



WORDCAMP
MANAGUA



WORDPRESS
SEGURO

ACERCA DE

- **Aura Lila Gutiérrez**
- **Desarrolladora web**
- **Colaboradora de la Comunidad WP Nicaragua**
- **Co-organizadora WordCamp Managua**

RECOMENDACIONES

- No usar el usuario admin como administrador
- No publicar contenido como administrador
- Esconder login
- Verificar permisos de directorios
- Protección de spam (Akismet)

RECOMENDACIONES

- Sólo instalar plugins y temas del repositorio oficial de wordpress
- Mantener actualizado WP sobre todo cuando es una actualización de seguridad.
- Salt - <https://api.wordpress.org/secret-key/1.1/salt/>
- Rest API, quitar permisos para listar usuarios

REST API

- <http://v2.wp-api.org/reference/users/>
- <http://demo.wp-api.org/wp-json/wp/v2/users>

```
[{"id":1,"name":"Human Made","url":"","description":"","link":"https://demo.wp-api.org/author/humanmade/","slug":"humanmade","avatar_urls":{"24":"http://2.gravatar.com/avatar/83888eb8aea456e4322577f96b4dbaab?s=24&d=mm&r=g","48":"http://2.gravatar.com/avatar/83888eb8aea456e4322577f96b4dbaab?s=48&d=mm&r=g","96":"http://2.gravatar.com/avatar/83888eb8aea456e4322577f96b4dbaab?s=96&d=mm&r=g"},"meta":[],"_links":{"self":[{"href":"https://demo.wp-api.org/wp-json/wp/v2/users/1"}],"collection":[{"href":"https://demo.wp-api.org/wp-json/wp/v2/users"}]}}
```

