

The logo consists of a solid orange rounded square containing the word "GAMAKER" in white, sans-serif font. The letters are slightly slanted to the right. The "A" has a small dot above its top curve, and the "E" has a small dot above its middle vertical stroke.

GAMAKER



"To start, press any key."  
Where's the "any" key?

# Complejo ecosistema





# Entorno cambiente

VUCA: volatile uncertain complex and ambiguous world



Todo comienza por establecer la **colaboración**, la **coordinación** y el **compromiso** entre todas las personas interesadas (internas y externas.)

# Hackers



**White Hat**

People who specialized hacking check the faults of the system



**Grey Hat**

Exploit a security to the attention of the owners

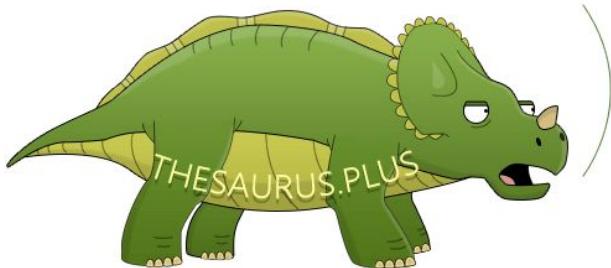


**Black Hat**

People who break into networks and harm to the network and property

## synonyms for hacking:

cut, chop, hew, slash, whoop, hack, lop, saw, cut up, bother



**White Hat is known as Ethical Hacker**



what are other  
words for  
hack?



chop, cut, nag, cab, taxi, jade,  
drudge, hew, notch, gash

Thesaurus.plus



# ¿Hacker?

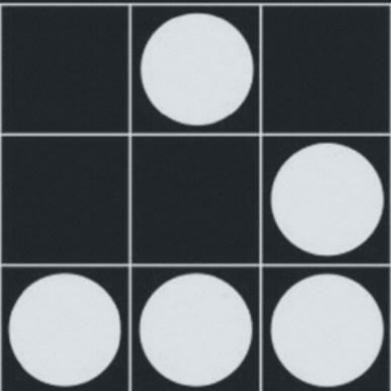
Hacker era el que conseguía programar esa rutina aun mas pequeña y bella.

Hacker era aquel que respetaba el trabajo de otros a los que reconocía como iguales.



main endp  
end main

```
.stack  
.data  
    saludo db "Hola mundo", "0"  
.code \x68\x61\x63\x6b\x73\x74  
main proc  
    mov ax,seg saludo  
    mov ds,ax  
    mov ah,09  
    lea dx,saludo  
    int 21h  
    mov ax,4c00h  
    int 21h  
main endp
```

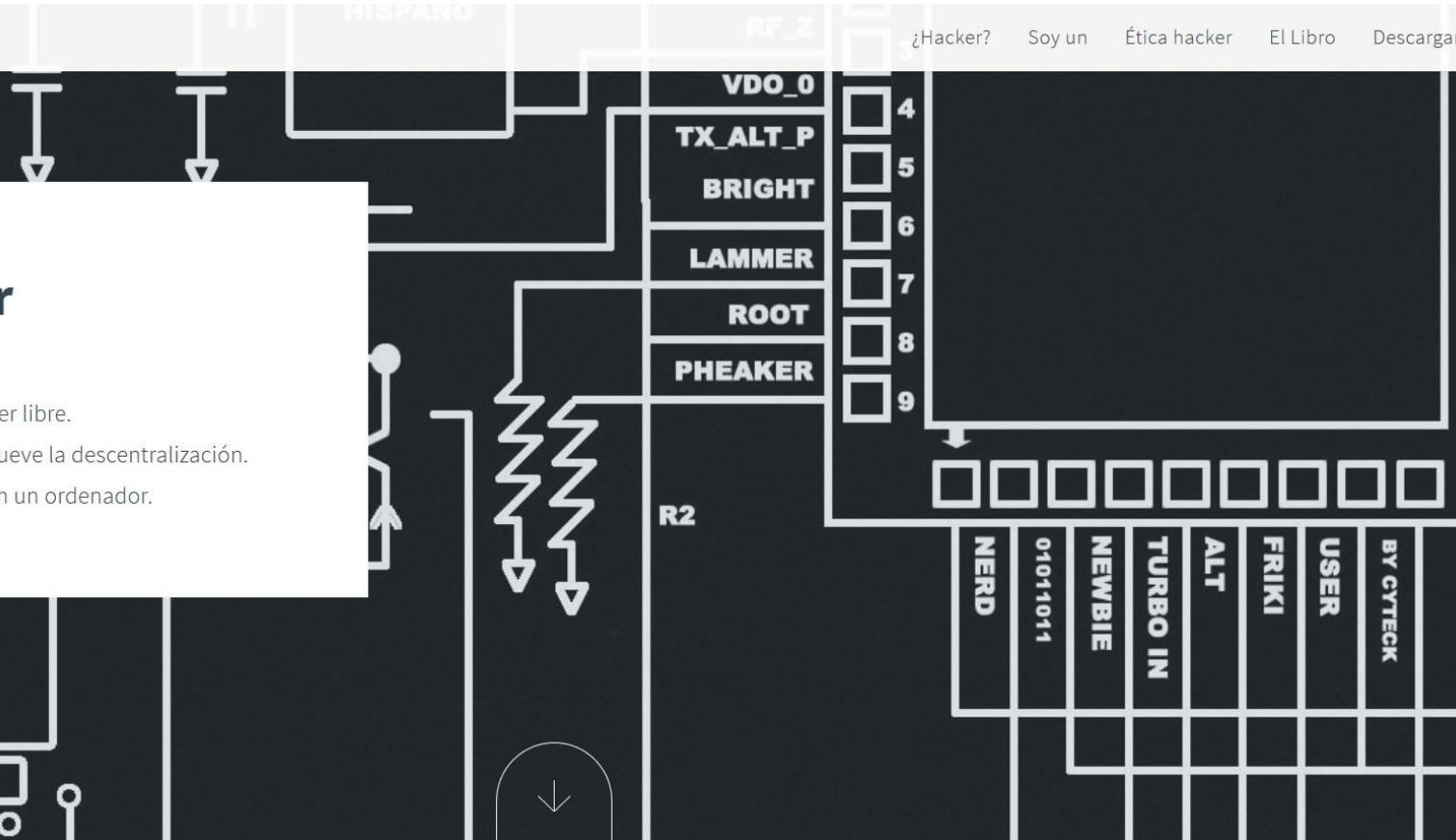
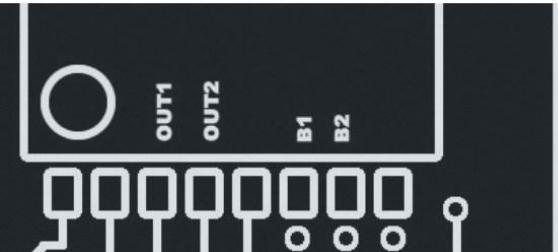


