

El coste de un Hackeo



Néstor Angulo de Ugarte



**WORDCAMP
GRIÑÓN**

Néstor Angulo de Ugarte

Ingeniero informático por la ULPGC

Analista de Seguridad

@ GoDaddy WebSecurity

@ Sucuri.net

CISSP (ISC2.org - 2022)

Twitter: @pharar

#WCGriñón



DISCLAIMER

- NO soy abogado
- NO vengo a publicitar a ninguna empresa en esta charla.
- Soy responsable de lo que digo, no de lo que interpretes.





WORDCAMP
GRINÓN



HACKED By m4g!c_mUn5h!

[Cyb3R_Sw0rd Hacking Group Form Bangladesh]

[Security Doesn't Exit Our Dictionary....]

[Feel The Power Of Cyb3R_Sw0rd.....]

Sh00tz : Bl4ck_C0D3R | Haxor_Injector | R3D C0D3R | ALL Member Cyb3R_Sw0rd



WORDCAMP
GRINÓN







Users [Add New](#)

Screen Options ▾

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)

Bulk Actions ▾ Apply Change role to... ▾ Change

<input type="checkbox"/>	Username	Name	Email	Role	Posts
<input type="checkbox"/>	 admin	[Redacted]	[Redacted]	Administrator	78
<input checked="" type="checkbox"/>	 akmin	[Redacted]	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.lHmp6			None	



<input type="checkbox"/>	Username	Name	Email	Role	Posts
--------------------------	----------	------	-------	------	-------



DESIGNS
FREE SHIPPING !!!
BUY VIAGRA
NOW

Name *

Phone:

Phone *

Address:

E-Mail *

Email:



Message *

SEND LETTER



WORDCAMP
GRINÓN

ctions ▾

[e here >>](#)

Sea

Posts

78

1

0

33

0

Posts



Current Revision by
3 months ago (4 Mar @ 09:03)

[Restore This Revision](#)

Title

Hacked By **BALA SNIPER**

Hacked By **GeNERAL**

Content

```
<p>Hacked By BALA SNIPER<br />
```

```
Kurdish Hacker Here<br />
```

```
If you want Fix Problem Website &#8230; !<br />
```

```
Contact Me via Gmail : darinsniper007@ gmail.com<br />
```

```
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></b><p align='center'><font color='red' /><font  
face='Superdie' size='5' color='#FF0000'>~! Hacked By  
GeNERAL! !</font></font></p>
```



**WORDCAMP
GRINÓN**

Previous

Next



Title

Has

Con

<p>

Ku

If

Co

Co


/ba

ns

u

Security error x

Google



The site ahead contains harmful programs

Attackers on _____ 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](#)

is Revision

/thumbs

Z :

nt



WORDCAMP
GRINÓN

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/lvUxxxp1D](#)

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/lpNxxxxx58vuK](#)

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/lv1CxxxxxlQVH](#)

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

Cheap Jordan Flight 45 - Natural Medicine Journal

[anotherinfectedsite.dom/page/lRxxxxxyvn5](#)

Cheap jordan flight shop jordan flight shoes at foot locker.All of the popular jordan flight high max release date jordan flight shoe models like cheap jordan flight ...

Paypal Cheap Air Jordans 13 Cheap Custom Air Jordans ...

[anotherinfectedsite.dom/page/lvxxxxRNH](#)

Cheap authentic retro jordans with paypal.Cheap buy wholesale air jordan retro xiii he got game.Need new jordans for valentines 2014 new laces.Og 2014 nike ...





site:anotherinf

Remote site: /home/in/html



Filename

All

- ..
- wp-includes-srcbak
- wp-admin-srcbak
- wp-content
- yyociwe
- c01fce
- docs
- zkwjuce
- wp-includes
- wp-admin
- .sucuriquarantine
- DISABLED
- info.php
- .user.ini
- .htaccess
- gd-config.php
- robots.txt
- license.txt
- zkwjuce.zip
- 69089f65dd9.php.suspected
- 11380aa99fe.php.suspected
- history-template.php.suspected
- wp-config.php
- 7513c638c52.php.suspected
- index.php
- wp-blog-header.php

Search tools

About 91,311

Cheap Nike

anotherinf

cheap nike

now for gre

Air Yeez

anotherinf

Results gre

casual sho

Cheap J

anotherinf

Cheap jor

jordan web

Cheap J

anotherinf

Cheap jor

high max r

Paypal C

anotherinf

Cheap aut

got game.N



WORDCAMP
GRINÓN



Congratulations

January 26 at 12:03am

Every Tuesday we select 10 lucky Apple users as our sponsors. This free gift is **exclusively** for our loyal Apple users. This is just our way to 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!

Question 1 of 4: Who founded Google?

Bill Gates

Mark Zuckerberg

Larry Page



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

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





This site can't be reached

nogluten.com's server IP address could not be found.

DNS_PROBE_FINISHED_NXDOMAIN

Reload



YOU'VE BEEN HACKED!