Deshabilitar REST API

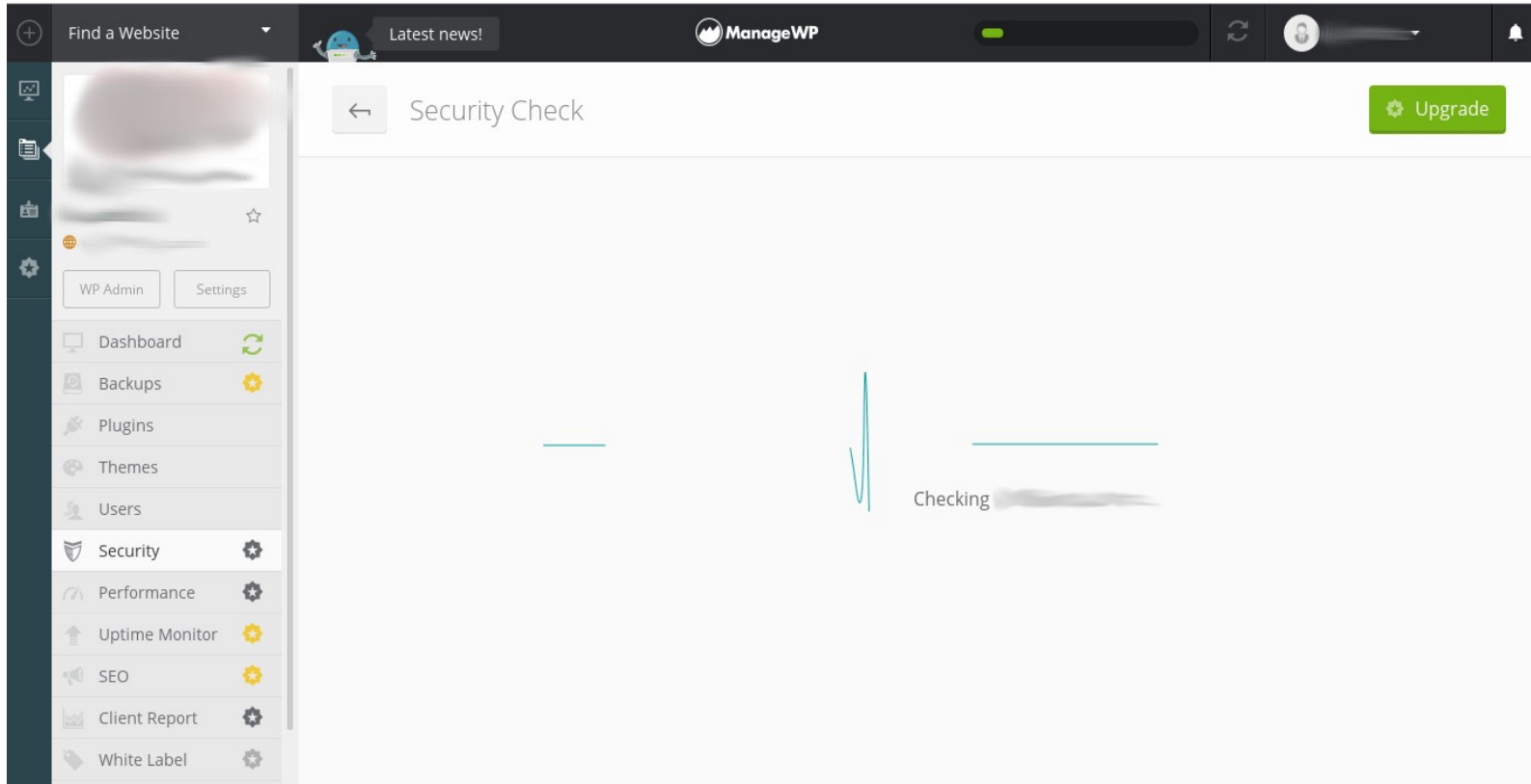
<https://repl.it/IU2M>

Deshabilitar los endpoints de users

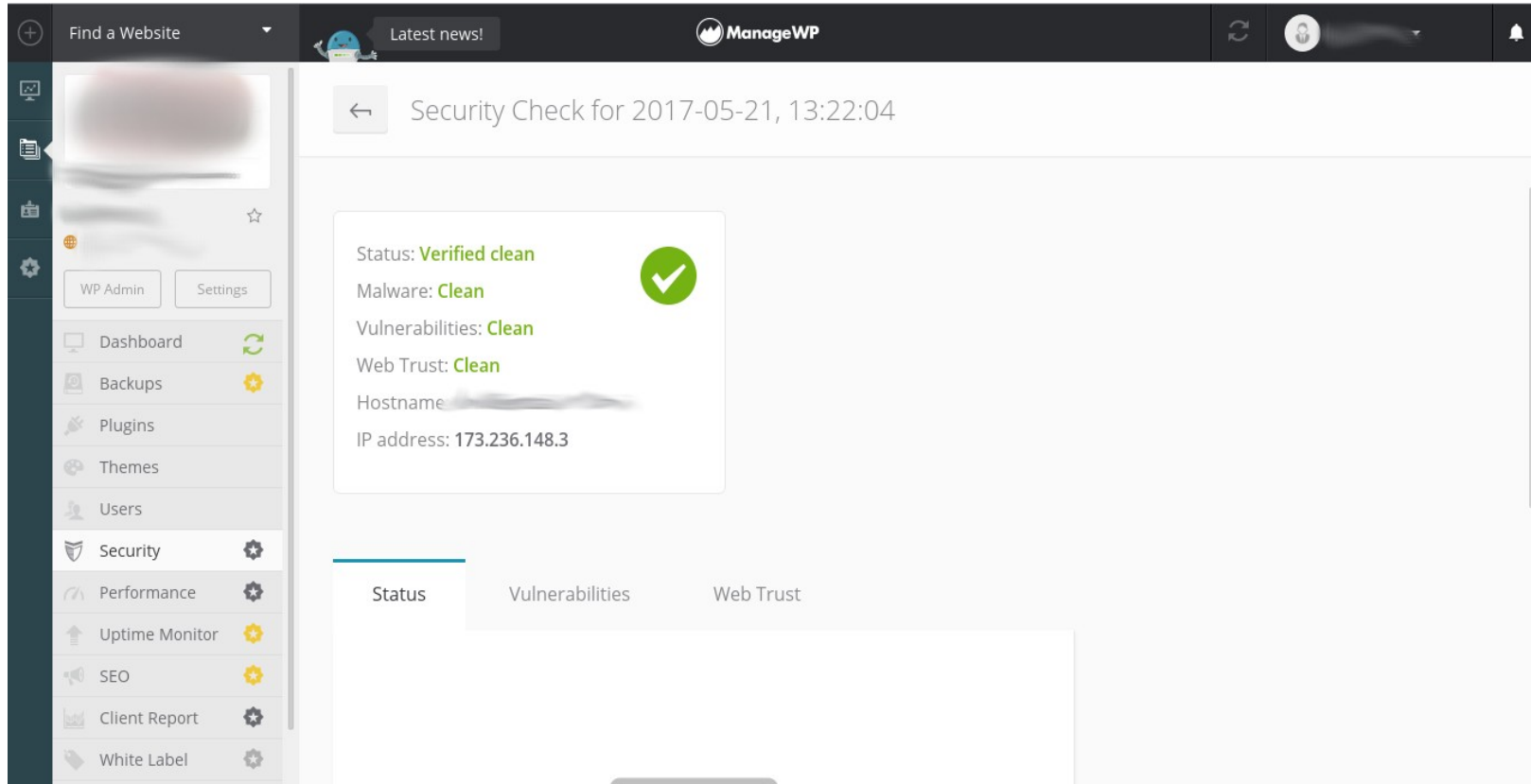
<https://repl.it/IU1z>



ManageWP - Seguridad



ManageWP – Seguridad

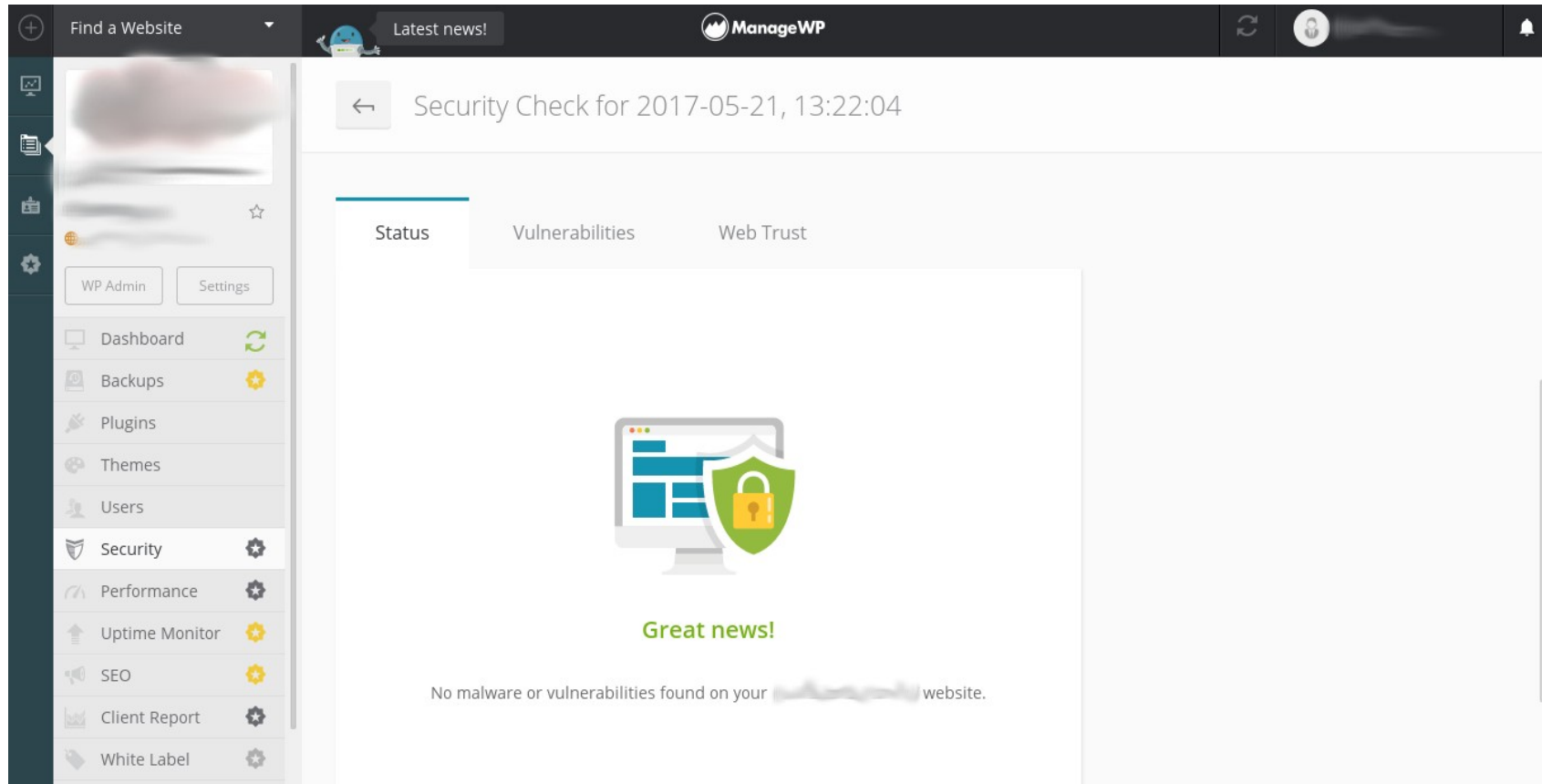


The screenshot displays the ManageWP dashboard interface. On the left is a dark sidebar with navigation icons and a menu. The main content area shows a 'Security Check for 2017-05-21, 13:22:04' result. A white box contains the following information:

- Status: **Verified clean** (with a green checkmark icon)
- Malware: **Clean**
- Vulnerabilities: **Clean**
- Web Trust: **Clean**
- Hostname: [redacted]
- IP address: 173.236.148.3

Below this box are three tabs: 'Status' (active), 'Vulnerabilities', and 'Web Trust'. The 'Status' tab is currently selected.

ManageWP - Seguridad



The screenshot displays the ManageWP dashboard interface. At the top, there's a dark header bar with a 'Find a Website' dropdown, a 'Latest news!' notification, the 'ManageWP' logo, and user profile icons. The left sidebar contains a list of management tools: Dashboard, Backups, Plugins, Themes, Users, Security (highlighted), Performance, Uptime Monitor, SEO, Client Report, and White Label. The main content area shows a 'Security Check for 2017-05-21, 13:22:04' result. It features three tabs: 'Status' (active), 'Vulnerabilities', and 'Web Trust'. Under the 'Status' tab, a large green shield icon with a padlock is centered, accompanied by the text 'Great news!' and 'No malware or vulnerabilities found on your [redacted] website.'