## Sí, soy un delincuente.

Mi delito es la curiosidad. Mi delito es juzgar a la gente por lo que dice y por lo que piensa, no por lo que parece. Mi delito es ser más inteligente que vosotros, algo que nunca me perdonaréis. Soy un hacker, y éste es mi manifiesto. Podéis eliminar a algunos de nosotros, pero no a todos... después de todo, somos todos iguales." THE MENTOR

## La Ética hacker

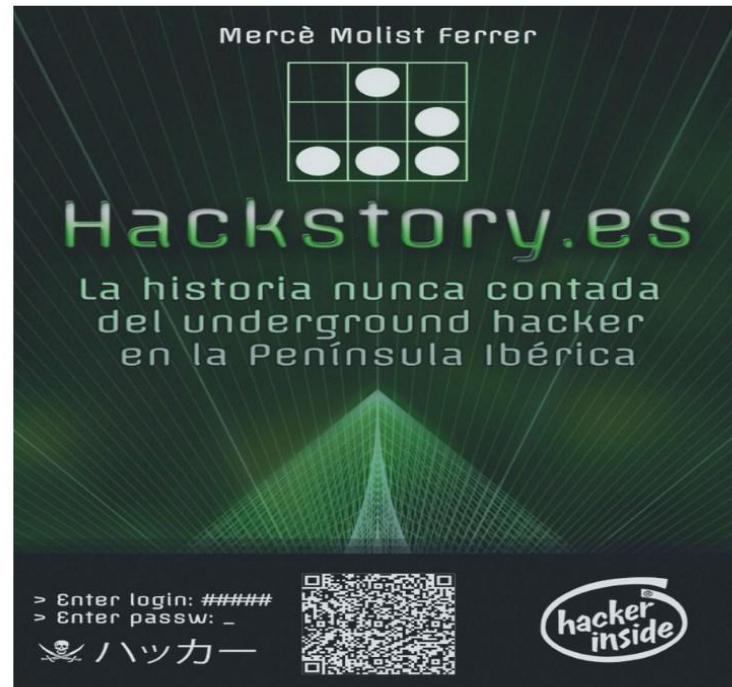
1. Pon las cosas en práctica.
2. Toda la información debería ser libre.
3. No creas a la autoridad. Promueve la descentralización.
4. Puedes crear arte y belleza con un ordenador.



## El Libro

Hackstory.es

La historia nunca contada del underground hacker en la península Ibérica.





Ya están aquí...



### Maker / Hacker

**Definición 1 :** Término para designar a alguien con talento, conocimiento, inteligencia e ingenio, especialmente relacionadas con las operaciones de computadora, redes, seguridad, etc.

**Definición 2 :** Persona que disfruta aprendiendo detalles de los sistemas de programación y cómo extender sus capacidades y que investiga hasta el fondo como están hechas las cosas.



### Analógico / Digital

Medios físicos como herramientas, maquinaria y componentes para poder desarrollar y llevar a la realidad todas las ideas.

Medios digitales de divulgación y comunicación.

Entornos lógicos para compartir el conocimiento en internet y telefonía móvil.



### Crecimiento personal y profesional

Suma de conocimientos de múltiples disciplinas que logran evaluar y desarrollar una idea desde varios puntos de vista.

Educación técnica y formación constante con un bajo coste.

Possibilidad inmediata de networking con el resto de socios y con organizaciones afines.



### Espacio de ideas

Un espacio donde poner en común las ideas y el conocimiento.

Entorno de intereses comunes en aprender y contagiar del espíritu maker donde los proyectos surgen con fluidez de manera espontánea sin ningún tipo de frenos impuestos por ventas o tesorería.



### FAB LAB

Un **Fab lab** (*Fabrication Laboratory*) es un espacio de producción de objetos físicos a escala personal o local que agrupa máquinas controladas por ordenadores.