A person wearing a dark hoodie is sitting at a desk, looking down at a laptop. The background is dark with various cybersecurity terms and icons in a light green, distressed font. The terms include PHISHING, BOTNET, SPAM, HACKER, MALWARE, DDOS, VIRUS, KEYLOGGER, and SPYWARE. There are also icons for a magnifying glass, a speech bubble, a Wi-Fi signal, a padlock, a bomb, and gears. The text 'PERO, PERO, PERO ¿¿Qué ha pasado??' is centered over the person's face.

PERO, PERO, PERO
¿¿Qué ha pasado??

AKA
CONCEPTOS

¿Hackers?

Persona **curiosa** que va más allá de límites y convencionalismos

AKA Hacker

#WCGriñón





#WCGrinon



WORDCAMP
GRINÓN



#WCGriñón



WORDGAME
GRINÓN

- Thales de Mileto.
- Leonardo da Vinci.
- Thomas Edison.
- Arquímedes.
- Benjamin Franklin.
- Louis Pasteur y Alexander Fleming.
- Hermanos Montgolfier y Clément Ader.
- Nikola Tesla.

Eureka!



¿Entonces a qué le llamamos Hacker?



Hacker informático
cuyo objetivo es
enriquecerse o ganar
fama.

AKA Ciberterrorista



MR.

ROBOT

USA

#WCGriñón



WORDCAMP
GRIÑÓN



El Malo

**Black hat hacker,
terrorista, ladrón,
ciberdelicuenta...**

El Feo

**Un Bueno usando
métodos de Malo**

El Bueno

**Analista de
seguridad,
hacker ético...**



El **Black hat** **terrorista, Aaron, mefodos de Malo** **seguridad,**
ciberdelicuyente... **hacker ético...**



El M
Black hat
terrorista, ladrón, métodos de Malo
ciberdelicuenta...

#WCGriñón

eno
ta de
seguridad,
hacker





**¡Los Analistas
de Seguridad, son
los que hackean
bonito!**

#WCGriñón

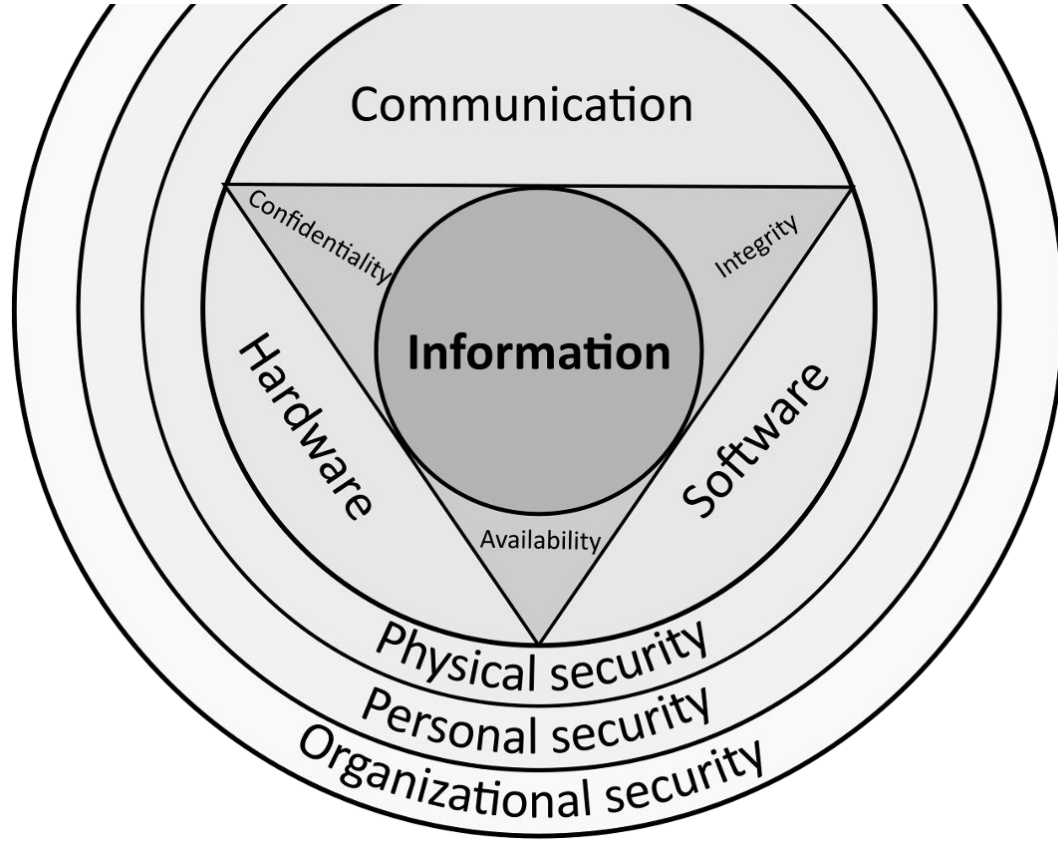


¿Qué es CIBERSEGURIDAD?