ManageWP - Seguridad

The screenshot displays the ManageWP dashboard for a specific website. The top navigation bar includes a search function, a 'Latest news!' notification, the ManageWP logo, a refresh button, a user profile, and a bell icon. The left sidebar contains a menu with options: WP Admin, Settings, Dashboard, Backups, Plugins, Themes, Users, Security (highlighted), Performance, Uptime Monitor, SEO, Client Report, and White Label. The main content area is titled 'Security Check for 2016-12-24, 07:21:15'. It features a status box with a red exclamation mark icon indicating 'Problems detected'. The status details are as follows:

- Status: **Problems detected**
- Malware: **Clean**
- Vulnerabilities: **Detected**
- Web Trust: **Clean**
- Hostname: [Redacted]
- IP address: [Redacted]

Below the status box, there are three tabs: 'Status', 'Vulnerabilities' (which is active), and 'Web Trust'. Under the 'Vulnerabilities' tab, a message states '1 vulnerability found.' followed by a list of vulnerabilities, with the first one partially visible as 'WordPress Default User Exists'.

ManageWP - Seguridad

The screenshot shows the ManageWP dashboard with a dark header. The left sidebar contains navigation links: Find a Website, Latest news!, WP Admin, Settings, Dashboard, Backups, Plugins, Themes, Users, Security (highlighted), Performance, Uptime Monitor, SEO, Client Report, and White Label. The main content area displays a 'Security Check for 2016-12-24, 07:21:15'. It lists 'vulnerabilities: Detected', 'Web Trust: Clean', and 'Hostname: [redacted]'. Below this, there are tabs for Status, Vulnerabilities (selected), and Web Trust. The Vulnerabilities tab shows '1 vulnerability found.' and a list item '+ WordPress Debug Log Exists'.

Find a Website

Latest news!

ManageWP

Security Check for 2016-12-24, 07:21:15

vulnerabilities: **Detected**

Web Trust: **Clean**

Hostname: [redacted]

IP address: [redacted]

WP Admin Settings

Dashboard Backups Plugins Themes Users Security Performance Uptime Monitor SEO Client Report White Label

Status Vulnerabilities Web Trust

1 vulnerability found.

+ WordPress Debug Log Exists

ManageWP - Seguridad

The screenshot displays the ManageWP dashboard with a sidebar on the left containing navigation links: Dashboard, Backups, Plugins, Themes, Users, Security (highlighted), Performance, Uptime Monitor, SEO, Client Report, and White Label. The main content area shows a 'Security Check for 2017-05-21, 13:22:04' with tabs for Status, Vulnerabilities, and Web Trust. The 'Web Trust' tab is active, showing a 'Domain clean on' status and a list of security checks, all of which are marked with green checkmarks and include a 'Learn more...' link.

Check	Status	Action
Google Safe Browsing	✓	Learn more...
Norton Safe Web	✓	Learn more...
Phish tank	✓	Learn more...
Opera browser	✓	Learn more...
SiteAdvisor	✓	Learn more...
Sucuri Malware Labs blacklist	✓	Learn more...
SpamHaus DBL	✓	Learn more...
Yandex (via Sophos)	✓	Learn more...

ManageWP - Uptime

The screenshot shows the ManageWP Uptime Monitor interface. The top navigation bar includes a search bar, a 'Latest news!' notification, the ManageWP logo, and user profile controls. The left sidebar contains a list of site management tools, with 'Uptime Monitor' highlighted. The main content area is titled 'Uptime Monitor' and features a 'Deactivate' button. It is divided into two tabs: 'Uptime Activity' (selected) and 'Settings'. Under 'Uptime Activity', a large green circle with 'UP' indicates the site is online. Text shows an overall uptime of 99.89% and a duration of 59d 1h. A toggle switch is set to 'On'. A 'Latest downtime' event is listed: '2017-03-23, 11:52:53, lasted for 4m 37s'. Below this, an 'Uptime overview' section shows three boxes, each with '100%' uptime for different periods: 'last 24 hours', 'last 7 days', and 'last 30 days'. A 'Latest events' section at the bottom shows a green 'Up' status with the message 'Everything is ok' and a timestamp '2017-03-23, 11:57:30 for 59d 1h'.

Find a Website

Latest news!

ManageWP

Uptime Monitor

Deactivate

Uptime Activity

Settings

UP

Overall uptime is **99.89%**
Up for 59d 1h

Off On

Latest downtime: 2017-03-23, 11:52:53, lasted for 4m 37s

Uptime overview

100%
(last 24 hours)

100%
(last 7 days)

100%
(last 30 days)

Latest events

Up Everything is ok 2017-03-23, 11:57:30 for 59d 1h

ManageWP - Uptime

Find a Website Latest news! ManageWP

Uptime Monitor Deactivate

Uptime overview

- 100% (last 24 hours)
- 100% (last 7 days)
- 100% (last 30 days)

Latest events

▲ Up	Everything is ok	2017-03-23, 11:57:30 for 59d 1h
▼ Down	503 Service Unavailable	2017-03-23, 11:52:53 for 4m 37s
▲ Up	Everything is ok	2017-03-23, 02:14:07 for 9h 38m
▼ Down	Connection Timeout	2017-03-23, 01:37:01 for 37m 6s
▲ Up	Everything is ok	2017-03-22, 18:03:07 for 7h 33m

Show more...

ManageWP - Uptime

The screenshot shows the ManageWP interface. The top navigation bar includes a 'Find a Website' dropdown, a 'Latest news!' notification, the 'ManageWP' logo, a refresh button, a user profile icon, and a bell icon. The left sidebar contains a 'Find a Website' dropdown, a blurred website preview, and a list of tools: WP Admin, Settings, Dashboard, Backups, Plugins, Themes, Users, Security, Performance, Uptime Monitor (highlighted), SEO, Client Report, and White Label. The main content area is titled 'Uptime Monitor' with a 'Deactivate' button. Under the 'General' tab, the 'Monitoring interval' is set to 'Every 5 minutes' on a slider ranging from 1 minute to 15 minutes. The 'Notification delay' is set to 'No delay' on a slider ranging from 0 to 60 minutes. A text box explains that the notification delay option will delay sending of the notification by given time, and if the website comes back up during this interval, the notification will not be sent. There is an unchecked checkbox for 'Use keyword monitoring' with an information icon, and a text input field below it with the placeholder 'Enter the keyword you want to monitor here'.

Find a Website

Latest news!

ManageWP

Uptime Monitor

Deactivate

General

Monitoring interval: Every 5 minutes

1 minute 5 minutes 10 minutes 15 minutes

Notification delay: No delay

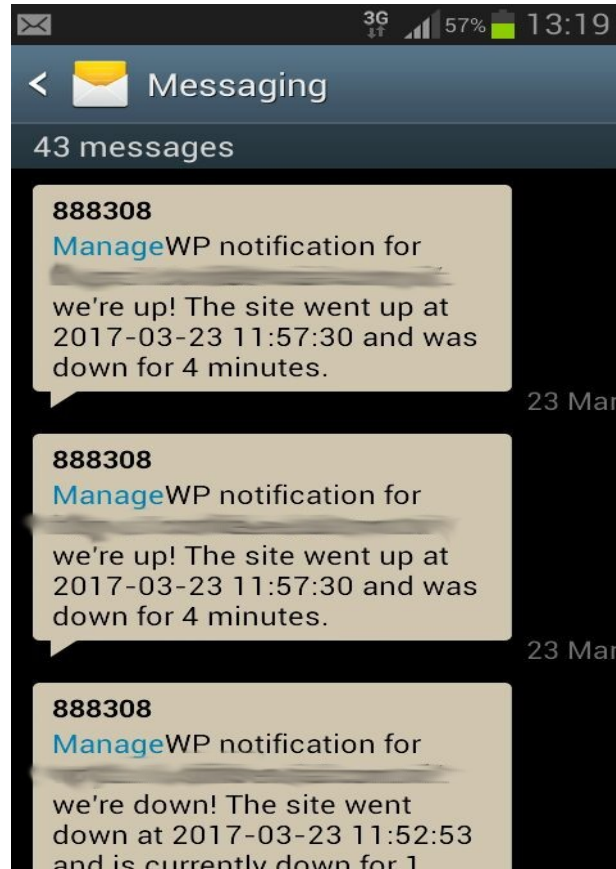
No delay 5m 10m 15m 20m 30m 45m 60m

This option will delay sending of the notification by given time. If the website comes back up during this interval, the notification will not be sent.

