países

**ESCENARIO A**

**Lo que aconseja el consultor de países**

Bloquear países con perfil de ataque y casi sin personas reduciría el 4,6 % de los escáneres.

**Por qué:** Con el escenario A, perderías 3,2 % de tus personas y quitarías 4,6 % de los escáneres. B no porque pierdes más personas (5,5 %) y C no porque no sabes tu negocio.

Informe NGFW de swpanel.com generado por SWPanel

# Bloqueo de bots

**IA** El consultor opina

Se han bloqueado 6 bots, principalmente de inteligencia artificial. El perfil de bloqueo actual (B) es recomendado, ya que permite bloquear bots no esenciales sin afectar a los motores de búsqueda.

| 3.361 | 2.830 | 2.643 | 2.532 |
|---|---|---|---|
| PETICIONES DE PERSONAS | DE BOTS CONOCIDOS | DE ROBOTS SIN CATALOGAR | DE ESCÁNERES |

| 38 | 6 | 8 | B |
|---|---|---|---|
| BOTS DETECTADOS | BOTS BLOQUEADOS | AGENTES NUEVOS DESCUBIERTOS | PERFIL ACTUAL |

## Los bots detectados

| Bot | Familia | Peticiones | Estado |
|---|---|---|---|
| **GPTBot (OpenAI)** | IAG | 57 | • Bloqueada |
| **Meta-WebIndexer (Meta AI)** | IAG | 55 | • Bloqueada |
| **Googlebot** | BUS | 51 | Permitido |
| **PerplexityBot** | IAG | 45 | • Bloqueada |
| **Bytespider (ByteDance)** | IAG | 34 | • Bloqueada |
| **AhrefsBot** | SEO | 32 | Permitido |
| **ChatGPT-User** | IAG | 32 | • Bloqueada |
| **OnCrawl** | SEO | 31 | Permitido |
| **ClaudeBot (Anthropic)** | IAG | 30 | • Bloqueada |
| **Kimi-SearchBot (Moonshot AI)** | IAG | 30 | Permitido |
| **Qwenbot (Alibaba)** | IAG | 29 | Permitido |
| **DuckAssistBot (DuckDuckGo)** | IAG | 29 | Permitido |
| **Applebot** | BUS | 28 | Permitido |
| **KimiBot (Moonshot AI)** | IAG | 27 | Permitido |
| **YouBot (You.com)** | IAG | 26 | Permitido |

Informe NGFW de swpanel.com generado por SWPanel

# Bloqueo de bots

## Los perfiles de bloqueo y lo que cortaría cada uno

| Perfil | Bots que corta | Nuevos | Peticiones | Los principales |
|---|---|---|---|---|
| **A** | 2 | 2 | 184 | |
| **B** · aconsejable | 6 | 4 | 642 | |
| **C** | 11 | 5 | 1.415 | |

**ESCENARIO B**

**Lo que aconseja el consultor de bots**

Bloquear 4 bots ahorra 0,9 % de tu tráfico sin afectar bots clave.

**Por qué:** El escenario B bloquea 0,9 % de tu tráfico, lo que representa un ahorro moderado en consumo sin afectar bots clave como Googlebot o GPTBot (OpenAI). A no porque no bloquea nada, y C no porque bloquea bots que podrían afectar tu visibilidad o análisis de SEO.

## Análisis de código

**IA** **El consultor opina**

El análisis del código no ha encontrado errores ni archivos sospechosos. El último análisis ha dado un score de 86, lo que indica que el código está en buen estado.

| 86 | 1 | 0 | 0 |
|---|---|---|---|
| PUNTUACIÓN DEL CÓDIGO | HALLAZGOS DE SEGURIDAD | CRÍTICOS | FICHEROS SOSPECHOSOS |
| **3** | **0** | **0** | **PHP 8.3** |
| ERRORES DE CÓDIGO | ERRORES SQL | RESPUESTAS 5XX | VERSIÓN DE PHP |

Último análisis completo: 16/10/2026 · 4 análisis en el periodo.

Informe NGFW de swpanel.com generado por SWPanel

# Bloqueo de bots

## WAF adaptativo

**IA** El consultor opina

El WAF está en modo protección y ha detectado 72 alertas de alto riesgo. Se recomienda revisar las reglas y las acciones tomadas para asegurar que están bloqueando correctamente las amenazas.

| Solo observa | aplica | 7 | 20 |
|---|---|---|---|
| MODO | AUTONOMÍA DE LA IA | REGLAS | DISPAROS EN SOMBRA |

**OBSERVA**

El WAF adaptativo está en modo observación: detecta y propone reglas, pero no bloquea por sí solo. Pásalo a automático si quieres que actúe.