#WCGriñón

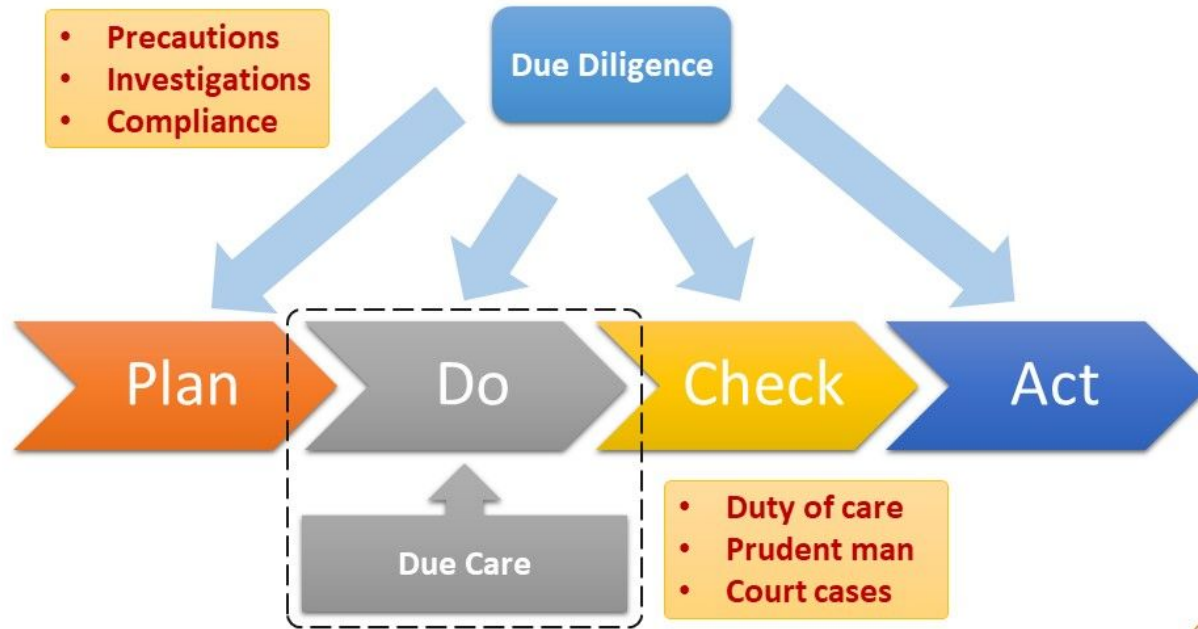


¿Qué es InfoSec?

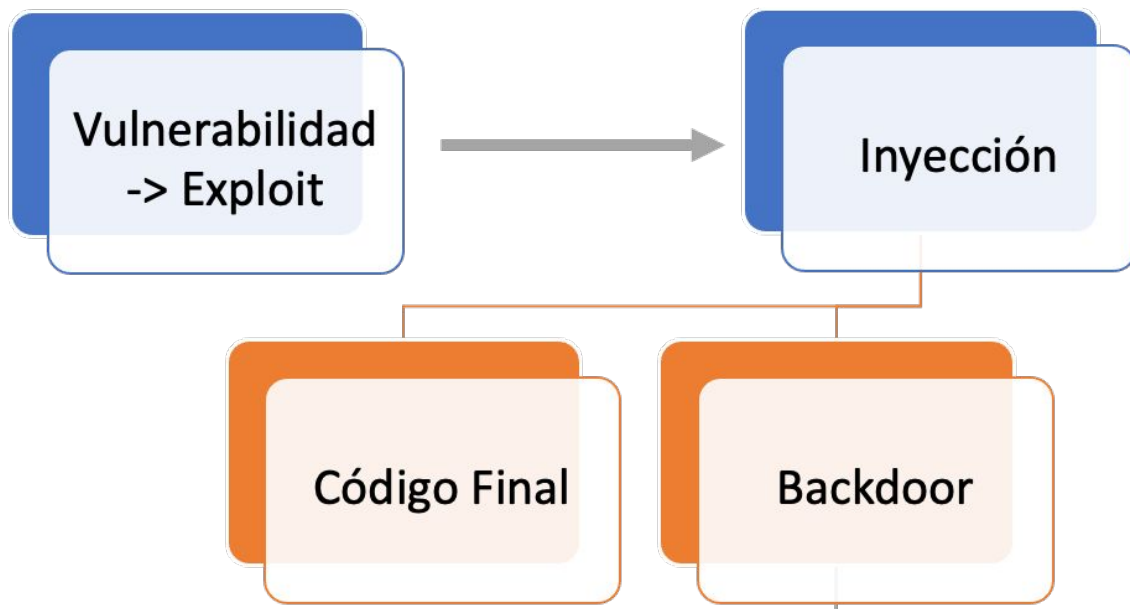


Ser diligente y tomar acciones

Due Diligence and Due Care



Cómo se hackea un WordPress



A 3D perspective illustration of a maze. In the center, the word "DATA" is rendered in white, blocky, uppercase letters. Below it, the word "BREACH" is rendered in red, blocky, uppercase letters. A red crown is positioned above the "A" in "DATA", appearing to be broken or falling apart, with several white, angular fragments floating around it. The maze walls are white and recede into the distance, creating a sense of depth.

DATA
BREACH

#WCGriñón



¿Qué ES una brecha de datos?