### HackSpace

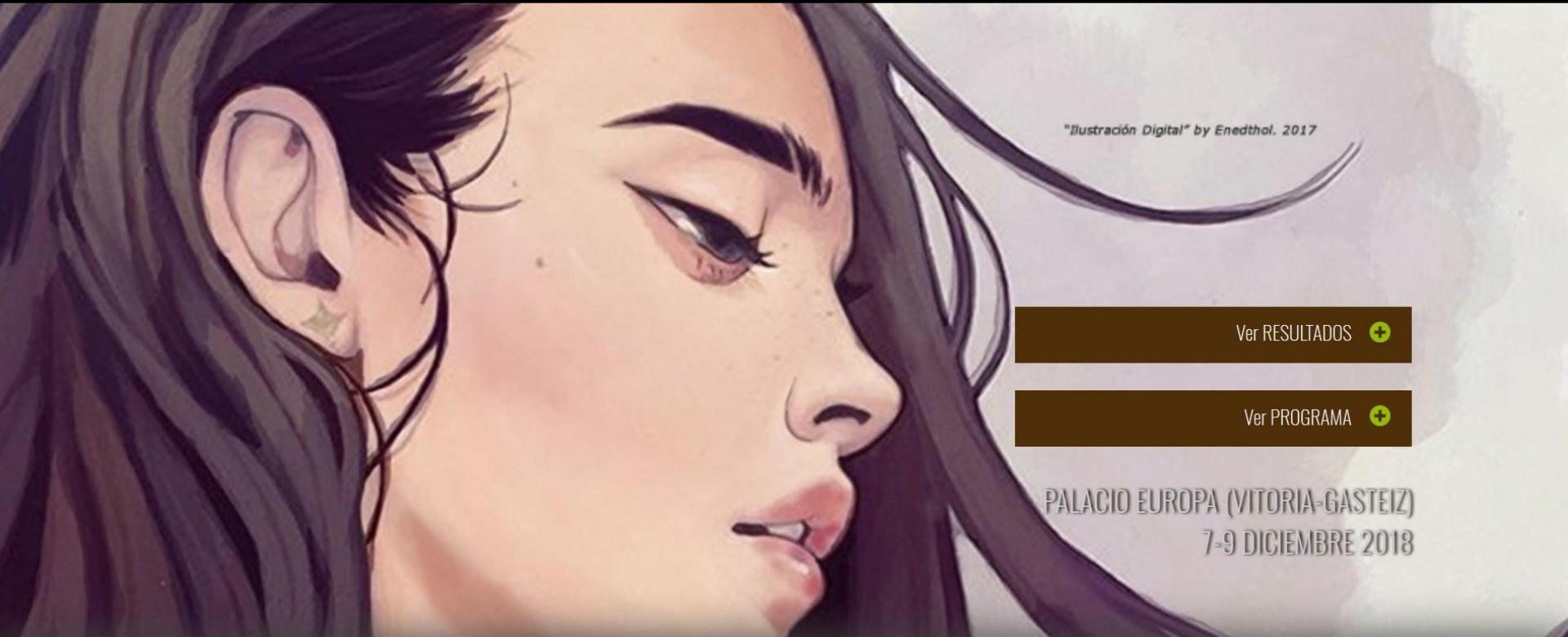
También llamado Hacklab o Hackspace (*espacio de hackers*) es un sitio físico donde gente con intereses en ciencia, nuevas tecnologías, y artes digitales o electrónicas se puede conocer, socializar y colaborar.



### MakeSpace

Espacio de creación, donde los makers utilizan máquinas y instrumentación de medida para hacer realidad sus proyectos innovadores.





"Ilustración Digital" by Enedhol. 2017

Ver RESULTADOS 

Ver PROGRAMA 

PALACIO EUROPA (VITORIA-GASTEIZ)  
7-9 DICIEMBRE 2018

Videos



Fotos



VER MÁS FOTOS

VER MÁS VÍDEOS



# EUSKALHACK SECURITY CONGRESS III

22-23 DE JUNIO DE 2018

COLEGIO MAYOR OLARAIN

DONOSTIA

CAPTURE THE FLAG

COMPRAR ENTRADA

PATROCINAR EVENTO





## UN CONGRESO DONDE TÚ ERES EL PROTAGONISTA

Desde EuskalHack estamos poniendo todo nuestro empeño por realizar - un año más - un congreso inolvidable para todos los asistentes

## ABIERTO EL PERIODO DE CALL FOR PAPERS

El envío de propuestas deberá llevarse a cabo antes del 19 de marzo, valorando especialmente su originalidad y contribución a la comunidad





## EVENTO ABIERTO A TODOS LOS PÚBLICOS

Nos esforzamos por ofrecer contenido dirigido a profesionales, investigadores, estudiantes y aficionados a la seguridad informática

## AMBIENTE DISTENDIDO SIN PRECEDENTES

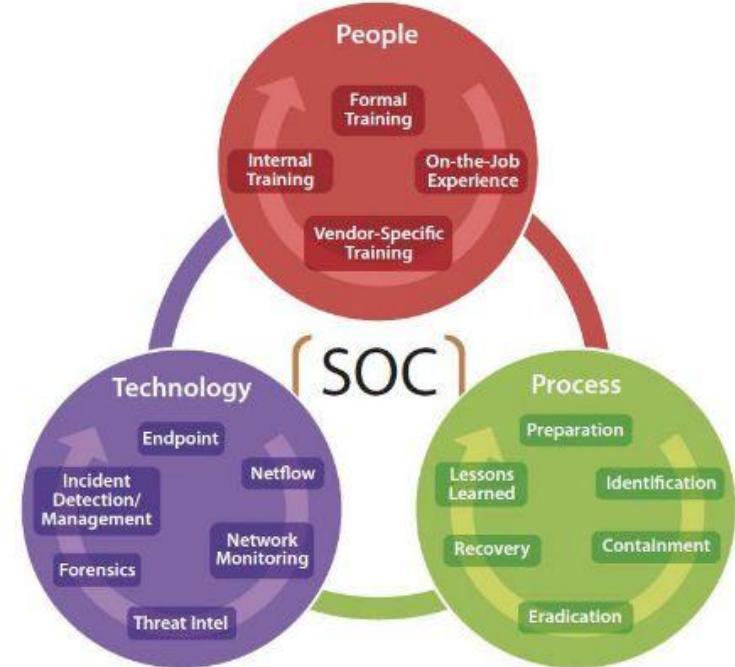
Queremos que los asistentes se encuentren como en casa. Como no podía ser de otro modo, incluimos el almuerzo en el precio de la entrada