## Lo que ha hecho el WAF en el periodo

| Acción | Quién | Resultado | Veces |
|---|---|---|---|
| **hallazgo:alta** | panel | abierto | 72 |
| **hallazgo:no_visto** | panel | corregido | 8 |
| **hallazgo:visto** | panel | abierto | 7 |

Informe NGFW de swpanel.com generado por SWPanel

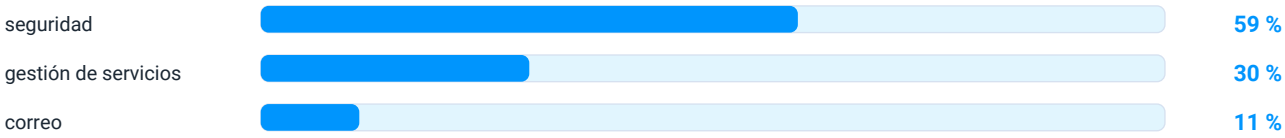
# Qué se ha hecho en el periodo

**IA** El consultor opina

SWPanel y su AI han realizado 64 acciones en el periodo, incluyendo bloqueos de IPs y ajustes de seguridad. El cliente no ha realizado cambios manuales en el firewall ni en el WAF.

| 64 | 11 | 4 | 0 |
|---|---|---|---|
| ACCIONES REGISTRADAS | HECHAS POR LA IA DE SWPANEL | POR API | IPS BLOQUEADAS EN EL FIREWALL |

## Por área




## Las últimas acciones

| Fecha | Quién | Servicio | Qué |
|---|---|---|---|
| 2026-10-14 09:12 | **Titular** | SWP01 | Se ha añadido la IP 203.0.113.50 (oficina) a la lista de permitidas del FireWall. |
| 2026-10-12 03:40 | **SWPanel (IA)** | SWP01 | El consultor de IA ha preparado un informe de los bots que visitan la web. Perfil recomendado: B. |
| 2026-10-11 18:05 | **Titular** | SWP01 | Se ha aplicado el perfil de bloqueo de bots B (6 bots bloqueados). |
| 2026-10-09 02:15 | **SWPanel** | SWP01 | El WAF adaptativo ha activado una regla contra rutas de ataque a /wp-login.php y /.env. |
| 2026-10-07 11:30 | **Titular** | SWP01 | Se ha cambiado la versión de PHP de 8.1 a 8.3. |
| 2026-10-03 04:02 | **SWPanel (IA)** | SWP01 | El consultor de IA ha preparado un informe del tráfico por países. Escenario recomendado: A. |
| 2026-10-02 16:48 | **API** | SWP01 | Bloqueo de la IP 198.51.100.77 durante 24 horas por intentos repetidos de acceso. |
| 2026-09-28 10:20 | **Titular** | SWP01 | Se ha renovado el certificado SSL de swpanel.com. |
| 2026-09-22 08:15 | **SWPanel** | SWP01 | Copia de seguridad completa verificada correctamente. |

Informe NGFW de swpanel.com generado por SWPanel

# Qué hemos hecho por ti

Lo que SWPanel, su SOC y su IA han hecho por tu servicio en el periodo, sacado de los registros: no son intenciones, son acciones hechas.

| 9 | 87 | 5 | 4 |
|---|---|---|---|
| IPS BLOQUEADAS POR SWPANEL | ACCIONES DEL WAF | HALLAZGOS RESUELTOS (7 DÍAS) | ACCIONES AUTOMÁTICAS RECIENTES |

## Las últimas acciones de SWPanel

| Fecha | Quién | Qué |
|---|---|---|
| 2026-10-12 03:40 | **SWPanel (IA)** | El consultor de IA ha preparado un informe de los bots que visitan la web. Perfil recomendado: B. |
| 2026-10-09 02:15 | **SWPanel** | El WAF adaptativo ha activado una regla contra rutas de ataque a /wp-login.php y /.env. |
| 2026-10-03 04:02 | **SWPanel (IA)** | El consultor de IA ha preparado un informe del tráfico por países. Escenario recomendado: A. |
| 2026-09-22 08:15 | **SWPanel** | Copia de seguridad completa verificada correctamente. |

