



WordCamp
Torrelodones
2023

Aspire... Espire...

Yoga



para recuperar
tu sitio y tu reputación
después de un hackeo.

Néstor Angulo de Ugarte

#WCTorre



Néstor Angulo de Ugarte

.....
**CISSP, Ingeniero Informático, emprendedor y
Tecnólogo Humanista**

< 2015 -> 4 empresas

2015 -> Sucuri.net

2017 -> GoDaddy WebSecurity

**2023 -> Nuevo comienzo:
nestorangulo.pro**

Twitter: @pharar



WordCamp
Torrelodones
2023



#WCTorre

- Dashboard
- All in One SEO
- Jetpack
- Unyson
- Blog Posts
- Media
- Pages
- Comments
- Forms
- FooGallery
- Portfolio
- Feedback
- Forms
- Appearance
- Plugins
- Users**
- All Users
- Add New

Users [Add New](#)

Welcome to the newest version of WP Smush! Auto-smushing on upload is lightning fast now that we handle all the smushing asynchronously. [Find out more here >>](#)

All (5) | Administrator (3) | Contributor (2)

 Search Users

Bulk Actions
 Change role to...
6 items

<input type="checkbox"/>	Username	Name	Email	Role	Posts
<input type="checkbox"/>	admin	[Redacted]	[Redacted]	Administrator	78
<input checked="" type="checkbox"/>	akmin		no@email.com	Administrator	1
<input type="checkbox"/>	janel	[Redacted]	[Redacted]	Contributor	0
<input type="checkbox"/>	levy	[Redacted]	[Redacted]	Contributor	33
<input checked="" type="checkbox"/>	managed-wp-migration-465790ae	Managed WordPress Migration User	noreply@secureserver.net	Administrator	0
<input checked="" type="checkbox"/>	wp.service.controller@hmgp			None	0

Aministradores falsos...

Bulk Actions
 Change role to...
6 items



Title

Hacked By **BALA SNIPER**

Hacked By **GeNErAL**

Content

<p>Hacked By BALA SNIPER

Kurdish Hacker Here

If you want Fix Problem Website … !

Contact Me via Gmail : darinsniper007@ gmail.com

Contact Me Via Facebook : https://www.facebook.com
/balasniper007 </p>

```
<title>~!Hacked By GeNErAL alias Mathis!~</title>
<h2>Hacked By GeNErAL</h2>&nbsp;</font></p><img
border='0' src='http://www.officialpsds.com/images/thumbs
/Baby-Devil-Toon-psd9848.png'><br><br><br><b>Greetz :
Kuroi'SH, RxR, ~ </b><br><br></FOOTER><b><code>
<h1>\! /Just for Fun ~Hacked By GeNErAL\! /</code>
<h1></h1><p align='center'><font color='red' /><font
size='5' color='#FF0000'>Hacked By
GeNErAL! !</font></font></p>
```

Tus post cambian...

Aparece una portada
"ligeramente" diferente...



HACKED By m4g!c_mUn5h!

[Cyb3R_Sw0rD Hacking Group Form Bangladesh]
[Security Doesn't Exit Our Dictionary....]
[Feel The Power Of Cyb3R_Sw0rD.....]
Sh00tz : B!4cK_C0D3R | Hax0r_Inject0r | R3D C0D3R | All Member Cyb3R_Sw0rD

We Are : —| B!4cK_C0D3R - Hax0r_Inject0r - m4g!c_mUn5h! - H3ART_B!33D - G!0w!Ng - F!R3 - H3X_KHAN - X!33TX_SN4P3R - C!YB3R_DARK - L33T_C0D3R - L33T_T0M0N - !NCRYPT0_HAX0R - T!G3R_TR4C3 - MR.CYB3R_K!ll3R |—

Hacked by El Moujahidin



#Free Syria
#Free Palestine

Tell Your Gov , To Know About Palestine
We Will Countinue Hacking The Sites , To Send The Message Of Our Palestine And All Arabs
We Dont Accept Killing Muslims Evry Where, Stop Killing US
#We Are El Moujahidin Team We Will Not End This War
#AttaCker fr0m #Algeria



FRASA

DESIGNS

[ABOUT](#) [OUR WORK](#) [SERVICES](#) [CONTACT](#)

FREE SHIPPING !!!
BUY VIAGRA
NOW

Name *

Phone *

E-Mail *

Message *

Phone: 562.381.2702
Address: 6831 Suva St Bell Gardens, CA 90201
Email: graphicdesign@frasadesigns.com

Venta de viagra y similares ...



Remote site: /public_html/wp-content/plugins

Filename ^	Filesize
..	
Login-wall-KiLxb	
Login-wall-NUJIF	
advanced-custom-fields	
all-in-one-wp-security-and-firewall	
alltimeusdflowingin	
contact-form-7	
disable-comments	
google-sitemap-generator	
joomjs	
js_composer	
page-links-to	
really-simple-captcha	
sucuri-scanner	
wordfence	
wordpress-seo	
wp-pagenavi-master	
hello.php	24313
index.php	28

Remote site: /public_html/wp-content/plugins/joomjs

Filename	Filesize
..	
_inc	
views	
index8632.php	
joomjs.php.suspected	
index.php	
akismet.php	
class.akismet-widget.php	
error_log	
readme.txt	
wrapper.php	
class.akismet-admin.php	3
class.akismet.php	3




Account Suspended

This Account has been suspended.

Contact your hosting provider for more information.