# Cyber Security?

La ciberseguridad es el conjunto de:

- herramientas,
- políticas,
- conceptos de seguridad,
- salvaguardas de seguridad,
- directrices,
- métodos de gestión de riesgos,
- acciones,
- formación,
- prácticas idóneas,
- (ciber)seguros,
- tecnologías



... que pueden utilizarse para proteger los activos de la organización y a las personas en el ciber-entorno.



# Perspectiva histórica... ¿Cuándo empezó todo?

- Comienzos del siglo XX
- Los años 30
- Los años 60
- Década de los 70
- Años 80
- Años 90
- Siglo XXI
- Ciberseguridad en el mundo actual





# Perspectiva histórica... Comienzos del siglo XX.

1903:

**John Nevil Maskelyne** (ilusionista e inventor británico) es considerado el primer hacker de la historia.



Empleando un transmisor de código morse y una antena de 50 metros, pudo llevar a cabo la interceptación de un mensaje del telégrafo inalámbrico, enviado desde la Royal Institution de Londres, a larga distancia donde se encontraba Marconi.

Logró su objetivo de emitir él su propia mezcla de insultos y frases de Shakespeare.



# Perspectiva histórica... Los años 30:

Alan Turing fue el principal responsable de descifrar Enigma, el código secreto utilizado por el Ejército alemán en la Segunda Guerra Mundial, contribuyendo con ello a acortar la guerra. Inventó una máquina, llamada la bomba, que permitía descifrar mensajes Enigma de forma masiva. En 1943 se desvelaban 84.000 mensajes alemanes al mes. Sus métodos de criptoanálisis fueron decisivos para paliar la amenaza de los submarinos en la Batalla del Atlántico

[https://www.eldiario.es/turing/criptografia/alan-turing-enigma-codigo\\_0\\_226078042.html](https://www.eldiario.es/turing/criptografia/alan-turing-enigma-codigo_0_226078042.html)



# Perspectiva histórica...



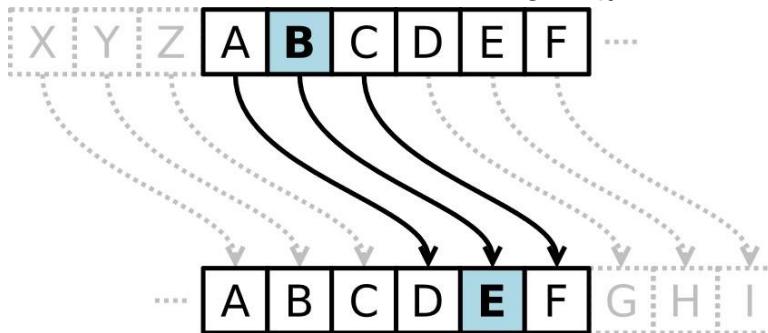
Julio Iglesias  
Cantante

Julio Iglesias ha entrado en una polémica sin quererlo por la decisión de Ana Botella de investirle como hijo predilecto. O, por lo menos, la posición es la que ha criticado este reconocimiento porque, dicen, es una decisión que ha llegado sin el acuerdo de los grupos. Estas propuestas, aseguran, las tienen que alcanzar los partidos en consenso, pues son unos «honores que la ciudad tiene que entregar y no otorgarlos sólo el Gobierno». Al margen de esto, se prevé que marzo sea el mes en que Madrid otorgue el premio al cantante.



## Aproximación a la criptografía.

- **Esteganografía:** Ocultar un mensaje (en textos, imágenes,...)
- **Código:** Correspondencia (palabras, realidad,...)
- **Criptografía:** Herramientas para transformar el mensaje (primeros cifrados por sustitución ej. Cifrado César.)



A ↗	H ↘	N ←	U ↖
B ↙	I ↗	O ↘	V ↖
C ↙ or ↘	J ↗	P ↘	W ↖
D ↙	K ↗	Q ↘	X ↙ or ↘
E ↗ or ↘ or ↙	L ↗	R ↘	Y ↗ or ↘
F ↖	S ↗	Z ↗	—
G ↙	M ↗	T ↘	SH ↗

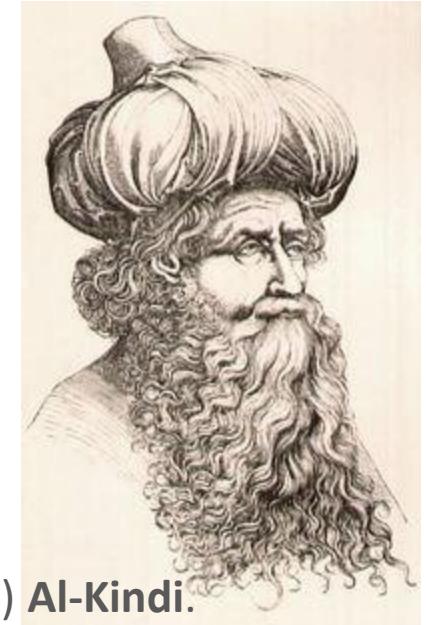
# Perspectiva histórica...

Aproximación a la criptografía.