GDPR: “todas aquellas **violaciones de la seguridad** que ocasionen la **destrucción, pérdida o alteración** accidental o ilícita de **datos personales** transmitidos, conservados o tratados de otra forma, o **la comunicación o acceso no autorizados** a dichos datos”.

¿Qué NO ES una brecha de datos?

Un **incidente de seguridad que no ha afectado a datos personales o tratamientos de datos personales** no es una brecha de datos personales, dado que **no podría producir daños sobre los derechos y libertades de las personas físicas** cuyos datos son objeto del tratamiento, independientemente de otros perjuicios que pueda producir al responsable o encargado del tratamiento.

¿Qué significa daños o perjuicios?

Consecuencias para los afectados

Imposibilidad de ejercer algún derecho o acceso a un servicio

Usurpación de la identidad

Víctima de campañas de phishing/spamming

Pérdidas financieras

Daños reputacionales

Pérdida de confidencialidad de datos afectados por secreto profesional

Daños psicológicos o físicos

Pérdida de control sobre sus datos personales

Perfiles de personas físicas

Perfiles de las personas físicas afectadas
Clientes / ciudadanos
Estudiantes / alumnos
Usuarios
Pacientes
Suscriptores / potenciales clientes
Afiliados / asociados
Fuerzas y Cuerpos de Seguridad del Estado
Empleados
Otros

¿Qué se consideran datos sensibles?



#WCGriñón

Categorías de datos	Significado
Datos básicos	Nombre, apellidos o la fecha de nacimiento de los afectados
Datos de contacto	Número de teléfono, email o dirección física de las personas
Imágenes (foto/video)	Imágenes individuales o colectivas de las personas afectada
Documento identificativo	NIF, NIE, pasaporte, número de Seguridad Social o cualquier otro identificador a nivel nacional o extra nacional
Datos económicos o financieros	Datos referidos a nóminas, extractos bancarios, estudios económicos o cualquier otra información que pueda revelar información económica de los afectados
Datos de localización (datos de ubicación de la persona en un determinado momento o durante un periodo de tiempo)	Datos de posicionamiento, coordenadas o direcciones habituales (no residencia) de los afectados
Medios de pago (números de tarjeta o cuenta bancaria)	Información de los afectados referido a métodos de pago como números de tarjeta, cuentas bancarias, métodos de pago online como Paypal, bitcoins, etc.
Credenciales de acceso o identificación	Nombres de usuarios, contraseñas ya estén en claro, hasheadas o cifradas y datos como tarjetas de coordenadas o segundos factores de autenticación
Datos de perfiles	Perfiles de usuarios en redes o datos de perfilado psicosocial o que permitan realizar perfilados de personas físicas
Sobre la vida sexual	Datos relativos a la salud sexual, hábitos, orientación o tendencias sexuales, así como información que permita inferirlo.

¿Qué se consideran datos sensibles?

Religión o creencias	Religión que profesan los afectados, así como información sobre posturas religiosas, agnósticas o ateas
Origen racial o étnico	Información que refleje o permitan establecer el origen racial o la pertenencia a una determinada etnia de las personas
Datos de salud de empleados	Información sobre la salud que un responsable trate sobre sus empleados o personas con las que mantiene una relación laboral, como puedan ser partes de baja o informes sanitarios
Datos de salud de pacientes	Referido a la información que los responsables del sector sanitario dispongan de las personas
Opinión política	Información que refleje o permita averiguar la opinión o tendencias políticas de las personas
Datos genéticos	Características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica
Datos sobre condenas e infracciones penales	Certificados de antecedentes penales o los certificados de delitos de naturaleza sexual
Datos biométricos	Características físicas, fisiológicas o conductuales de una persona física, que permita su identificación
Datos sobre afiliación sindical	Informan sobre la pertenencia o afiliación de una persona a un sindicato

OBLIGADO si hay una Brecha de Datos

- **Comunicar** a la autoridad competente (España/Europa es la AEPD) en **menos de 72h** desde que se tiene constancia de la brecha.
- Hacer una **valoración de riesgo** para las personas afectadas **y de alcance** de la brecha.

Probabilidad	Muy alta	Obligación			
	Alta				
	Baja	Afectados			
	Improbable ³⁴				
Comunicar afectados		Comunicar afectados			
Baja - Muy limitada		Media - Limitado	Alta - Significativo	Muy alta - Muy significativo	
Severidad (Gravedad del impacto)					