Security error

Google



The site ahead contains harmful programs

Attackers on [redacted] might attempt to trick you into installing programs that harm your browsing experience (for example, by changing your homepage or showing extra ads on sites you visit).

Automatically report details of possible security incidents to Google. [Privacy policy](#)

[Details](#) [Back to safety](#)



site:anotherinfectedsite.dom cheap



All

Images

Shopping

Videos

Maps

More ▾

Search tools

About 91,300 results (0.31 seconds)

[Cheap Nike Shox Boys 6.5 23 Air Jordan Comforters ...](#)

[anotherinfectedsite.dom/page/lvUxxp1D](#) ▾

cheap nike shox boys 6.5. Shop our premium selection of boys nike shox turbo online now for great prices. Boys' toddler nike air max 90 premium running shoes.

[Air Yeezy Shoes Cheap Real Air Yeezy Shoes - Natural ...](#)

[anotherinfectedsite.dom/page/lpNxxxx58vuK](#) ▾

Results great but cheap air yeezy shoe,cheap shoes,men's casual shoes,women's casual shoes,men's flats,as well as cheap and more online get.Size 6 nike air ...

[Cheap Jordan Sneakers Wholesale Cheap Jordan Website ...](#)

[anotherinfectedsite.dom/page/lv1CxxxxlQVH](#) ▾

Cheap jordan sneakers wholesale we cheap jordan sneakers wholesale are a cheap jordan website large wholesaler cheap wholesale nike dunks and retailer ...

[Example Domain](#)

[www.example.com/](#) ▾

This site may be hacked.

Example Domain. This domain is established to be used for illustrative examples in documents. You may use this domain in examples without prior coordination or asking for permission. More information...

Not eligible

Ad disapproved due to:

 Malicious or unwanted software

- [Read the policy](#)

[Appeal](#)

[Edit ad](#)



Ad stat



Ad

Campaign

Ad group

Status

[Your Website Ad | Advertising for Revenue](#)
[example.com](#)

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna.

[Example Campaign](#)

[Example Ad Group](#)

Disapproved
Malicious or unwanted software



Google Membership Rewards



Congratulations

January 26 at 12:03am

Every Tuesday we select 10 lucky Apple users from our sponsors. This free gift is **exclusively** for loyal Apple users. It's our way of saying thank you for your continuous support for our product and services.

You have been selected to win a gift from [redacted] worth up to \$749 if you answer the next 4 questions correctly.

ACT NOW! 9 other Apple users have received this invitation with only 5 prizes to win.

You have **1 minutes 30 seconds** to answer the questions before someone else takes over your spot. Good luck!

The page at promotion.com-rewards.club says: x

Congratulations iPad user!

You are selected by Google to be among the first few persons to win an iPhone 6s or other Google prizes! This free gift is exclusively only for loyal Apple users in Canada.

Please confirm that you are the owner of this iPad phone by clicking OK.

OK

Google Gift!

[redacted] (d!) from [redacted]
This is just our way to thank you for your

Question 1 of 4: Who founded Google?

Bill Gates

Mark Zuckerberg

Larry Page

newsfile.club wants to

Show notifications

Block Allow





CONCLUSIÓN

- E-commerce con uso normal:
 - **Beneficios:** 50.000€ - 100.000€
- Hackeado
 - **Pérdidas:** - (270.000€ - 300.000€)
- **Coste de medidas de seguridad** -> 500€ - 1.000€



BOTNET

SPAM

PHISHING

HACKER

MALWARE

DDOS

VIRUS

KEYLOGGER

SPYWARE



La Policía en tu casa....

Hacked By JakRa

kan, berani mati | indonesian,

Tidak ada seorangpun, hewan atau banci yang disakiti dalam hacking ini
Jiwa Kegelapan Team





OHMMMMMM





Si, lo sé ...



¡GRITEMOS!



Es aceptable sentirse hecho polvo...



Pero después de todo esto ...



¡ACTUEMOS!