- 900 aC: La **Escítala** en Grecia.
- 100 aC - 41 aC: Cifrado César (se sustituye por la tercera letra).
- 801 dC - 873 dC: Primer criptoanálisis (science of code breaking) **Al-Kindi**.
- 1491: **Cifrado Homófonos**; ej. Isabel la Católica a su embajador de Londres

"considerando si la ciudad de 12 debe ser 90 o 39 90, estamos construyendo una 88 allí -en Santa Fe- en la que esperamos reunir buenas 97 para 94 12 o, al menos, para tenerla tan estrechamente cercada que 39 sea necesario 94 de nuevo."

- 90 = *conquistar*
- 94 = *sitiar*



# Perspectiva histórica...

Aproximación a la criptografía.



- 1523 - 1596: Blais de Vigenere: **Cifrado Vigenere**.
- 1860 aprox.: **Criptanálisis Kasiski**. En 1863 Friedrich Kasiski publica: *Escritura secreta y el arte de descifrarla*. Expone cómo romper el cifrado Vigenere.

Entrada CLAVE

0	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
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	
B	C	D	E	F	G	H	I	J	K	L	M	N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	
C	D	E	F	G	H	I	J	K	L	M	N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	
D	E	F	G	H	I	J	K	L	M	N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	
E	F	G	H	I	J	K	L	M	N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	
F	G	H	I	J	K	L	M	N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	
G	H	I	J	K	L	M	N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	
H	I	J	K	L	M	N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	
I	J	K	L	M	N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	
J	K	L	M	N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	
K	L	M	N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	
L	M	N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	
M	N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	N	
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	N		
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	N	O		
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	N	O	P		
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	N	O	P	Q		
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	N	O	P	Q	R		
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	N	O	P	Q	R	S		
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	N	O	P	Q	R	S	T		
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	N	O	P	Q	R	S	T	U		
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	N	O	P	Q	R	S	T	U	V		
Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	N	O	P	Q	R	S	T	U	V	W		



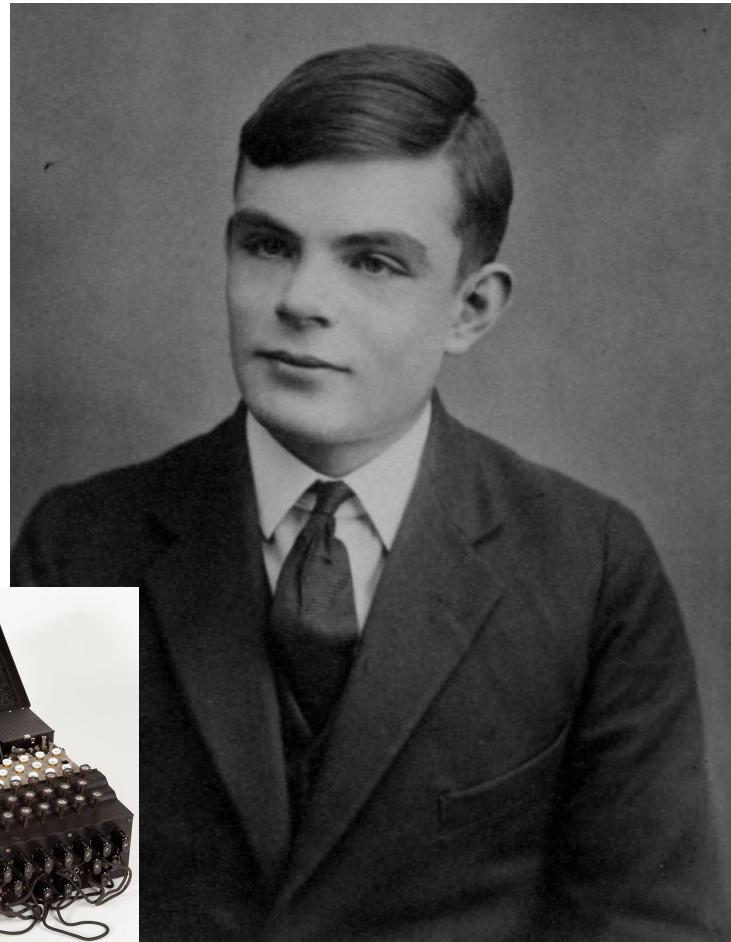
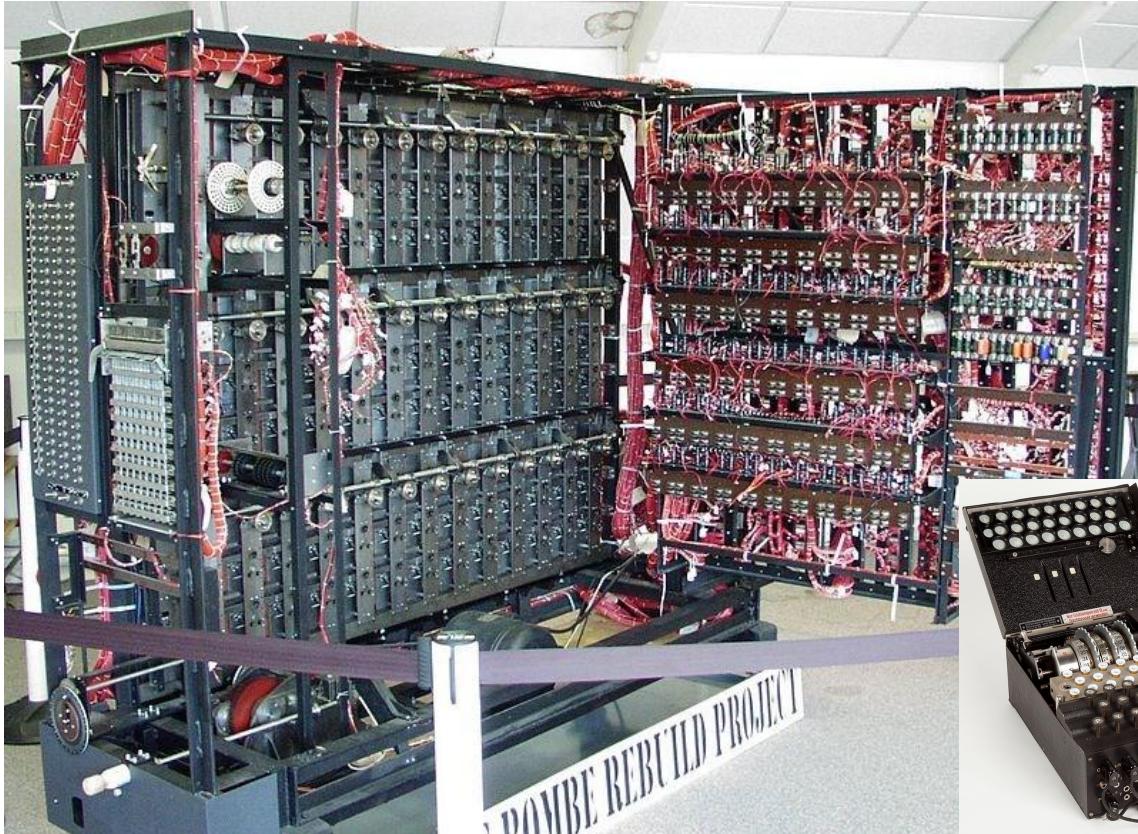
# Perspectiva histórica... Desiderata de Kerckhoffs:

1. El sistema tiene que ser indescifrable en la práctica, si no lo es matemáticamente.
2. **El método de cifrado no debería requerir secreto y no debería ser un problema que cayese en manos del enemigo.**
3. Deber ser posible comunicarse y recordar la clave sin usar notas escritas. Los usuarios pueden cambiar la clave a voluntad.
4. Debe ser aplicable a las comunicaciones telegráficas.
5. Debe ser portable y no tiene que requerir a muchas personas para operarlo.
6. El sistema debe ser fácil de usar y no debe requerir que los usuarios sepan una larga lista de reglas.

Criptografía Militar, Journal des sciences militaires, 1883



# Perspectiva histórica... Descifrando Enigma



# Perspectiva histórica... Hedy Lamarr

Glamurosa espía, mujer fatal, la actriz más bella de Hollywood, investigadora científica e “inventora” del sistema de comunicaciones precursor de los actuales sistemas de tecnologías radar, GPS y WiFi.

Cleptómana y adicta a las pastillas, mantuvo oculta su actividad de inventora. Desarrolló el actual concepto de **salto de frecuencia** empleado para teledirigir torpedos.

El 9 de noviembre se celebra en su homenaje el *Día Internacional del Inventor*.

La actriz, famosa tras protagonizar el primer desnudo en una película comercial y después de que Gustav Machaty filmase su orgasmo en *Éxtasis*, huyó de su marido (Hedy tenía raíces judías y estaba casada por conveniencia con un antisemita, Fritz Mandl, magnate fabricante de armas austriaco y aliado y amigo de Hitler y Mussolini) para mudarse a Estados Unidos y triunfar en Hollywood. Rechazó los guiones para protagonizar *Casablanca* y *Luz que agoniza*. Hedy Lamarr cedió gratuitamente durante la Segunda Guerra Mundial al ejército estadounidense una patente registrada en 1942 de su propiedad (sin reconocimiento) para desarrollar un sistema secreto de comunicaciones.



# Perspectiva histórica... Teoría de la Información

Claude E. Shannon (1916 - 2001)

Durante la 2a Guerra Mundial, Shannon creó las bases para los sistemas de comunicaciones actuales. Se publicaron al acabar la Guerra.

- A Mathematical Theory of Communication,  
Bell System Technical Journal 27, 1948
- Communication Theory of Secrecy Systems,  
Bell System Technical Journal 28, 1949



# Perspectiva histórica... Década de los años 60:

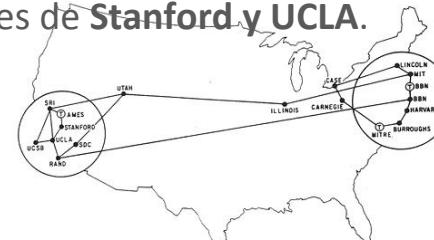
1965:

- William D. Mathews (MIT) publica la **primera vulnerabilidad** que permite conocer el contenido del fichero de claves en Multics CTSS sobre IBM 7094.
- La explotación de la vulnerabilidad se basa en los ficheros temporales con el mismo nombre al editar el fichero.