Informe NGFW de swpanel.com generado por SWPanel

# Recursos y disponibilidad cruzados con la seguridad

**IA El consultor opina**

Los recursos del servidor han sido utilizados de forma moderada. La CPU ha tenido un máximo del 29%, la RAM un máximo del 49% y no se han producido caídas ni degradaciones de servicio.

| | | | |
|---|---|---|---|
| **1,1 %** CPU MEDIA | **29 %** CPU MÁXIMA (MEDIA DIARIA) | **1,7 / 4** CARGA MÁXIMA / VCORES | **49 %** RAM MÁXIMA |
| **0** CAÍDAS | **0 min** TIEMPO CAÍDO | **0** EPISODIOS DE DEGRADACIÓN | **0** PARADAS POR SEGURIDAD |
| **0** HORAS AL LÍMITE | **0** DE GRAVEDAD ALTA | **0** RESPUESTAS 5XX | **0** TIMEOUTS |

## El cruce: seguridad y rendimiento

**IA Escrito por el Asistente IA de seguridad de SWPanel**

No se han observado picos de uso del CPU ni degradaciones del servicio que coincidan con ataques o tráfico de bots. Esto sugiere que el firewall y el bloqueo de bots están funcionando correctamente.

El tráfico de escaneo ha sido elevado, pero no ha causado picos de carga ni errores en el servidor. Esto indica que el firewall está filtrando correctamente la mayor parte del tráfico malicioso.

No hay coincidencias entre los errores del código y los picos de tráfico. Esto sugiere que el código no es un factor en los picos de actividad, pero no se pueden descartar problemas futuros si el tráfico aumenta.

Informe NGFW de swpanel.com generado por SWPanel

# Riesgos pendientes y qué decidir

IA Escrito por el Asistente IA de seguridad de SWPanel

IMPACTO MEDIO

**Falta de SPF y DMARC**

**Qué hemos observado:** No se han configurado los registros SPF ni DMARC en el dominio.

**En qué nos basamos:** Esto permite que cualquiera envíe correos en nombre del dominio, facilitando el suplantamiento y el phishing.

**Qué significa:** Tu dominio no tiene protección contra el correo falso, lo que puede afectar tu reputación y la seguridad de tus usuarios.

**Qué falta comprobar:** Configurar los registros SPF y DMARC en el DNS del dominio.

**Qué recomendamos:** Configura los registros SPF y DMARC en el DNS de tu dominio para proteger contra el suplantamiento de correo.

**Cómo lo verificaremos:** Verifica que los registros SPF y DMARC estén configurados correctamente y que el correo no sea rechazado por los proveedores.

IMPACTO MEDIO

**IPs con actividad de bots**

**Qué hemos observado:** Se han detectado IPs con actividad de bots de alto riesgo en el tráfico del servidor.

**En qué nos basamos:** Estas IPs han realizado múltiples intentos de escaneo y ataque.

**Qué significa:** Esto indica que tu servidor es objetivo de bots maliciosos que intentan encontrar vulnerabilidades.

**Qué falta comprobar:** Bloquear estas IPs o aplicar medidas adicionales para evitar que accedan al servidor.

**Qué recomendamos:** Bloquea las IPs con actividad de bots o aplica reglas adicionales en el firewall para limitar su acceso.

**Cómo lo verificaremos:** Verifica que las IPs bloqueadas ya no estén realizando actividad maliciosa y que el tráfico se reduzca.

Informe NGFW de swpanel.com generado por SWPanel

# Riesgos pendientes y qué decidir

IMPACTO BAJO

**Falta de bloqueo por países**

**Qué hemos observado:** No se han aplicado bloqueos por países para reducir el tráfico de escaneo.

**En qué nos basamos:** El tráfico malicioso proviene de países con alto índice de riesgo.

**Qué significa:** Esto permite que bots y escaneadores accedan al servidor desde estas ubicaciones.

**Qué falta comprobar:** Aplicar un bloqueo por países para reducir el tráfico de escaneo y ataque.

**Qué recomendamos:** Aplica un bloqueo por países siguiendo el escenario recomendado por el asesor de países para reducir el tráfico malicioso.

**Cómo lo verificaremos:** Verifica que el bloqueo se haya aplicado correctamente y que el tráfico de los países bloqueados disminuya.

## Qué deberías decidir

Decide si aplicas el bloqueo por países recomendado por el asesor de países. Esto reducirá el tráfico de escaneo y ataque sin afectar a los usuarios legítimos. Si no lo aplicas, considera otras medidas como ajustar el firewall o revisar las reglas del WAF.