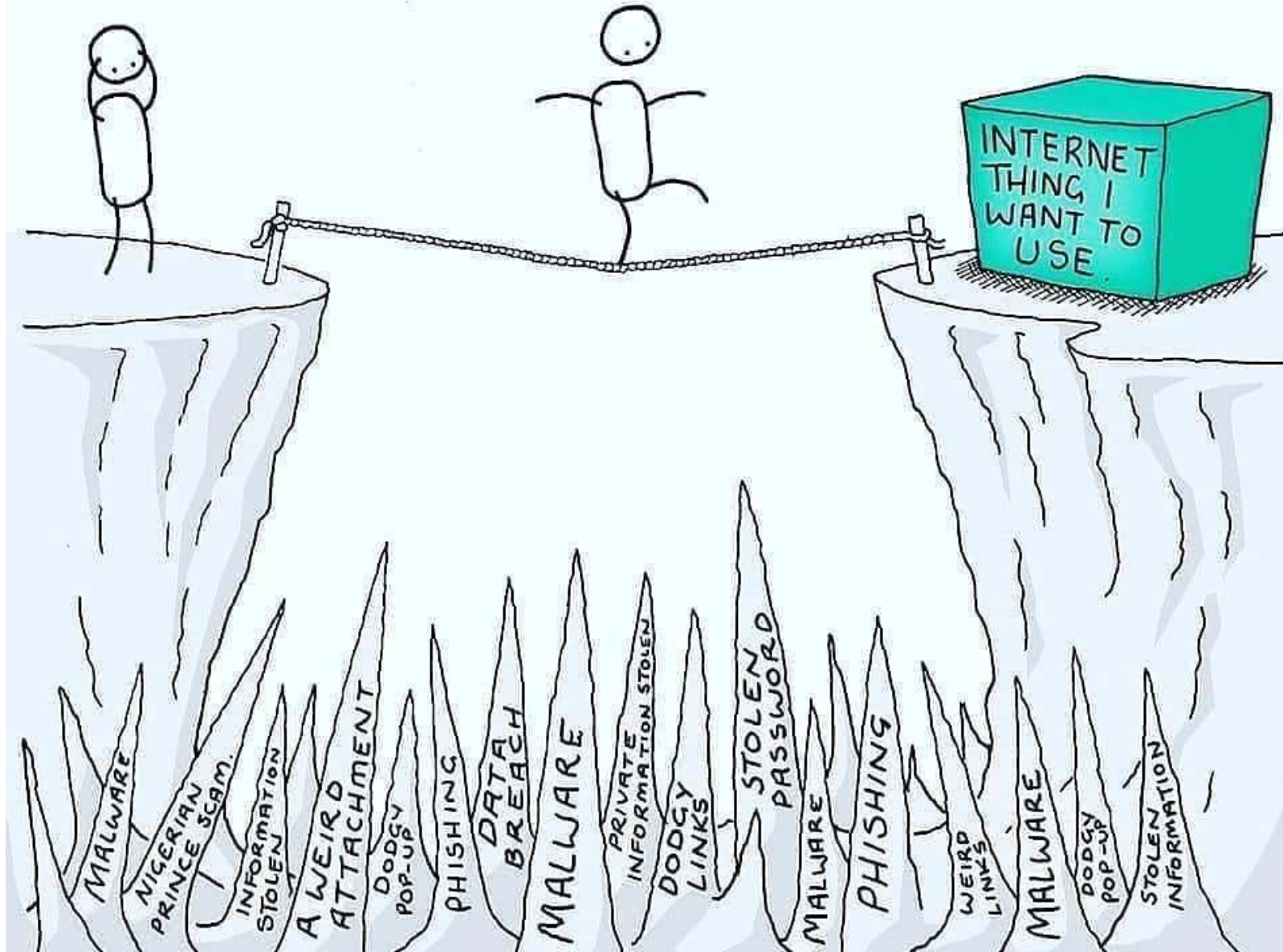
Primero... **Conceptos**

There are two types of companies: those who have been hacked, and those who don't yet know they have been hacked.

John Chambers
Chief Executive Officer of Cisco



DEALING WITH CYBER STRESS





PHISHING

BOTNET

SPAM

HACKER

MALWARE

DDOS

VIRUS

KEYLOGGER

SPYWARE

Hackers vs Ciberterrorista



Hacker

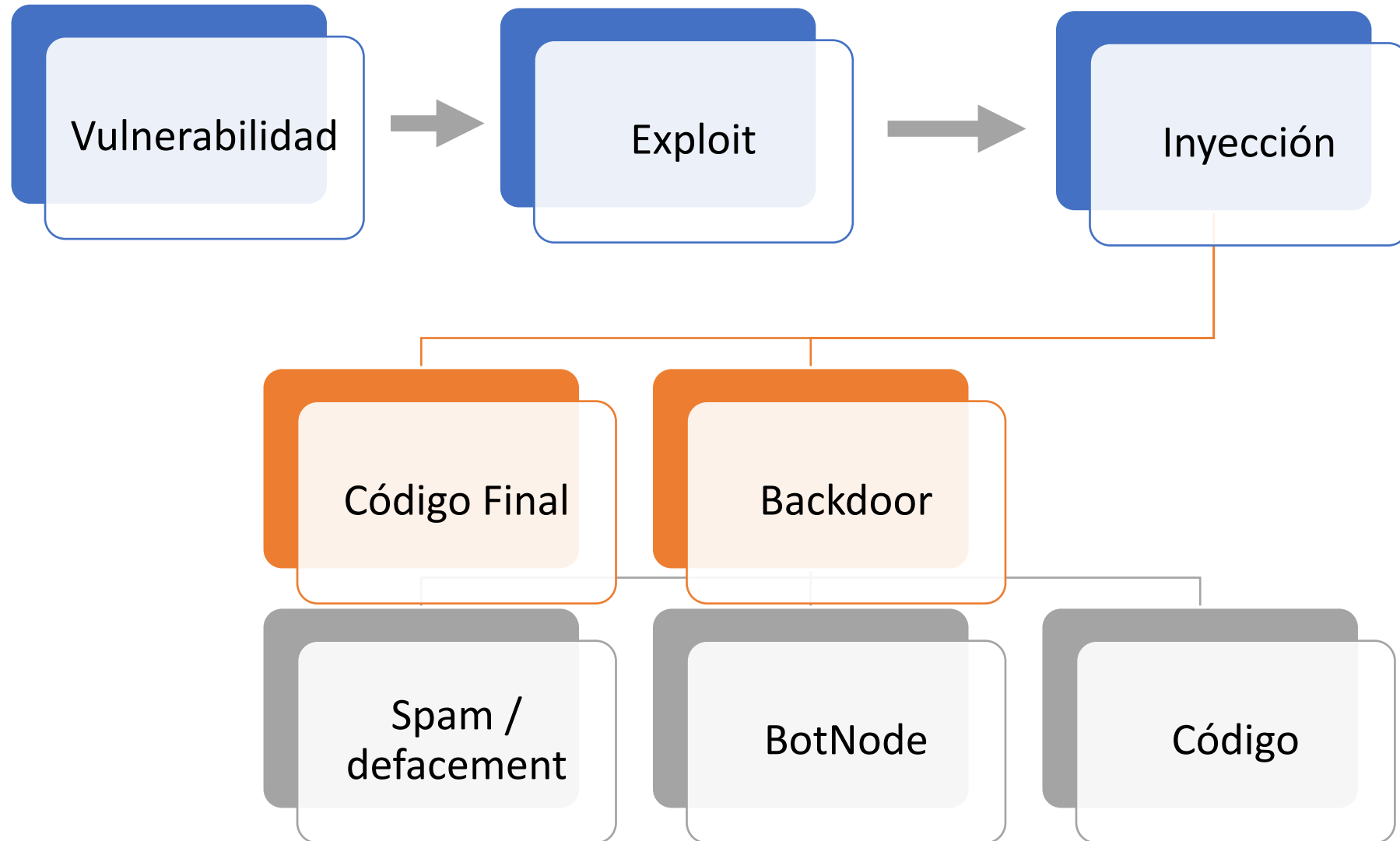
- **Persona curiosa** que disfruta yendo más allá de los límites y convenciones.