☐ Use keyword monitoring ⓘ

Enter the keyword you want to monitor here

ManageWP - Uptime



ManageWP - Update

The screenshot shows the ManageWP dashboard interface. At the top, there's a header with a search bar, a 'Latest news!' notification, the ManageWP logo, and user profile icons. The left sidebar contains a 'Find a Website' dropdown, a list of 'Add-ons' (Free Backups, Free Security Ch..., Free Performan..., Backups, Uptime Monitor, SEO, Free Client Rep...), a 'Status' section (Disconnected, Multisite Netwo..., SSL enabled, SSL not enabled, Updates availab...), and 'Tags' (Clientes, Comunidad, Desarrollo, Live). The main content area is divided into two sections: 'Updates' and 'Services'.

Updates Section:

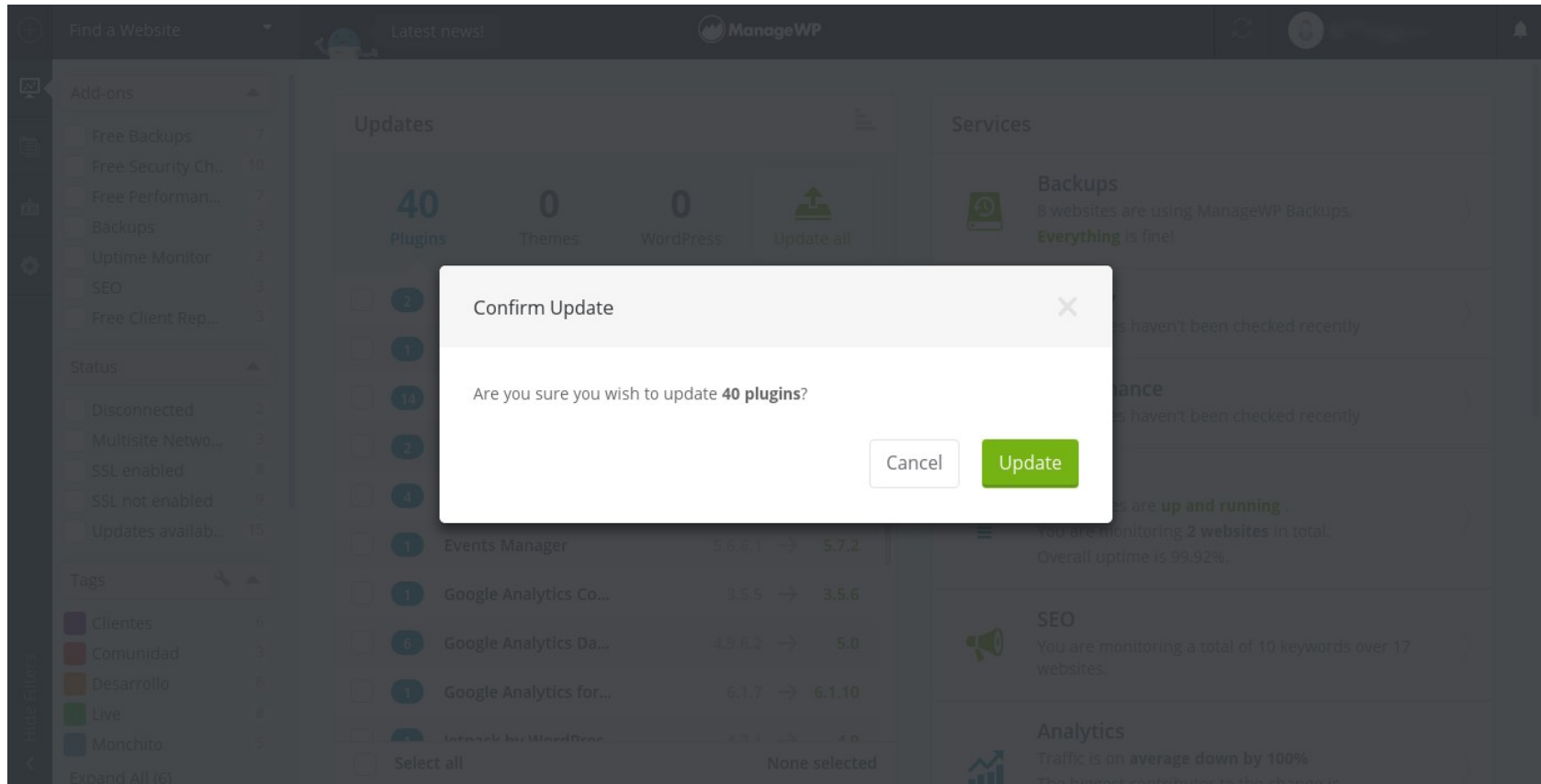
- Summary: 40 Plugins, 0 Themes, 0 WordPress. An 'Update all' button is present.
- Table of updates:

Plugin/Theme	Current Version	Latest Version
Advanced Ads	1.7.24	1.7.25
Ajax Search Lite	4.7.3	4.7.4
Akismet Anti-Spam	3.3.1	3.3.2
Coming Soon Page &...	5.0.9	5.0.10
Duplicator	1.2.6	1.2.8
Events Manager	5.6.6.1	5.7.2
Google Analytics Co...	3.5.5	3.5.6
Google Analytics Da...	4.9.6.2	5.0
Google Analytics for...	6.1.7	6.1.10
Intack by WordPress	4.7.1	4.8

Services Section:

- Backups:** 8 websites are using ManageWP Backups. **Everything** is fine!
- Security:** 16 websites haven't been checked recently.
- Performance:** 17 websites haven't been checked recently.
- Uptime:** All websites are **up and running**. You are monitoring **2 websites** in total. Overall uptime is 99.92%.
- SEO:** You are monitoring a total of 10 keywords over 17 websites.
- Analytics:** Traffic is on **average down by 100%**. The highest contributor to the change is...

ManageWP - Update



ManageWP - Update

Find a Website

Latest news!