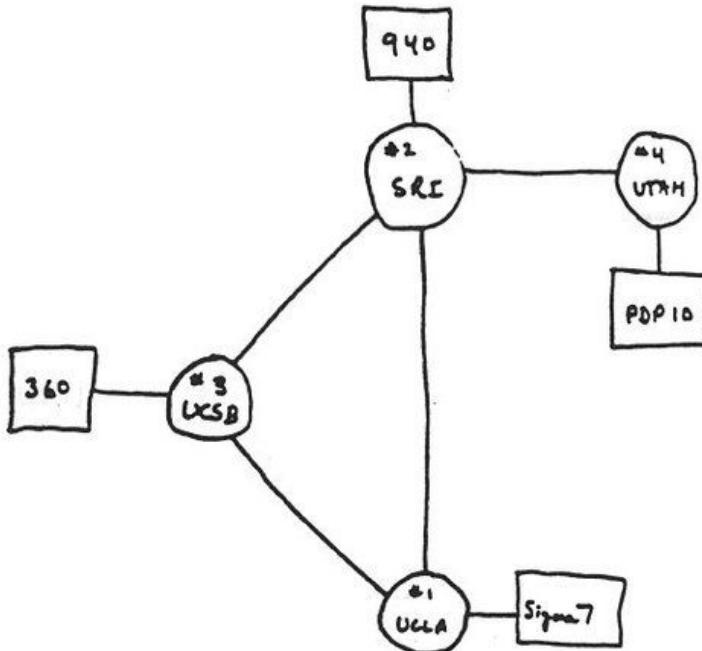
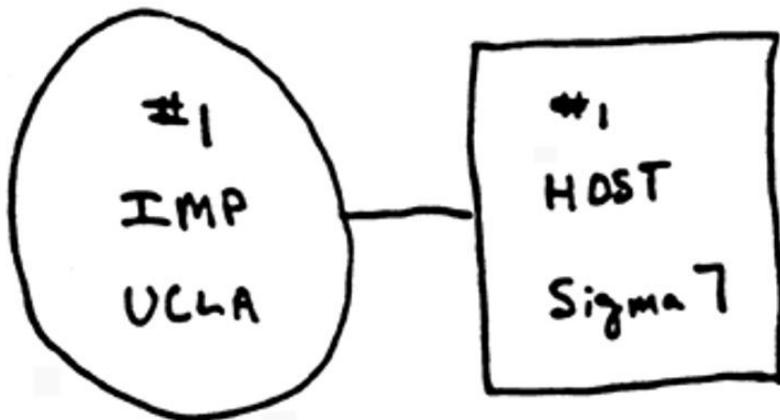


El 29 de Octubre de 1969 se transmite el **primer mensaje** a través de ARPANET.

El 21 de Noviembre de 1969 se establece el **primer enlace** entre las universidades de **Stanford** y **UCLA**.