Ciberterrorista

- **Hacker informático**, cuyo objetivo es enriquecerse.
- **El malo.**

Cómo se infecta un sitio WordPress:



Hechos

Un hackeo **casi nunca**
está orientado a un
cliente
(98% of cases)

Casi siempre se debe
a **mal mantenimiento**
o **mal control.**

Un certificado SSL
no es un
escudo anti- hacking

Los parches de
seguridad aparecen
después de identificar
los exploits

Errare Humanum Est
(El Ser Humano falla)

La seguridad no es
100% efectiva
(**Y NUNCA lo será**)

Agentes (si algo sale mal)

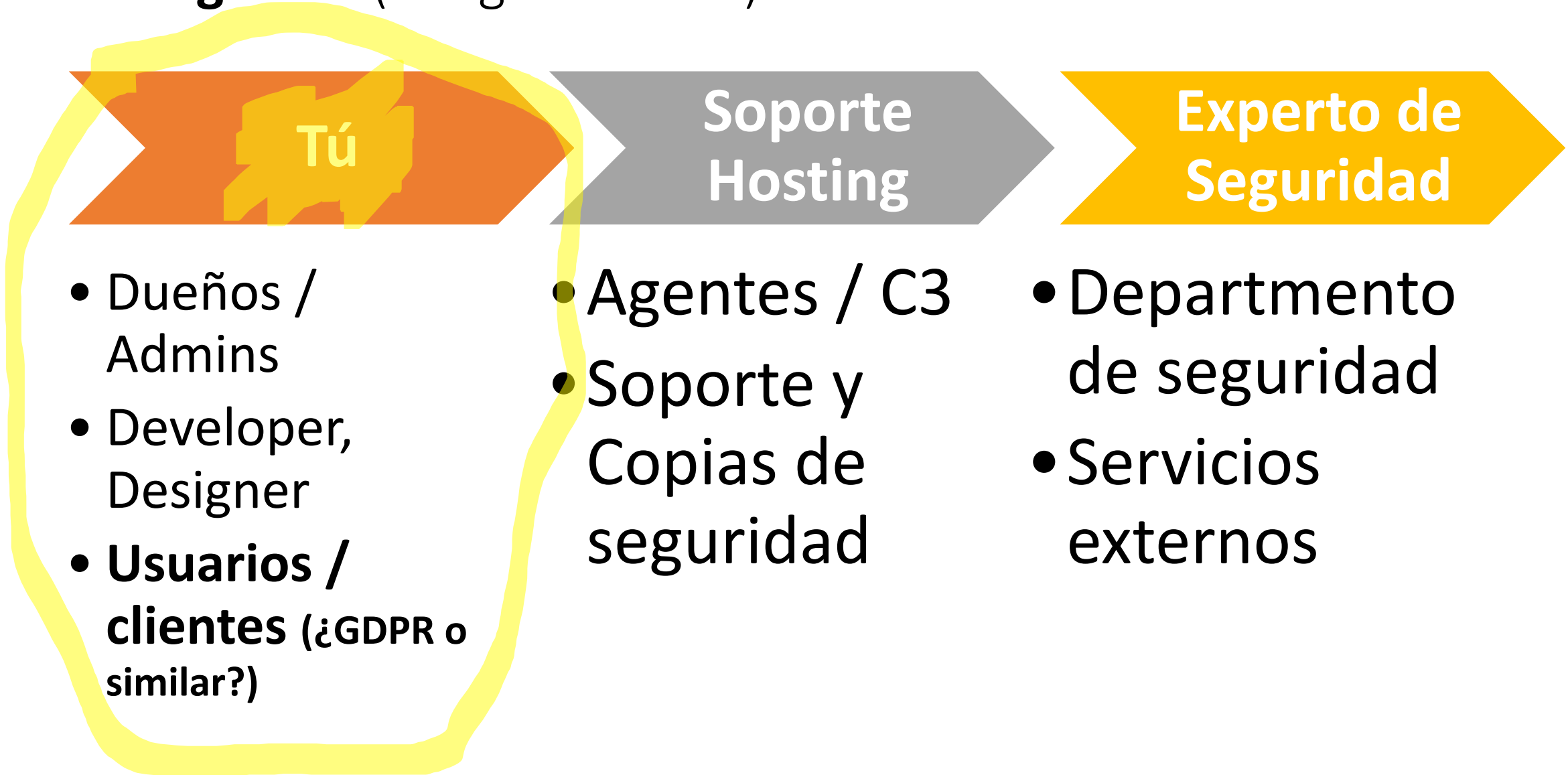


- Dueños / Admins
- Developer, Designer
- **Usuarios / clientes** (¿GDPR o similar?)