EJEMPLO 1

Blog + Newsletter

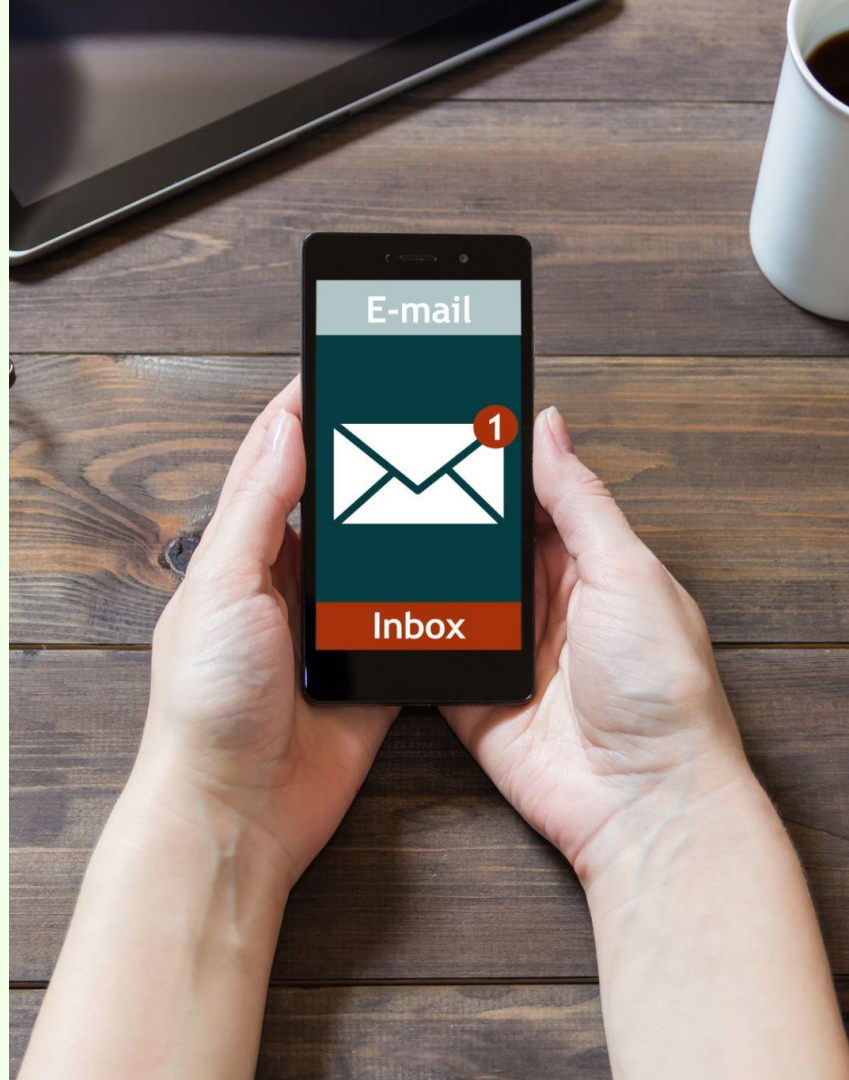


WORDCAMP
GRIÑÓN

Datos que se recopilan

- Subscribers/leads
 - Nombres y apellidos
 - Correo
 - Teléfono¿?
 - Cargo¿?
 - Empresa¿?
 - Edad¿?
- Cookies / Analíticas
- Usuario y contraseña

#WCGriñón



Ingresos - Costes -> Beneficios:

1.000€ - 4.000€

Paquete	Concepto	Precio (rango)	Cantidad	Total	Notas
Sitio Web	Hosting + dominio	100€ - 200€	1	100€ - 200€	
	Diseño	0€ - 3.000€	1	0€ - 3.000€	
	Plugins / servicios	0€ - 200€	1	0€ - 200€	SEO, Newsletter, forms...
TIEMPO	Hora de dedicación	20€	300 - 450	6.000€ - 9.000€	
Ingresos	Reputación	10.000€	1	10.000€	Consultoría, afiliados, ads...

Y qué pasa si te hackean...

Concepto	Tipo
Entender qué ha pasado	Tiempo
Implementar Medidas de Seguridad	Tiempo, Dinero
Servicio para limpiar el sitio	Tiempo, Dinero
Comunicación a la AEPD < 72h	Tiempo
Estudio de riesgo e impacto	Tiempo

Y si la severidad del hackeo es alta...

Concepto	Tipo
Notificar a clientes / Usuarios	Tiempo
Lidiar con las quejas y comunicaciones (Demandas?)	Tiempo/Dinero
Estrés	Tiempo, Dinero
Multa GDPR ($\leq 20.000\text{€}$), si siguen el protocolo	Tiempo, Dinero
Multa GDPR ($\leq 40.000\text{€}$), si no siguen el protocolo	Tiempo, Dinero

Ingresos - Costes -> Beneficios: - (14.000€ - 22.000€)

Paquete	Concepto	Precio (rango)	Cantidad	Total	Notas
Sitio Web	Hosting + dominio	100€ - 200€	1	100€ - 200€	
	Diseño	0€ - 3.000€	1	0€ - 3.000€	
	Plugins / servicios	0€ - 200€	1	0€ - 200€	SEO, Newsletter, forms...
TIEMPO	Hora de dedicación	20€	600 - 1000	12.000€ - 20.000€	
Multas	Según protocolo	8.000€	1	8.000 €	
Ingresos	Reputación	10.000€ - 40%	1	6.000€	Consultoría, afiliados, ads.