ManageWP

Manage Plugins

+ Add plugin

Filter plugins

12 Active 4 Inactive 3 Updates

<input type="checkbox"/>	 Advanced Custom Fields ☆ Customise WordPress with powerful, professional and intuitive fields	4.4.11
<input type="checkbox"/>	 Akismet Anti-Spam ☆ Akismet checks your comments and contact form submissions against our global database of spam to...	3.3.1
<input type="checkbox"/>	 BackWPup ☆ Schedule complete automatic backups of your WordPress installation. Decide which content will be stored (Dro...	3.3.7
<input type="checkbox"/>	 Duplicator ☆ WordPress migration and backups are much easier with Duplicator! Clone, backup, move and transfer an entire...	1.2.6
<input type="checkbox"/>	Select all	

None selected Deactivate Deactivate & Delete

ManageWP - Update

The screenshot displays the ManageWP dashboard. On the left is a sidebar with navigation links: Find a Website, WP Admin, Settings, Dashboard, Backups, Plugins, Themes, Users, Security, Performance, Uptime Monitor, SEO, Client Report, and White Label. The main header includes a 'Latest news!' notification, the ManageWP logo, and user profile controls. The 'Manage Plugins' section is active, showing a search bar and filters for 12 Active, 4 Inactive, and 3 Updates plugins. Three plugins are listed with checkboxes for selection: Akismet Anti-Spam (3.3.1 to 3.3.2), Duplicator (1.2.6 to 1.2.8), and Google Analytics Dashboard for WP (4.9.6.2 to 5.0). At the bottom, a 'Deselect all' checkbox is on the left, and a summary bar on the right shows 'With 3 selected:' and an 'Update' button.

Plugin	Current Version	Latest Version
Akismet Anti-Spam	3.3.1	3.3.2
Duplicator	1.2.6	1.2.8
Google Analytics Dashboard for WP	4.9.6.2	5.0

ManageWP - Respaldo

The screenshot displays the ManageWP interface for managing WordPress backups. The top navigation bar includes a search bar, a 'Latest news!' notification, the ManageWP logo, and user controls. The left sidebar contains a list of site management tools: WP Admin, Settings, Dashboard, Backups, Plugins, Themes, Users, Security, Performance, Uptime Monitor, SEO, Client Report, White Label, and More Tools... The main content area is titled 'Backups' and features a calendar for May 2017. The calendar shows a backup scheduled for May 20th at 00:47:26. To the right of the calendar, there are buttons for 'Off', 'On', and 'Backup Now'. Below the calendar, it states 'Backups for 2017-05-20' and 'Scheduled backup - Every day'. The right sidebar contains a 'Deactivate' button, tabs for 'Overview', 'Content', 'Settings', and 'Restore from ZIP', and buttons for 'Restore', 'Download', and 'Clone'. It also displays site information: WordPress version: 4.7.5, Active theme: Choccolita v1.0.0, Active Plugins: 23, Published posts: 644, and Approved comments: 107. At the bottom, there is a preview of the website being managed.

Find a Website

Latest news!

ManageWP

Backups

Deactivate

WP Admin Settings

Dashboard

Backups

Plugins

Themes

Users

Security

Performance

Uptime Monitor

SEO

Client Report

White Label

More Tools...

System Info

Maintenance Mode

MAY 2017

30 1 2 3 4 5 6

7 8 9 10 11 12 13

14 15 16 17 18 19 20

21 22 23 24 25 26 27

28 29 30 31 1 2 3

4 5 6 7 8 9 10

Off On

Latest backup:
2017-05-21, 01:00:11

Next backup:
2017-05-22, 00:14:25

Backup Now

Backups for 2017-05-20

00:47:26 Scheduled backup - Every day

Overview Content Settings Restore from ZIP

Restore Download Clone

WordPress version: 4.7.5

Active theme: Choccolita v1.0.0

Active Plugins: 23 Published posts: 644

Approved comments: 107

WORDCAMP
MANAGUA 2017:

ManageWP - Clonar

The screenshot displays the ManageWP dashboard. On the left is a sidebar with a search bar 'Find a Website', a 'Latest news!' notification, and a menu with items: WP Admin, Settings, Dashboard, Backups, Plugins, Themes, Users, Security, Performance, Uptime Monitor, SEO, Client Report, White Label, More Tools..., System Info, and Maintenance Mode. The main content area is titled 'Backups > Clone'. It shows a 'Source' section with a preview of a website and the text 'Using snapshot from: 2017-05-20, 00:47:26'. Below this is 'Step 1: Choose Clone Type' with three options: 'Existing website in ManageWP', 'Same domain on a new server', and 'New website', separated by 'OR' indicators.

ManageWP - Admin

The screenshot displays the ManageWP Admin interface. At the top, there's a dark header with a 'Find a Website' dropdown, a 'Latest news!' notification, the 'ManageWP' logo, and user profile icons. The left sidebar contains a navigation menu with options like Dashboard, Backups, Plugins, Themes, Users (highlighted), Security, Performance, Uptime Monitor, SEO, Client Report, and White Label. The main content area is titled 'Manage Users' and includes a '+ Add New User' button. Below this, there are two tabs: 'Administrator' (with a count of 2) and 'Editor' (with a count of 1). The user list shows two entries, both with the role 'Administrator' and the text 'No biographical info'. At the bottom, there's a 'Select all' checkbox, a 'None selected' status, and three action buttons: 'Change Role', 'Change Password', and 'Delete'.

ManageWP - Admin

The screenshot displays the ManageWP Admin dashboard. The top navigation bar includes a 'Find a Website' dropdown, a 'Latest news!' notification, the 'ManageWP' logo, a refresh button, a user profile icon, and a bell icon. The left sidebar contains a vertical menu with icons and labels for: Dashboard, Backups, Plugins, Themes (highlighted), Users, Security, Performance, Uptime Monitor, SEO, Client Report, and White Label. The main content area is titled 'Manage Themes' and features a green '+ Add theme' button. Below the title is a 'Filter themes' search box. A tabbed interface shows 'Active' (1) and 'Inactive' (1) themes. The 'Active' tab is selected, showing a theme card for 'Sacuanjoché' with a star icon, a description, and the version '1.0-wpcom'. At the bottom, a grey informational banner states: 'One theme must always be active'.

ManageWP - Panel





Wordfence™
Securing your **WordPress** website

Wordfence

WP Nicaragua

0

Nuevo

Hola,

Medios

Páginas

Comentarios

Apariencia

Plugins

Usuarios

Herramientas

Ajustes

SunshinePlugin

Wordfence 4

Dashboard

Scan

Firewall

Blocking

Live Traffic

Tools

Options

Upgrade To Premium

Cerrar menú

Top IPs Blocked

24 Hours7 Days30 Days

IP	Country	Block Count
80.67.249.55	Russian Federation	29
91.144.149.126	Russian Federation	22
81.1.212.101	Russian Federation	22
37.113.130.68	Russian Federation	20
95.191.227.221	Russian Federation	20
194.135.247.146	Russian Federation	19
94.29.124.189	Russian Federation	17
78.107.234.199	Russian Federation	17
46.172.208.41	Ukraine	16
89.188.124.197	Russian Federation	16

Show more

Login Attempts

Total Attacks

Last Updated: 29 mins ago

Top Countries by Number of Attacks - Last 7 Days

Local SiteWordfence Network

Country	Block Count
Turkey	4
United States	4
Ukraine	1
India	1
Indonesia	1
-	-

Wordfence

The screenshot displays the Wordfence interface within a WordPress dashboard. The left sidebar contains navigation links: Medios, Páginas, Comentarios, Apariencia, Plugins, Usuarios, Herramientas, Ajustes, SunshinePlugin, Wordfence (highlighted), Dashboard, Scan, Firewall, Blocking, Live Traffic, Tools, Options, Upgrade To Premium, and Cerrar menú. The main content area shows the Wordfence 'Blocking' section. At the top, there's a status bar with 'Human', 'Bot', 'Warning', and 'Blocked' indicators. Below this is the 'Sucuri Uptime Monitor' section with buttons for 'Block this IP', 'Block this network', 'Run WHOIS on 72.14.187.58', and 'See recent traffic'. The main list shows several blocked entries from an IP in Ukraine (91.200.14.171). Each entry includes a message about being blocked by a firewall for CVE-2017-18342, the timestamp '5/21/2017 7:13:58 AM (6 hours 51 mins ago)', and the IP address. Each entry also has buttons for 'Block this IP', 'Block this network', 'Run WHOIS on 91.200.14.171', 'See recent traffic', and 'Whitelist param from Firewall'.