- Agentes / C3
- Soporte y Copias de seguridad

- Departamento de seguridad
- Servicios externos

Agentes (si algo sale mal)



Medidas:



REACTIVAS

Cuando las cosas malas **ya han pasado**

Mitigación de **Daños**

INCIDENT RESPONSE



PROACTIVAS

Antes de que pase nada malo

Mitigación de **Riesgo**

ANÁLISIS Y MONITOREO



Segundo, la RESPUESTA A
INCIDENTES

Incident response (IR) is the effort to quickly identify an attack, minimize its effects, contain damage, and remediate the cause to reduce the risk of future incidents.

(vmware.com)

Medidas reactivas (AKA Incident Response)



1) ESCANEA tu sitio

Front-end: sitecheck.sucuri.net

Escáner gratis en plugin: WordFence, etc.



2) ACTUALIZA

TODO

Incluyendo el software del servidor.



3) CRC: Check, Remove and Change

Admins, plugins, temas, contraseñas ...

- webpagetest.org



0 restaurar **BACKUP Y Volver a 1)**

Posible pérdida de información

Posible re-instalación de malware

(PRIMERO)
ESCANEA
tu sitio

Intentemos primero entender que ha pasado.

FrontEnd análisis:
sitecheck.sucuri.net

Usar escáner gratuito
(i.e. WordFence)

Si tienes acceso al server,
ejecuta un antivirus (i.e. Clam AV)



Warning: Malware Detected

Infected with malware. Immediate action is required

[Request Cleanup](#)



58

URLs Scanned

Pages scanned: 37

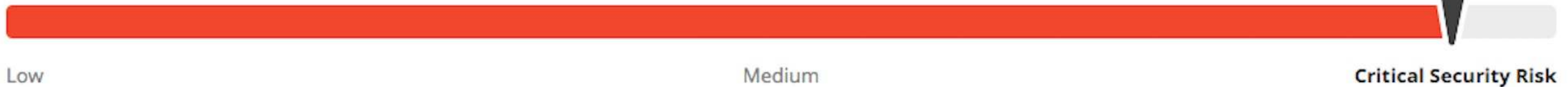
Javascript files scanned: 21

Other files: 0

System running on: LiteSpeed, Powered by: PHP/5.4.45

IP address:

[More Details](#)



Low

Medium

Critical Security Risk

Malware Found

[http://www.\[redacted\]/wp-includes/js/jquery/jquery.js?ver=1.12.4](http://www.[redacted]/wp-includes/js/jquery/jquery.js?ver=1.12.4) [\(More details\)](#)

Definition

[rogueads.unwanted_ads?9.5](#)

Malware Found

[http://www.\[redacted\]/wp-includes/js/jquery/jquery-migrate.min.js?ver=1.4.1](http://www.[redacted]/wp-includes/js/jquery/jquery-migrate.min.js?ver=1.4.1) [\(More details\)](#)

Definition

[rogueads.unwanted_ads?9.5](#)

(SEGUNDO) **ACTUALIZA**

Actualiza todo, incluidos plugins, temas y el propio WordPress.

Esto hará que tapemos agujeros de seguridad, evitando una posible infección.

También, **sobreescribirá código comprometido/corrupto con código confiable** del repositorio oficial.