CONCLUSIÓN

- Website con uso normal:
 - **Beneficios:** 1.000€ - 4.000€
- Hackeado
 - **Pérdidas:** - (14.000€ - 22.000€)

- **Coste de medidas de seguridad** -> 100€ - 300€
- > Diferencia-> - **(10.000€ - 21.000€)**



#WCGriñón



EJEMPLO 2

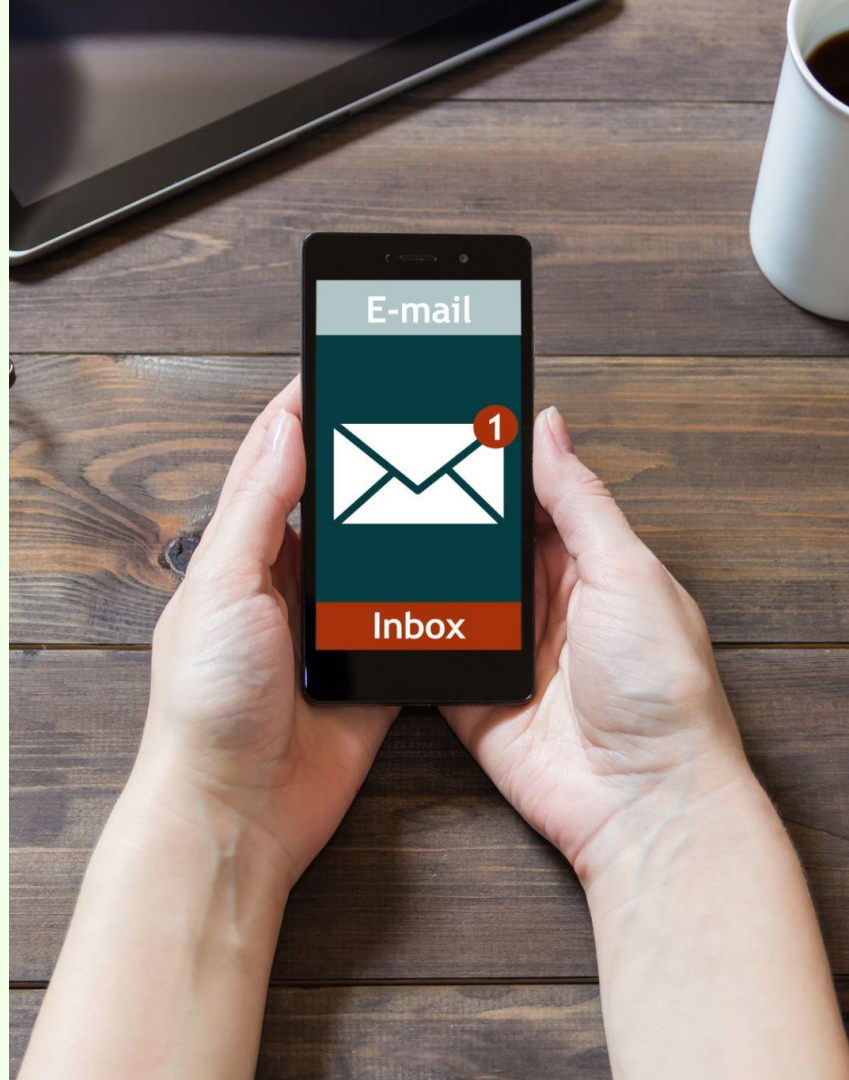
E-Commerce



WORDCAMP
GRINÓN

Datos que se recopilan

- Clientes
 - Nombres y apellidos
 - Correo
 - Teléfono
 - Medios de pago
 - Dirección física
 - DNI o similares
 - Edad
- Cookies / Analíticas
- Usuario y contraseña



Ingresos - Costes -> Beneficios:

~ 50.000€ - 100.000€

Paquete	Concepto	Precio (rango)	Cantidad	Total	Notas
Sitio Web	Hosting + dominio	100€ - 200€	1	100€ - 200€	
	Diseño	0€ - 3.000€	1	0€ - 3.000€	
	Plugins / servicios	300€ - 15.000€	1	300€ - 15.000€	SEO, Newsletter, forms...
	Otros costes	50.000€ - 80.000€	1	80.000€ - 100.000€	Manipulación, sueldos, imp...
TIEMPO	Hora de dedicación	20€	900 - 1500	18.000€ - 30.000€	
Ingresos	Reputación	20.000€	1	20.000€	Consultoría, afiliados, ads...
	Ventas	200.000 €	1	200.000€	

Y qué pasa si te hackean...

Concepto	Tipo
Entender qué ha pasado	Tiempo
Implementar Medidas de Seguridad	Tiempo, Dinero
Servicio para limpiar el sitio	Tiempo, Dinero
Comunicación a la AEPD < 72h	Tiempo
Estudio de riesgo e impacto	Tiempo

Y si la severidad del hackeo es alta...