WP Nicaragua 0 + Nuevo Hola, [User Avatar]

Medios
Páginas
Comentarios
Apariencia
Plugins
Usuarios
Herramientas
Ajustes
SunshinePlugin
Wordfence
Dashboard
Scan
Firewall
Blocking
Live Traffic
Tools
Options
Upgrade To Premium
Cerrar menú

Dallas, United States visited <http://wpnicaragua.org/>

Human Bot Warning Blocked

Sucuri Uptime Monitor

Block this IP Block this network Run WHOIS on 72.14.187.58 See recent traffic

Ukraine was blocked by firewall for CYSTEME Finder <= 1.3 - Multiple Unauthenticated Vulnerabilities at <http://wpnicaragua.org/wp-content/plugins/cysteme-finder/php/connector.php?wphome=%2F>
5/21/2017 7:13:58 AM (6 hours 51 mins ago) IP: 91.200.14.171 [block] Hostname: email.example.com

Block this IP Block this network Run WHOIS on 91.200.14.171 See recent traffic Whitelist param from Firewall

Ukraine tried to access non-existent page <https://wpnicaragua.org/wp-content/plugins/easyrotator-for-wordpress/c.php>
5/21/2017 7:13:57 AM (6 hours 51 mins ago) IP: 91.200.14.171 [block] Hostname: email.example.com

Block this IP Block this network Run WHOIS on 91.200.14.171 See recent traffic

Ukraine visited <https://wpnicaragua.org/wp-content/plugins/easyrotator-for-wordpress/c.php>
5/21/2017 7:13:56 AM (6 hours 51 mins ago) IP: 91.200.14.171 [block] Hostname: email.example.com

Block this IP Block this network Run WHOIS on 91.200.14.171 See recent traffic

Ukraine visited <http://wpnicaragua.org/wp-content/plugins/easyrotator-for-wordpress/c.php>
5/21/2017 7:13:55 AM (6 hours 51 mins ago) IP: 91.200.14.171 [block] Hostname: email.example.com

Block this IP Block this network Run WHOIS on 91.200.14.171 See recent traffic

Ukraine tried to access non-existent page <https://wpnicaragua.org/wp-content/plugins/easyrotator-for-wordpress/b.php>
5/21/2017 7:13:55 AM (6 hours 51 mins ago) IP: 91.200.14.171 [block] Hostname: email.example.com

Block this IP Block this network Run WHOIS on 91.200.14.171 See recent traffic

Ukraine visited <https://wpnicaragua.org/wp-content/plugins/easyrotator-for-wordpress/b.php>
5/21/2017 7:13:54 AM (6 hours 51 mins ago) IP: 91.200.14.171 [block] Hostname: email.example.com

Block this IP Block this network Run WHOIS on 91.200.14.171 See recent traffic

Wordfence

The screenshot shows the Wordfence plugin interface in a WordPress dashboard. The left sidebar contains the following menu items: Escritorio, Entradas, Medios, Páginas, Comentarios, Apariencia, Plugins, Usuarios, Herramientas, Ajustes, SunshinePlugin, Wordfence (highlighted with a blue bar and a yellow notification bubble with the number 4), Dashboard, Scan, Firewall, Blocking, Live Traffic, Tools, and Options. The main content area is titled 'Select which countries to block' and features two buttons: 'Block All' (in blue) and 'Unblock All' (in white). Below these buttons are three alphabetical lists of countries, each with a grid of buttons to select or unselect them. The first list (A) includes Afghanistan, Aland Islands, Albania, Algeria, American Samoa, Andorra, and Angola. The second list (B) includes Anguilla, Antarctica, Antigua and Barbuda, Argentina, Armenia, Aruba, and Australia. The third list (C) includes Austria and Azerbaijan. The interface is clean and modern, with a dark sidebar and a light gray main area.

WP Nicaragua 0 + Nuevo Hola, [User Avatar]

Select which countries to block

A — ☒ A B C D E F G H I J K L M N O P Q R S T U V W Y Z

Afghanistan	Aland Islands	Albania	Algeria	American Samoa	Andorra	Angola
Anguilla	Antarctica	Antigua and Barbuda	Argentina	Armenia	Aruba	Australia
Austria	Azerbaijan					

B — A ☒ B C D E F G H I J K L M N O P Q R S T U V W Y Z

Bahamas	Bahrain	Bangladesh	Barbados	Belarus	Belgium	Belize
Benin	Bermuda	Bhutan	Bolivia	Bonaire, Saint Eustatius and Saba	Bosnia and Herzegovina	Botswana
Bouvet Island	Brazil	British Indian Ocean Territory	Brunei Darussalam	Bulgaria	Burkina Faso	Burundi

C — A B ☒ C D E F G H I J K L M N O P Q R S T U V W Y Z

Cambodia	Cameroon	Canada	Cape Verde	Cayman Islands	Central African Republic	Chad
			Cocos			

Wordfence

The screenshot shows the Wordfence WordPress plugin interface. The top navigation bar includes a home icon, 'WP Nicaragua', a notification bell with '0', a '+ Nuevo' button, and a user profile with the name 'Hola,'. The left sidebar contains a menu with items: Escritorio, Entradas, Medios, Páginas, Comentarios, Apariencia, Plugins, Usuarios, Herramientas, Ajustes, and Wordfence (highlighted with a yellow bar and a plus icon). Below the sidebar, the main content area is titled 'Wordfence Live Activity: Idle'. It features three tabs: 'Blocked IPs', 'Country Blocking', and 'Advanced Blocking' (which is selected). A link 'Learn more about Advanced Blocking' is provided. A yellow warning box states: 'Rate limiting rules and advanced blocking are disabled. You can enable it on the [Wordfence Options page](#) at the top.' The 'Advanced Blocking' section contains several input fields for defining blocking rules: 'IP address range' (with examples: 192.168.200.200 - 192.168.200.220), 'Hostname' (with examples: *.amazonaws.com, *.linode.com and a note about DNS queries), 'User-Agent (browser) that matches' (with examples: *badRobot*, AnotherBadRobot*, *someBrowserSuffix), 'Referer (website visitor arrived from) that matches' (with examples: *badWebsite*, AnotherBadWebsite*, *someWebsiteSuffix), and 'Enter a reason you're blocking this' (with a note about case insensitivity). On the right side, there is a promotional banner for 'Upgrade Your Protection' for Wordfence Premium, featuring an illustration of two people at laptops and a server rack, with a 'GET PREMIUM' button. Below this is a section titled 'Have you been hacked?' with text about security experts and a small illustration of a blue tool.