ACTUALIZA

PLUGINS

TEMAS

CORE

PHP

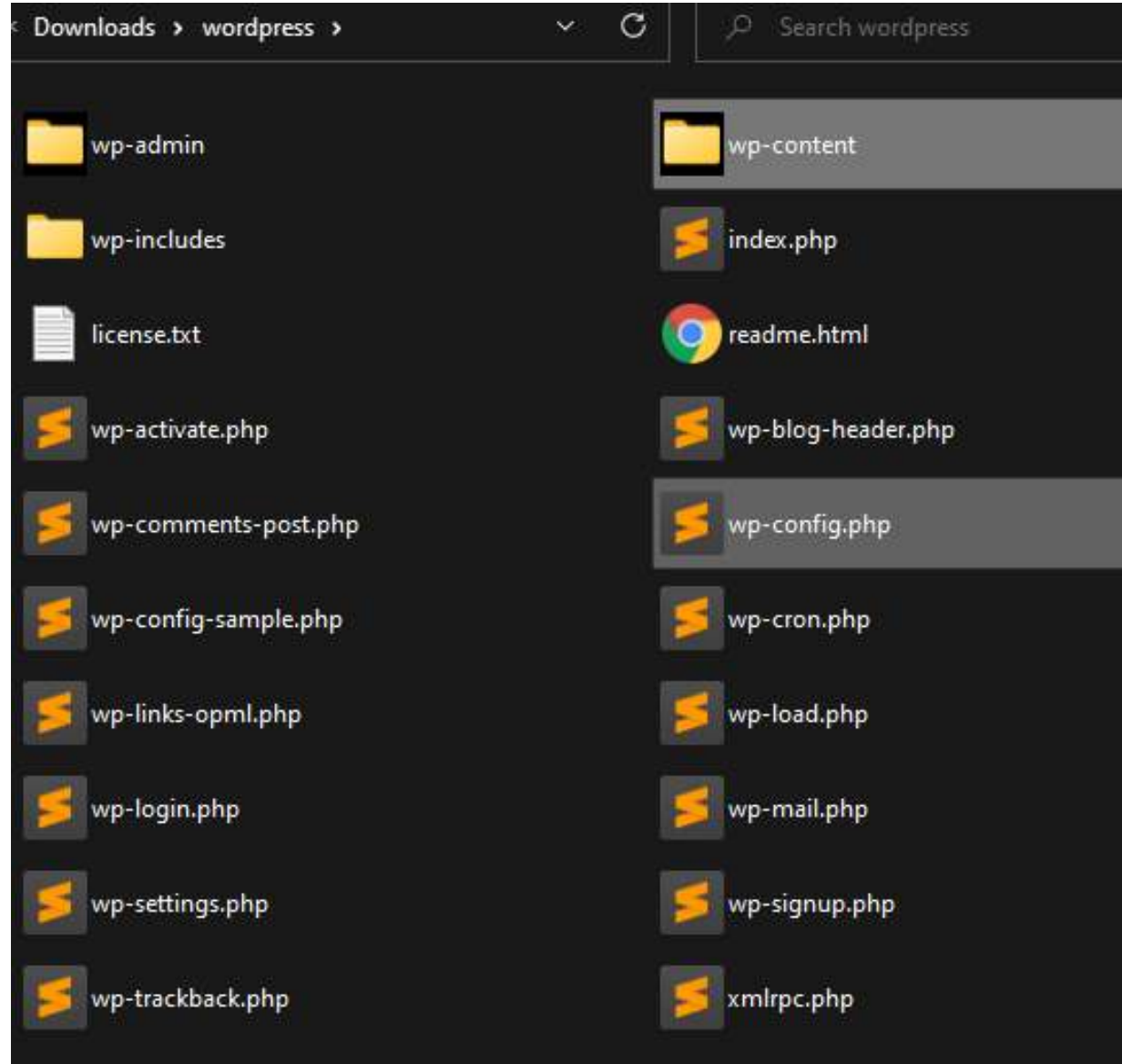
APACHE /
NGINX

SERVIDOR

CPANEL /
PLESK

...

iSECRETO!



(TERCERO) **CRC:** Check, remove and change

Check & Remove

- Admins innecesarios
- Plugins y temas que no sean estrictamente necesarios
- Copias de seguridad
- Sitios de test/en desarrollo en el servidor de producción.

Change Contraseñas

- Conexiones (cPanel, FTP, SSH, ...)
- Base de datos (recuerda actualizar luego el **wp-config.php**)
- Panel admin (**wp-admin**)
- Acceso al proveedor de hosting.

Atención: Se perderá cualquier personalización que hayas hecho a los archivos del

Actualizar temas

Seleccionar todos

 **Twenty Fifteen**
Tienes la versión 2.5. Actualiza a la 2.6.

 **Twenty Fourteen**
Tienes la versión 2.7. Actualiza a la 2.8.

 **Twenty Nineteen**
Tienes la versión 1.4. Actualiza a la 1.5.

 **Twenty Seventeen**
Tienes la versión 2.2. Actualiza a la 2.3.

 **Twenty Thirteen**
Tienes la versión 2.9. Actualiza a la 3.0.

 **Twenty Twenty**
Tienes la versión 1.1. Actualiza a la 1.2.

Seleccionar todos







Actualizar temas

Users [Add New](#)

Welcome to the newest version of WP Smush! Auto-smushing on upload is lightning fast now that we handle all the smushing asynchronously. f

All (5) | Administrator (3) | Contributor (2)

Bulk Actions Change role to...

<input type="checkbox"/>	Username	Name	Email	Role
<input type="checkbox"/>	 admin	[Redacted]	[Redacted]	Administrator
<input checked="" type="checkbox"/>	 akmin	[Redacted]	no@email.com	Administrator
<input type="checkbox"/>	 janel	[Redacted]	[Redacted]	Contributor
<input type="checkbox"/>	 levy	[Redacted]	[Redacted]	Contributor
<input checked="" type="checkbox"/>	 managed-wp-migration-465790ae	Managed WordPress Migration User	noreply@secureserver.net	Administrator
<input checked="" type="checkbox"/>	 wp.service.controller.lHmp6	[Redacted]	[Redacted]	None

Username Name Email Role

Bulk Actions Change role to...

(ÚLTIMA OPCIÓN) Restaurar una Copia de Seguridad

- Puedes perder información
- No sabemos a ciencia cierta cuándo comenzó la infección



COPIAS DE SEGURIDAD



Ten una buena
estrategia



Nunca las almacenes
en tu servidor de
producción



Una copia **FUNCIONAL**
puede ser **tu mejor**
amiga un mal día

¡RECUERDA! Medidas reactivas



1) ESCANEA tu sitio

Front-end: sitecheck.sucuri.net

Escáner gratis en plugin: WordFence, etc.



2) ACTUALIZA

TODO

Incluyendo el software del servidor.



3) CRC: Check, Remove and Change

Admins, plugins, temas, contraseñas ...