Concepto	Tipo
Notificar a clientes / Usuarios	Tiempo
Lidiar con las quejas y comunicaciones (Demandas?)	Tiempo/Dinero
Estrés	Tiempo, Dinero
Multa GDPR (≤ 10 mill€ o 2% de ingresos), si siguen el protocolo	Tiempo, Dinero
Multa GDPR (≤ 20 mill€ o 4% de ingresos), si no siguen el protocolo	Tiempo, Dinero

Ingresos - Costes -> Beneficios:

~ -(270.000€ - 300.000€)

















Paquete	Concepto	Precio (rango)	Cantidad	Total	Notas
Sitio Web	Hosting + dominio	100€ - 200€	1	100€ - 200€	
	Diseño	0€ - 3.000€	1	0€ - 3.000€	
	Plugins / servicios	300€ - 15.000€	1	300€ - 15.000€	SEO, Newsletter, forms...
	Otros costes	50.000€ - 80.000€	1	80.000€ - 100.000€	Manipulación, sueldos, imp...
TIEMPO	Hora de dedicación	20€	1200- 1700	24.000€ - 34.000€	
MULTAS	Según protocolo	300.000€	1	300.000€	

















Ingresos	Reputación	20.000€ - 40%	1	12.000€	Consultoría, afiliados, ads...
	Ventas	200k€ - 40%	1	120.000€	

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€

ETid	Country	Date of Decision	Fine [€]	Controller/Processor	Quoted Art.	Type	Source
<input type="text" value="Filter Column"/>	<input type="text" value="Filter Column"/>		<input type="text" value="Filter Column"/>	<input type="text" value="Filter Column"/>		<input type="text" value="Filter Column"/>	
 ETid-1493	 SPAIN	2022-08-11	197,000	AMPLIFON Hungary Trade and Service Provider LLC	Art. 5 (1) b) GDPR, Art. 6 (1) GDPR, Art. 12 (1) GDPR, Art. 14 GDPR	Non-compliance with general data processing principles	link
 ETid-1492	 SPAIN	2022-11-15	80,000	BANKINTER, S.A.	Art. 5 (1) f) GDPR, Art. 32 (1) GDPR	Non-compliance with general data processing principles	link
 ETid-1491	 SPAIN	2022-11-11	3,600	XASTRE DO PETO, S.L.	Art. 6 (1) GDPR, Art. 13 GDPR, Art. 21 GDPR	Insufficient legal basis for data processing	link
 ETid-1490	 SPAIN	2022-11-11	48,000	Banco Bilbao Vizcaya Argentaria S.L.	Art. 5 (1) f) GDPR, Art. 32 GDPR	Non-compliance with general data processing principles	link
 ETid-1489	 SPAIN	2022-11-10	900	Homeowners Association	Art. 5 (1) c) GDPR	Non-compliance with general data processing principles	link
 ETid-1488	 SPAIN	2022-11-10	300	Private individual	Art. 5 (1) c) GDPR	Non-compliance with general data processing principles	link
 ETid-1487	 SPAIN	2022-11-03	70,000	UNITED PARCEL SERVICE ESPAÑA LTD Y COMPAÑIA SRC	Art. 5 (1) f) GDPR, Art. 32 GDPR	Non-compliance with general data processing principles	link
 ETid-1486	 SPAIN	2022-10-31	525,000	TECHPUMP SOLUTIONS S.L.	Art. 5 (1) a), b), e) GDPR, Art. 6 (1) GDPR, Art. 8 GDPR,	Non-compliance with general data processing principles	link

ETid	Country	Date of Decision	Fine [€]	Controller/Processor	Quoted Art.	Type	Source
<input type="text" value="Filter Column"/>	<input type="text" value="Filter Column"/>		<input type="text" value="Filter Column"/>	<input type="text" value="Filter Column"/>		<input type="text" value="Filter Column"/>	
 ETid-1493	 SPAIN	2022-08-11	197,000	AMPLIFON Hungary Trade and Service Provider LLC	Art. 5 (1) b) GDPR, Art. 6 (1) GDPR, Art. 12 (1) GDPR, Art. 14 GDPR	Non-compliance with general data processing principles	link
 ETid-1492	 SPAIN	2022-11-15	80,000	BANKINTER, S.A.	Art. 5 (1) f) GDPR, Art. 32 (1) GDPR	Non-compliance with general data processing principles	link
 ETid-1491	 SPAIN	2022-11-11	3,600	XASTRE DO PETO, S.L.	Art. 6 (1) GDPR, Art. 13 GDPR, Art. 21 GDPR	Insufficient legal basis for data processing	link
 ETid-1490	 SPAIN	2022-11-11	48,000	Banco Bilbao Vizcaya Argentaria S.L.	Art. 5 (1) f) GDPR, Art. 32 GDPR	Non-compliance with general data processing principles	link
 ETid-1489	 SPAIN	2022-11-10	900	Homeowners Association	Art. 5 (1) c) GDPR	Non-compliance with general data processing principles	link
 ETid-1488	 SPAIN	2022-11-10	300	Private individual	Art. 5 (1) c) GDPR	Non-compliance with general data processing principles	link
 ETid-1487	 SPAIN	2022-11-03	70,000	UNITED PARCEL SERVICE ESPAÑA LTD Y COMPAÑIA SRC	Art. 5 (1) f) GDPR, Art. 32 GDPR	Non-compliance with general data processing principles	link
 ETid-1486	 SPAIN	2022-10-31	525,000	TECHPUMP SOLUTIONS S.L.	Art. 5 (1) a), b), e) GDPR, Art. 6 (1) GDPR, Art. 8 GDPR,	Non-compliance with general data processing principles	link