Informe NGFW de swpanel.com generado por SWPanel

# Plan del próximo mes

**ESTE MES**

**Configurar SPF y DMARC**

**Por qué:** Proteger contra el suplantamiento de correo y el phishing.

**Quién:** Tú

**Cómo lo comprobaremos:** Verificar que los registros SPF y DMARC estén configurados correctamente en el DNS del dominio.

**ESTE MES**

**Bloquear IPs con actividad de bots**

**Por qué:** Evitar que IPs con alto riesgo accedan al servidor.

**Quién:** Tú

**Cómo lo comprobaremos:** Verificar que las IPs bloqueadas ya no estén realizando actividad maliciosa.

**MEDIO PLAZO**

**Aplicar bloqueo por países**

**Por qué:** Reducir el tráfico de escaneo y ataque desde países de alto riesgo.

**Quién:** Tú

**Cómo lo comprobaremos:** Verificar que el bloqueo se haya aplicado correctamente y que el tráfico de los países bloqueados disminuya.

**ESTE MES**

**Revisar las reglas del WAF**

**Por qué:** Asegurar que el WAF esté bloqueando correctamente las amenazas detectadas.

**Quién:** SWPanel

**Cómo lo comprobaremos:** Verificar que las reglas del WAF hayan sido actualizadas y que estén bloqueando correctamente las amenazas.

**MEDIO PLAZO**

**Revisar el tráfico de bots**

**Por qué:** Asegurar que los bots no estén afectando el rendimiento del servidor.

**Quién:** Tú

**Cómo lo comprobaremos:** Verificar que el tráfico de bots se haya reducido y que no haya impacto en el rendimiento del servidor.

Informe NGFW de swpanel.com generado por SWPanel

# Plan del próximo mes

## Conclusiones de Seguridad 360

El nivel de actividad maliciosa es moderado, pero no se pueden descartar amenazas futuras. Es importante mantener actualizados los sistemas y revisar las configuraciones de seguridad.

La falta de SPF y DMARC es un riesgo para la seguridad del correo y la reputación del dominio. Se recomienda configurar estos registros lo antes posible.

El bloqueo por países puede ayudar a reducir el tráfico de escaneo y ataque, pero no es una medida definitiva. Se recomienda aplicar otras medidas de seguridad complementarias.

El WAF está funcionando correctamente, pero es importante revisar las reglas y las acciones tomadas para asegurar que están bloqueando correctamente las amenazas.

Informe NGFW de swpanel.com generado por SWPanel

07

# Conclusiones del análisis

Lo que concluye tu consultor después de ver todas las cifras, y tu plan de acción.

Informe NGFW de swpanel.com generado por SWPanel

# Conclusiones del análisis

**IA** **Escrito por el Asistente IA de seguridad de SWPanel**

El nivel de amenazas detectadas ha disminuido en comparación con el mes anterior, lo que sugiere que la protección actual es efectiva para rechazar las principales agresiones. Sin embargo, persisten intentos de ataque que merecen atención.

La mayor parte de los bloqueos corresponden a intentos de explotar vulnerabilidades, como en phpunit, que sí afectan al servicio. Esto indica que el panel está siendo apuntado con ataques específicos, aunque no se ha observado acceso no autorizado.

La baja cantidad de tráfico sospechoso y la configuración de sensibilidad media del firewall han permitido evitar acciones drásticas, pero es importante revisar los logs y mantener actualizados los componentes del servidor.

No se han detectado accesos SSH ni archivos sospechosos, lo que sugiere que el perímetro exterior no ha sido comprometido. Sin embargo, la vigilancia activa es clave para mantener la seguridad a largo plazo.

Informe NGFW de swpanel.com generado por SWPanel

## Tu plan de acción

**ESTE MES**
**Revisar los logs de WordPress y de Cloudflare**
**Por qué:** Para identificar si hubo actividad sospechosa detrás del IP de Cloudflare que intentó un ataque de fuerza bruta.
**Quién:** Tú
**Cómo lo comprobaremos:** Compartir con SWPanel un resumen de los logs revisados y cualquier hallazgo relevante.

**ESTE MES**
**Verificar y actualizar la versión de phpunit instalada**
**Por qué:** La vulnerabilidad detectada en phpunit es aplicable al servidor y podría ser explotada si la versión instalada está afectada.
**Quién:** Tú
**Cómo lo comprobaremos:** Confirmar con SWPanel la versión actual y la actualización realizada.