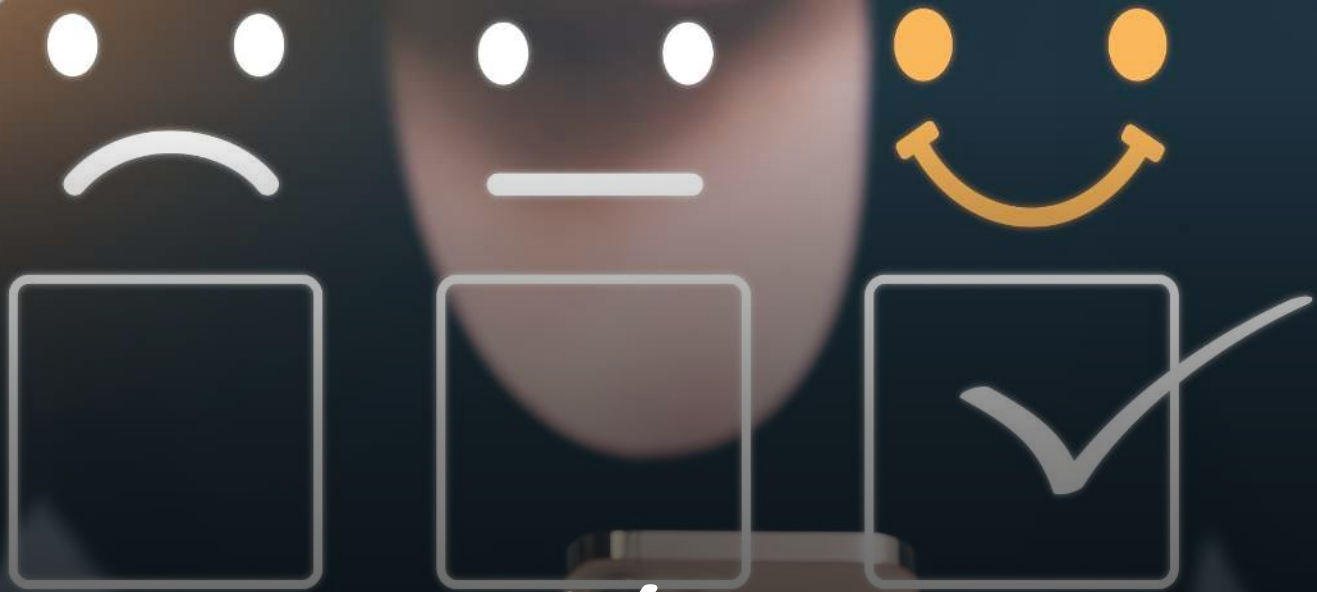
- webpagetest.org



o restaurar **BACKUP Y Volver a 1)**

Posible pérdida de información

Posible re-instalación de malware



Ahora, la Reputación



Bots, Motores de Búsqueda y Blocklists



INTERNET ESTÁ
CONSTANTEMENTE
RASTREADO POR
BOTS



LOS MOTORES DE
BÚSQUEDA Y
EMPRESAS DE
SEGURIDAD
TIENEN
BLOCKLISTS



**BLOCKLISTS ->
REPUTACIÓN**



MIENTRAS MÁS
FAMOSA SEA LA
BLOCKLIST MÁS
ACEPTADA.

Algunos hechos

No es un proceso inmediato

- La inclusion en blocklists toma su tiempo
- Salir también

Normalmente, no dan información de por qué

Las RRSS tienen en cuenta las blocklists

Las empresas de Ads bloquean campañas

Los motores de búsqueda eliminant el sitio de las SERP

- Algunos eliminan completamente to ranqueo de SEO

Un cosa (importante) más ...