Wordfence

The screenshot shows the Wordfence Scan interface within a WordPress dashboard. The top navigation bar includes the WordPress logo, site name 'WP Nicaragua', a notification bell with '0' items, and a '+ Nuevo' button. The user is logged in as 'Hola, [user]'. The left sidebar contains a menu with items: Escritorio, Entradas, Medios, Páginas, Comentarios, Apariencia, Plugins, Usuarios, Herramientas, Ajustes, and SunshinePlugin. The Wordfence plugin is highlighted with a notification badge showing '4' items. Below the sidebar, the Wordfence Scan interface is displayed. It has three tabs: 'Scan' (active), 'Scheduling', and 'Options'. A large blue button labeled 'START A WORDFENCE SCAN' is prominent, with a link 'Click to kill the current scan.' below it. A 'Learn more about scanning' link is also present. The 'Scan Summary' section shows a log of scan activities from May 21, 14:08:34 to 14:08:38. The log includes checks for domain blacklists, IP signatures, core/theme/plugin file signatures, malware files, and WordPress core files. The results show 'Secure.', 'Success.', and 'Success.' for the first three items, and 'Disabled' for the last two, with links to 'Visit Options to Enable'. A 'Paid Members Only' link is also visible. Below the log, a message states 'You are running the Wordfence Community Scan signatures.' A box titled 'The Wordfence Scan alerts you if you've been hacked' explains the Threat Defense Feed and offers a 'GET PREMIUM' button. On the right, a large blue banner promotes 'Upgrade Your Protection' for Wordfence Premium, highlighting features like firewall rules, malware signatures, and real-time updates, with a 'GET PREMIUM' button. Below this, a section titled 'Have you been hacked?' offers assistance from security experts.

WP Nicaragua 0 + Nuevo Hola, [user]

Escritorio Entradas Medios Páginas Comentarios Apariencia Plugins Usuarios Herramientas Ajustes SunshinePlugin Wordfence 4

Dashboard Scan Firewall Blocking Live Traffic Tools Options

Wordfence Scan

Scan Scheduling Options

[Learn more about scanning](#)

START A WORDFENCE SCAN

[Click to kill the current scan.](#)

Scan Summary

Log Entry	Status
[May 21 14:08:34] Checking if your site is on a domain blacklist is for paid members only	Paid Members Only
[May 21 14:08:36] Checking for the most secure way to get IPs	Secure.
[May 21 14:08:37] Fetching core, theme and plugin file signatures from Wordfence	Success.
[May 21 14:08:38] Fetching list of known malware files from Wordfence	Success.
[May 21 14:08:38] Comparing core WordPress files against originals in repository	000
[May 21 14:08:38] Skipping theme scan	Disabled Visit Options to Enable
[May 21 14:08:38] Skipping plugin scan	Disabled Visit Options to Enable

You are running the Wordfence Community Scan signatures.

The Wordfence Scan alerts you if you've been hacked

As new threats emerge, the Threat Defense Feed is updated to detect these new hacks. The Premium version of the Threat Defense Feed is updated in real-time protecting you immediately. As a free user **you are receiving the community version** of the feed which is updated 30 days later.

GET PREMIUM

Upgrade Your Protection

Wordfence Premium customers receive firewall rules, malware signatures and malicious IP updates in real time.

GET PREMIUM

Have you been hacked?

Our team of security experts will clean the infection and remove malicious content.

Wordfence

WP Nicaragua 0 + Nuevo

Hola,

- Receive real-time Firewall and Scan engine rule updates for protection as threats emerge
- Other advanced features like IP reputation monitoring, an advanced comment spam filter, advanced scanning options, cell phone sign-in and country blocking give you the best protection available
- Access to Premium Support
- Discounts of up to 90% available for multiyear and multi-license purchases

[GET PREMIUM](#)

Start a Password Audit

Audit your site passwords by having us securely simulate a password cracking attempt using our high performance servers. Your report will appear here and you can easily alert your users to a weak password or change their passwords and email them the change.

Select the kind of audit you would like to do

Audit administrator level accounts (extensive audit against a large dictionary of approx. 260 Million ▼)

Notify when ready

leo.telsen@gmail.com

Results will appear on this page. We will email you when they're ready.

[Start Password Audit](#)

Audit Status

You don't have any password auditing jobs in progress or completed yet.

Password Audit Results

You don't have any user accounts with a weak password at this time.

Gracias por crear con [WordPress](#).

Versión 4.7.5

Wordfence Premium customers receive firewall rules, malware signatures and malicious IP updates in real time.

[GET PREMIUM](#)

Have you been hacked?

Our team of security experts will clean the infection and remove malicious content. Once your site is restored we will provide a detailed report of our findings.

All for an affordable rate.

[GET HELP](#)

Would you like to remove these ads? [Get Premium](#)



**iThemes
Security**

iThemes Security – Ajustes Globales

Ajustes globales

Configurar los parámetros básicos que controlan la forma de funcionar de iThemes Security.

[Configurar ajustes](#)

iThemes Security – Ajustes Globales

Ajustes globales

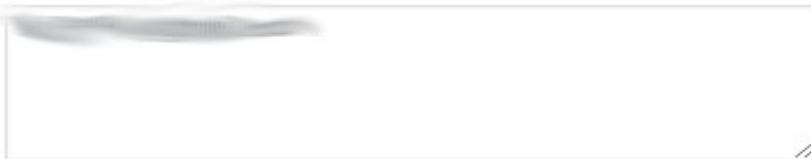
Las siguientes opciones modifican el funcionamiento de la mayoría de características ofrecidas por iThemes Security.

Escribir en los archivos

☒ **Permitir a iThemes Security modificar los archivos wp-config.php y .htaccess.**

Si deseas permitir o no que de forma automática iThemes Security tenga permisos de escritura en los archivos wp-config.php y .htaccess. Si está desactivado, será necesario que añadas manualmente las opciones de configuración en esos archivos.

Email de Notificación



La dirección de correo electrónico a donde todos los avisos de seguridad serán enviados. Una dirección por línea.

iThemes Security – Ajustes Globales

Mensaje de bloqueo al servidor

error

El mensaje que se mostrará cuando un ordenador (host) ha sido bloqueado.

Puedes utilizar HTML in tu mensaje. Las etiquetas permitidas incluyen: a, br, em, strong, h1, h2, h3, h4, h5, h6, div

Mensaje de bloqueo del usuario

You have been locked out due to too many invalid login attempts.

iThemes Security – Ajustes Globales

Lista negra de infractor reincidente

☒ **Habilitar lista negra de infractor reincidente**

Si esta casilla está marcada la dirección IP del equipo infractor será añadido a la lista negra de "Usuarios Prohibidos" después de haber alcanzado el número de bloqueos que se enumeran a continuación.

Umbral de lista negra

Bloqueos

El número de bloqueos por IP antes de que banear permanentemente de este sitio al servidor.

Período retroactivo Lista negra

Días

¿Cuántos días hay que recordar un bloqueo para cumplir con la cuenta de la lista negra anterior?

Período de bloqueo

Minutos

Lo que tarda un servidor o un usuario en ser baneado en este sitio tras alcanzar el límite de accesos incorrectos. El ajuste por defecto de 15 minutos es el recomendable, ya que incrementarlo puede evitar que IPs atacantes se añadan a la lista negra.

iThemes Security – Verificación de Permisos

Permisos de archivo






Lista los permisos de los archivos y directorios en las áreas clave del sitio.

Configurar ajustes

iThemes Security – Verificación de Permisos

Permisos de archivo

Volver a cargar los detalles de los permisos de archivo

Ruta relativa	Sugerencia	Valor	Resultado	Estado
/	755	755	OK	
wp-includes	755	755	OK	
wp-admin	755	755	OK	
wp-admin/js	755	755	OK	
wp-content	755	755	OK	
wp-content/themes	755	755	OK	
wp-content/plugins	755	755	OK	
wp-content/uploads	755	755	OK	



iThemes Security – Ocultar Escritorio

Ocultar escritorio

Ocultar la página de acceso cambiando su nombre y evitando el acceso a wp-login.php y wp-admin.