# Conclusiones del análisis

**MEDIO PLAZO**

**Revisar si Apache Shiro o OpenSSL están instalados y si están actualizados**

**Por qué:** Los intentos de ataque a estas tecnologías sugieren que podrían estar presentes en el servidor, y su actualización es clave para evitar explotaciones.

**Quién:** Tú

**Cómo lo comprobaremos:** Enviar a SWPanel el estado actual de estas dependencias y confirmar actualizaciones.

Estamos aquí para ayudarte a mantener tu servicio seguro y tranquilo. Si tienes dudas, no dudes en consultarnos en cualquier momento.

## Tu Asistente IA de seguridad de SWPanel

Texto redactado por el Asistente IA de SWPanel a partir de los datos de este informe, con un modelo que funciona en servidores propios de SW Hosting: tus datos no salen de nuestra infraestructura. Las cifras las calcula el sistema; la IA solo las interpreta.

Informe NGFW de swpanel.com generado por SWPanel

# Glosario

Los términos técnicos que salen en este informe, por orden alfabético.

### Amenaza bloqueada
La que el NGFW ha detenido antes de llegar al servidor, según la sensibilidad elegida.

### Amenaza registrada
La que se ha detectado y anotado pero no bloqueado, porque su gravedad está por debajo de la sensibilidad.

### Anomalía de protocolo
Tráfico que no se comporta como el protocolo que dice ser.

### Aplicación
Tipo de tráfico que el NGFW reconoce por su contenido (web-browsing, ssl, ftp), no solo por el puerto.

### CVE
Código público que identifica una vulnerabilidad conocida, por ejemplo CVE-2020-1967.

### Denegación de servicio
Ataque que satura o hace fallar un servicio hasta que deja de responder.

### Ejecución de código
Ataque que intenta que el servidor ejecute órdenes del atacante.

### Exploit
Programa o petición que aprovecha una vulnerabilidad concreta.

### Filtrado de información
Intento de sacar datos internos del servidor, como ficheros de configuración o contraseñas.

### Fuerza bruta
Probar muchas contraseñas seguidas hasta acertar.

### Gravedad
Nivel de riesgo de una amenaza: crítica, alta, media o baja.

### ID de amenaza
Identificador de la amenaza en el catálogo del fabricante del NGFW.

Informe NGFW de swpanel.com generado por SWPanel

# Glosario (continuación)

### Inyección SQL
Colar órdenes de base de datos en los datos que se envían a una aplicación.

### NGFW
Next Generation Firewall: cortafuegos que analiza el contenido del tráfico para detectar y bloquear amenazas.

### Sensibilidad
Gravedad a partir de la cual el NGFW bloquea. Por debajo, solo registra.

### Sesión
Una conexión completa entre dos equipos, del primer paquete al último.

### Tráfico de entrada y de salida
Los datos que llegan a tus servicios y los que salen de ellos.

### Vulnerabilidad
Fallo de seguridad de un programa que un atacante puede aprovechar.

Informe NGFW de swpanel.com generado por SWPanel

# Anexo: cómputo de IA

**IA** **Lo que ha costado escribir este informe con IA**

El asistente y las traducciones de este informe los ha generado un modelo de lenguaje que funciona en servidores propios de SW Hosting: tus datos no salen de nuestra infraestructura.

## Cómputo de IA

| | | |
|---|---|---|
| **qwen3-32b**<br>MODELO | **vLLM**<br>MOTOR | **2**<br>LLAMADAS AL MODELO |
| **4.365**<br>TOKENS LEÍDOS | **1.995**<br>TOKENS ESCRITOS | **39,2 s**<br>TIEMPO DE CÓMPUTO |

## Infraestructura

| | | |
|---|---|---|
| **NVIDIA A100**<br>GPU | **80 GB**<br>HBM2E | **312 TFLOPS**<br>FP16/BF16 |

## Energía y coste

| | | |
|---|---|---|
| **0,0063 kWh**<br>CONSUMO DE CÓMPUTO | **0,0157 kWh**<br>CONSUMO TOTAL (CON REFRIGERACIÓN) | **3,9 g**<br>CO2 EMITIDO |
| **0,0225 €**<br>COSTE DE CÓMPUTO | | |

Estimación: GPU a 575 W, refrigeración de 1,5 kW por kW de cómputo, 0,185 EUR/kWh, 1,8 EUR por hora de GPU y 250 g de CO2 por kWh.

Informe NGFW de swpanel.com generado por SWPanel

swpanel

https://www.swpanel.com

Documento: SW-S36-EJEMPLO-2026

Informe generado automáticamente por SWPanel · https://www.swpanel.com