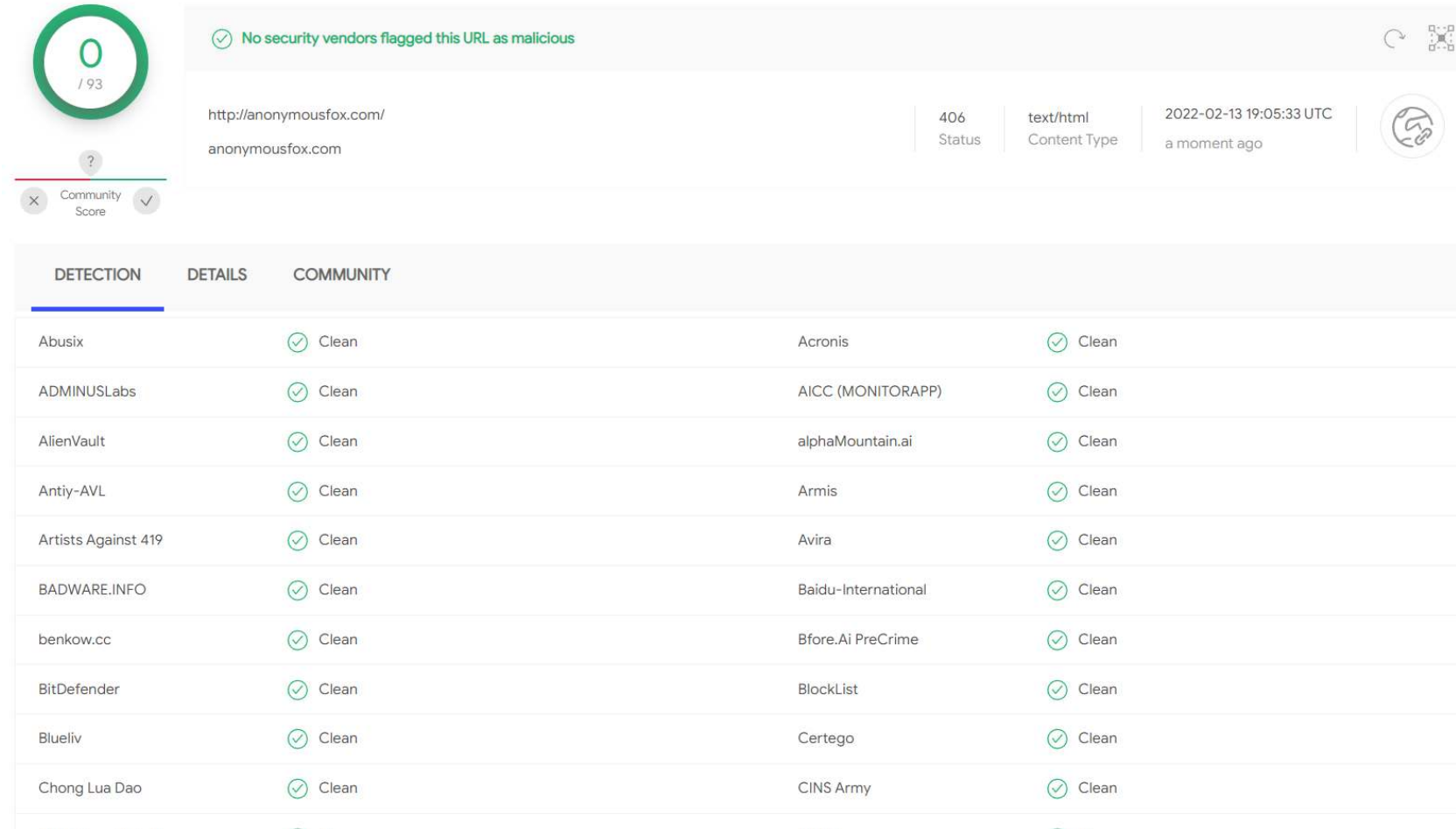
Algunas **leyes de protección de datos** pueden requerir que se reporte cualquier brecha de seguridad con pérdida de datos sensibles a las autoridades competentes

En el caso de que que **afecte a un ciudadano Europeo**, la **GDPR** da **72h** tras la detección de la brecha para notificarla.

Comprueba las leyes aplicables, depende de país en el que operes y la nacionalidad de los clients.

Solución a las blocklists

1. **UNA VEZ LIMPIA,** comprueba las blocklists:
Virustotal.com
2. **Procede a solicitar** una reconsideración por cada empresa en las blocklists, individualmente.



0 / 93

✓ No security vendors flagged this URL as malicious

http://anonymousfox.com/
anonymousfox.com

406 Status | text/html Content Type | 2022-02-13 19:05:33 UTC a moment ago

Community Score

DETECTION	DETAILS	COMMUNITY
Abusix	✓ Clean	Acronis ✓ Clean
ADMINUSLabs	✓ Clean	AICC (MONITORAPP) ✓ Clean
AlienVault	✓ Clean	alphaMountain.ai ✓ Clean
Antiy-AVL	✓ Clean	Armis ✓ Clean
Artists Against 419	✓ Clean	Avira ✓ Clean
BADWARE.INFO	✓ Clean	Baidu-International ✓ Clean
benkow.cc	✓ Clean	Bfore.Ai PreCrime ✓ Clean
BitDefender	✓ Clean	BlockList ✓ Clean
Blueliv	✓ Clean	Certego ✓ Clean
Chong Lua Dao	✓ Clean	CINS Army ✓ Clean



Informe Post-Mortem

Es **duro**, requiere servicios **forenses** y **expone** tu gestión.

Un informe claro de lo que pasó tras el ataque exitoso:

- Cómo y cuándo ocurrió
- Cómo y cuándo fue descubierto
- Qué se hizo para mitigar el daño y recuperar la situación normal
- Lecciones aprendidas

Ayuda a **aprender** para futuras situaciones

Ayuda a recuperar la **confianza de los usuarios**

Muestra tu compañía alineada con los conceptos de **transparencia**.

A woman with dark hair is shown in profile, wearing large black headphones and meditating with her eyes closed and hands clasped over her heart. She is sitting at a desk with a laptop open in front of her. To the left of the laptop is a stack of books and a large green succulent plant. To the right is a smaller green plant in a white pot. The background features a window with orange and white patterned curtains. The overall scene is calm and focused on mental well-being.

Y para finalizar...
¡Paz Mental!

Medidas Proactivas



Permisos y temas (LEAST PRIVILEGE RULE)



Contraseñas, cambiar periódicamente, 2FA + Fuertes



Parches (¡VALIDARLAS!)



Parches vienen DESPUÉS de los EXPLOITS)



Alertas (e.g. N.com, PatchStack & Integridad de Ficheros)



WAF (Web Application Firewall)



¡Recuerden! **INVERTIR** en:



HOSTING



SEGURIDAD

A black and white photograph showing the back of a person wearing a dark t-shirt. The t-shirt has the text "Everybody needs a hacker" printed on it in a white, sans-serif font. The person's hair is visible at the top of the frame, and the background is blurred, suggesting an outdoor setting with some light sources.

Everybody needs a hacker



Ponente

¡GRACIAS!

.....



WordCamp
Torrelodones
2023



#WCTorre



WordCamp Torrelodones 2023

#WCTorre