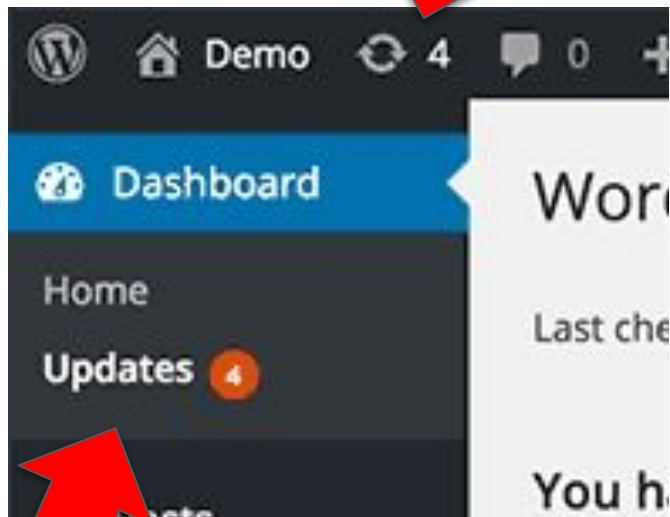


¡Que no me pase a mí!



La importancia de ACTUALIZAR

- Tapas agujeros de seguridad (**Security patches**)
- Los parches de seguridad aparecen después del exploit
- Sobreescribes con **código limpio**
- >70% de las infecciones son debidas a **plugins/temas desactualizados**.



¡RECUERDA!

∇ COSTO Web caída



∇ COSTO Web hackeada

La importancia de LAS CONTRASEÑAS & 2FA

Factores de **AUTENTICACIÓN**:

- Algo que el usuario **es**
(huella digital, identificación facial,...).
- Algo que el usuario **tiene**
(teléfono celular, yubikey, ...)
- Algo que el usuario **sabe**
(contraseña, PIN, ...).



Medidas Proactivas



Reducir administradores, plugins y plantillas



Copias de seguridad



Actualizaciones



Invertir en un buen Hosting y en Seguridad



Web Application Firewall





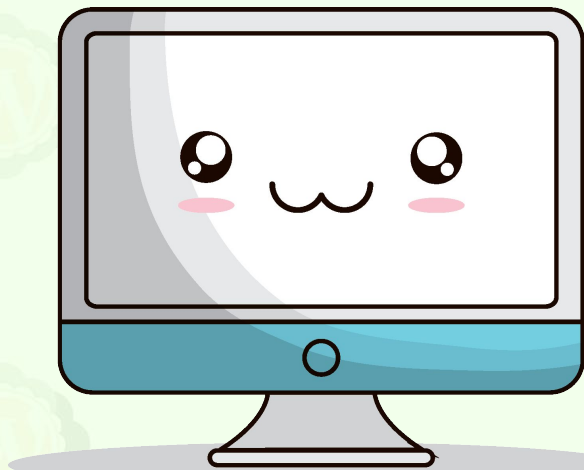
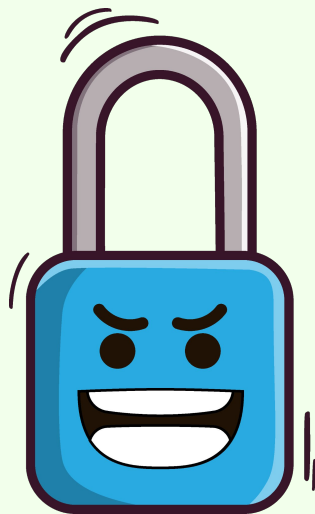
Mi combo ganador

- **SSL** (free)
- **Sucuri** (monitor + Firewall):
200€/año
- **WordFence** (free)
- **Updraft** (70€/año)
- **WP Fail2ban** (free)
- **Two Factor Authentication**
- **CAPTCHA Plugin**

#WCGriñón



BONUS: INVIERTE EN



#WCGriñón



WORDCAMP
GRINÓN

La importancia de tener un buen HOSTING



- Primera capa remota de seguridad
- Sistema de soporte
- Copias de seguridad
- Mantienen el software dependiente (Servidor Web, Base de Datos, Intérprete PHP, etc.) y el hardware.



Alojamiento Compartido vs Dedicado



#WCGriñón



REFERENCIAS: Por si quieres saber más...



#WCGriñón

- GDPR-INFO

<https://gdpr-info.eu/issues/personal-data/>

- GDPR GUIDE for business

<https://www.algoodbody.com/media/TheGDPR-AGuideforBusinesses1.pdf>

- [EnforcementTracker.com](https://www.enforcementtracker.com/) - Seguimiento de multas GDPR.
- [Websitesetup.org](https://www.websitesetup.org/) - How much does a web cost in 2022

<https://websitesetup.org/how-much-does-a-website-cost>

- [PurpleSec.us](https://www.purplesec.us/)

<https://purplesec.us/resources/cyber-security-statistics/>

- AEPD - Guia Brechas de Seguridad

<https://www.aepd.es/es/documento/guia-brechas-seguridad.pdf>

Everybody needs a hacker

#WCGriñón





Esto es todo amigos.

Por ahora...

¡Muchas **GRACIAS!**

Ahora... ¡**PREGUNTAS!**