[Configurar ajustes](#)

iThemes Security – Ocultar Escritorio



Todos (31) | Recomendable (25) | Avanzado (6)

Ocultar escritorio

Ocultar ajustes

Ocultar la página de inicio de sesión (wp-login.php, wp-admin, admin y login) por lo que es más difícil de encontrar por ataques automatizados y haciendo más fácil para los usuarios no familiarizados con la plataforma WordPress.

Ocultar escritorio ☒ **Habilita la función ocultar escritorio.**

Slug de Inicio de Sesión

URL de acceso: <http://teodolinda.com.ni/kronk>

El slug de la URL de acceso no puede ser "login", "admin", "escritorio," o "wp-login.php" ya que estos son los utilizados por defecto en WordPress.

Nota: Limitado a caracteres alfanuméricos, guiones bajos (_) y guiones normales (-). No están permitidos caracteres especiales como "." y "/" y se convertirán igual que en el título de una entrada. Por favor, revisa tu elección antes de desconectar.

Activar la redirección ☒ **Redirige a los usuarios a una ubicación personalizada de tu sitio, en vez de mostrar un error de 403 (prohibido).**

iThemes Security – Ocultar Escritorio

Slug de redirección

Ubicación de redirección:

El slug al que redirigir a los usuarios cuando traten de acceder a wp-admin sin estar conectados.

Acción de acceso
personalizada

WordPress utiliza a variable "action" para gestionar la mayoría de las funciones de acceso y desconexión. Por defecto este plugin puede gestionar las normales, pero algunos plugins y temas puede que utilicen alguna acción personalizada (como desconectar de una entrada privada). Si necesitas una acción personalizada, por favor, introdúcela aquí.

Guardar ajustes

Cancelar

iThemes Security – Usuarios baneados

Usuarios baneados

Bloquea direcciones IP específicas y agentes de usuario para que no accedan a este sitio.

Configurar ajustes

Desactivar

iThemes Security – Protección contra ataques de fuerza bruta

Usuarios baneados

Esta característica te permite banear totalmente servidores y agentes de usuario de tu sitio sin tener que gestionar cualquier configuración de tu servidor. A las direcciones IP o los agentes de usuario que se encuentran en la lista de abajo no se les permitirá ninguna visita a tu sitio.

Lista negra por defecto

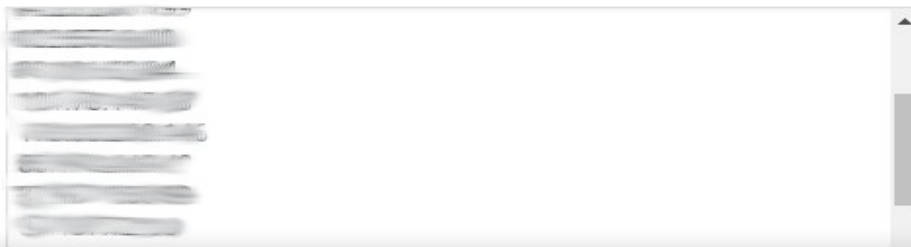
☐ **Habilitar la funcionalidad de lista negra de HackRepair.com**

Como base de inicio puedes incluir la lista negra creada por Jim Walker.

Listas de baneo

☒ **Activar listas de baneo**

Banear servidores



iThemes Security – Protección contra ataques de fuerza bruta

Activar protección contra fuerza bruta

Protege tu sitio contra atacantes que intenten acceder aleatoriamente a tu sitio.

Configurar ajustes

Desactivar

iThemes Security – Protección contra ataques de fuerza bruta

Tus ajustes actuales esta configurados así:

- **Baneo permanente:** sí
- **Número de bloqueos antes del baneo permanente:** 3
- **Cuántos bloqueos se guardan para el baneo:** 7
- **Mensaje de bloqueo al servidor:** error
- **Mensaje de bloqueo al usuario:** You have been locked out due to too many invalid login attempts.
- **Si este ordenador está en lista blanca:** sí

Máximo número de intentos de conexión por host

Intentos

El número de intentos de inicio de sesión de un usuario antes de que su servidor o el equipo quede bloqueado por el sistema. Se establece en 0 para registrar intentos fallidos de conexión sin bloquear el servidor.

Máximo número de intentos de conexión por usuario

Intentos

El número de intentos de acceso que hace un usuario antes de que el sistema bloquee su nombre de usuario. Date cuenta que esto difiere según los servidores en caso de que un atacante esté usando varios ordenadores. Además, si están usando tu nombre de acceso podrías bloquearte a ti mismo. Establece a 0 el registro de intentos de acceso fallidos por usuario

Automáticamente bloquear al usuario "admin"

☒ Inmediatamente bloquear un host que intente iniciar sesión con el nombre de usuario "admin".

iThemes Security - Copia de seguridad de base de datos

Copias de seguridad de bases de datos

Haz una copia de seguridad de la base de datos de tu sitio. Las copias de seguridad pueden hacerse de forma manual o programada.

[Configurar ajustes](#)[Desactivar](#)

iThemes Security – Copia de Seguridad de base de datos

Crear una copia de seguridad de la base de datos

Copia de seguridad completa de base de datos

☐ Marcar esta casilla hará que el script de copia de seguridad lleve a cabo una copia de seguridad de todas las tablas en su base de datos, incluso si no son parte de este sitio WordPress.

Método de copia de seguridad

Solo Correo ▼

Método Guardar copia de seguridad

Elige lo que debemos hacer con el archivo de copia de seguridad. Puedes hacer que te lo enviemos por correo electrónico, guardarlo localmente o ambos.

Copias de seguridad a guardar

3 Copias de seguridad

Limita el número de copias de seguridad almacenadas localmente (en este servidor). Cualquier copia de seguridad anterior por encima de este número se borrará. Establecerlo a "0" mantendrá todas las copias de seguridad.

Comprobación de seguridad

Comprobación de seguridad

Asegura que tu sitio web está usando los parámetros y funcionalidades recomendadas.

[Configurar ajustes](#)

Comprobación de seguridad

Comprobación de seguridad



Usuarios baneados está habilitado como es recomendable.



Copias de seguridad de bases de datos está habilitado como es recomendable.



Activar protección contra fuerza bruta está habilitado como es recomendable.



Protección contra fuerza bruta en la red está habilitado como es recomendable.



Refuerzo de la seguridad de la contraseña está habilitado como es recomendable.



Ajustes de WordPress está habilitado como es recomendable.

Ejecutar de nuevo Asegurar sitio

GRACIAS A

RAIN

tigo business
Una solución para cada negocio

 **BOLDGRID**

 **movistar**

 **KRONOSCODE**

 **JETPACK**

 **WooCommerce**

 **bluehost**

 **monchi.to**
DISEÑO & DESARROLLO WEB

 **MODERN TRIBE**

 **SiteGround**

 **dotcreek**

 **acedo**
profesionales - marketplace - servicios

 **TOPFLOOR**
MARKETING

 **DreamHost**

 **WPML.ORG**


 **SiteLock**



UCA
UNIVERSIDAD
CENTROAMERICANA

 **dinterweb**
Inbound Marketing Agency

SUCURI

 **Hotel Transión Teodolinda**

 **Bacanalnica.com**