MAP 4 September 1971



THE ARPA NETWORK

DEC 1969

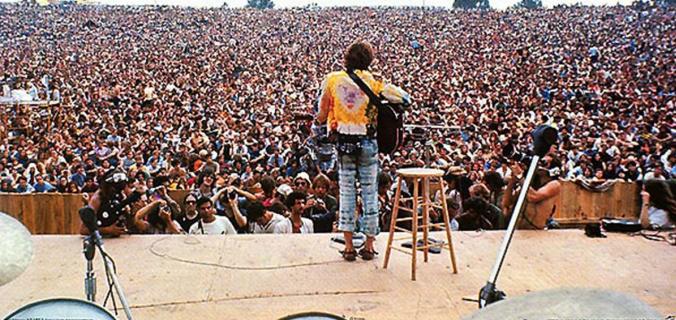
4 NODES

# WOODSTOCK

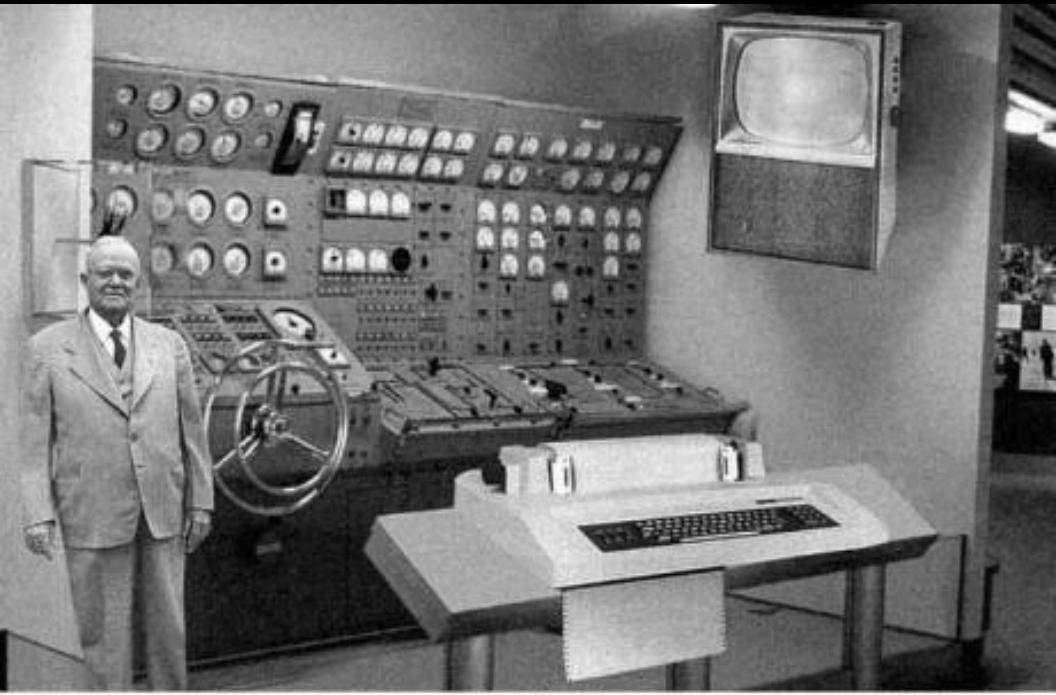
3 DAYS OF PEACE & MUSIC 1969



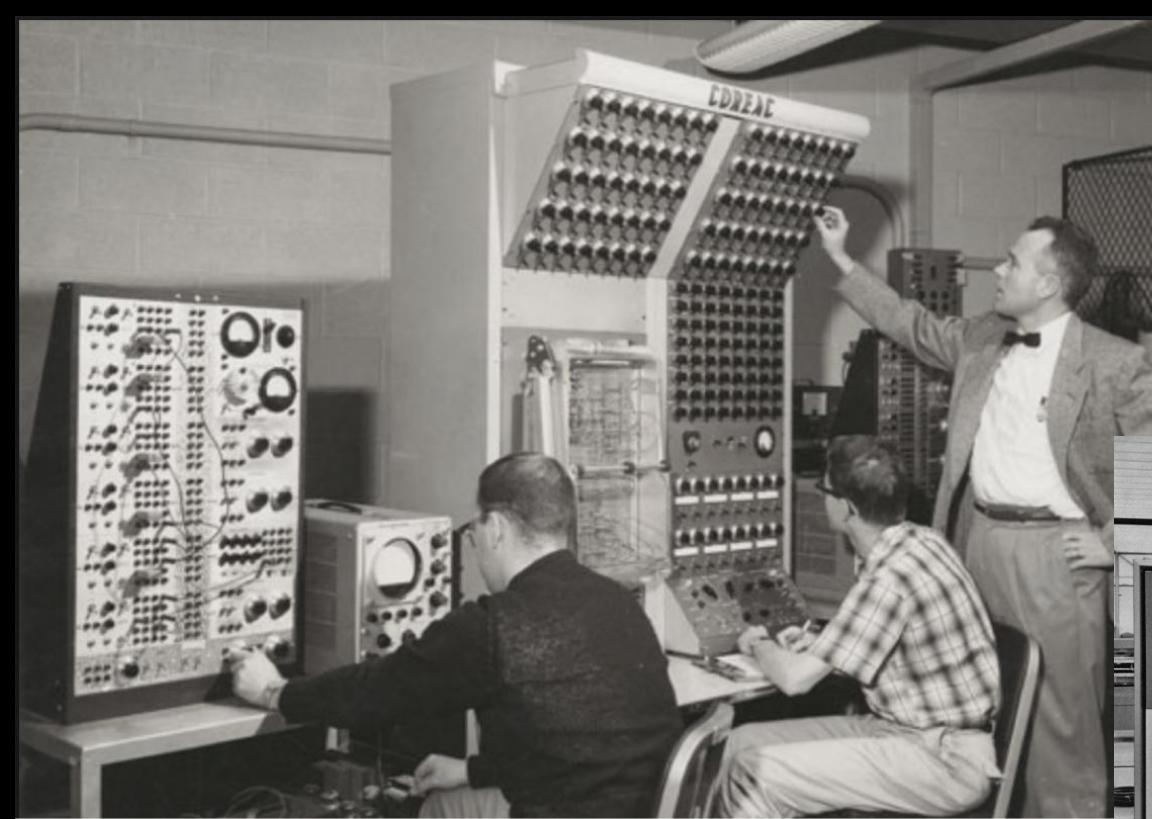
1969







*Scientists from the RAND Corporation have created this model to illustrate how a "home computer" could look like in the year 2004. However the needed technology will not be economically feasible for the average home. Also the scientists readily admit that the computer will require not yet invented technology to actually work, but 30 years from now scientific progress is expected to solve these problems. With teletype interface and the Fortran language, the computer will be easy to use.*



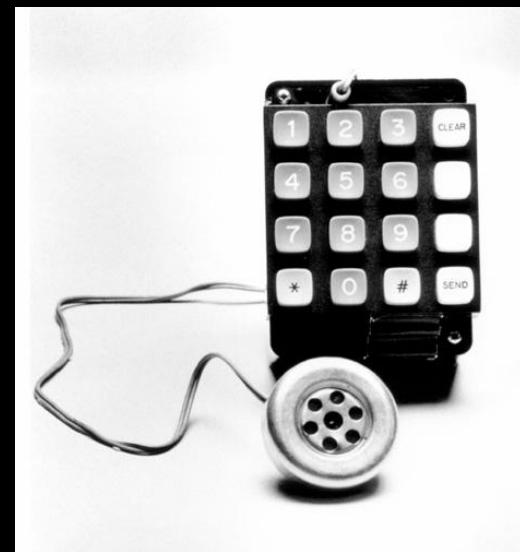
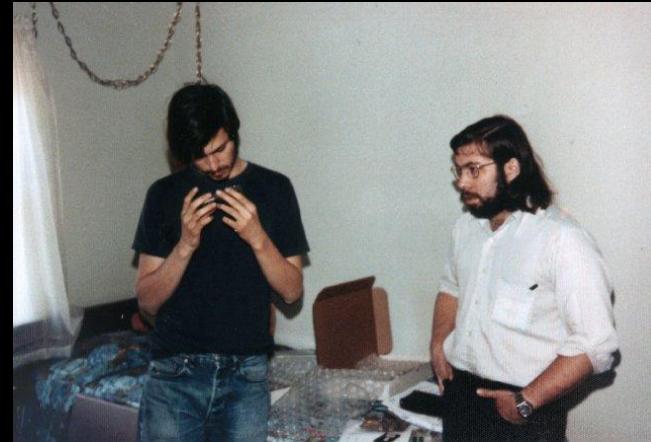
# Perspectiva histórica... Década de los años 70:



El silbato que cambió el mundo... <https://www.mundosilbato.es/blog/el-silbato-que-cambio-el-mundo>

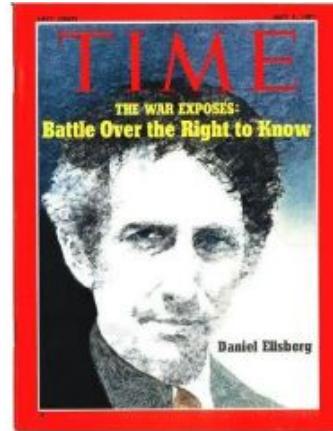
En 1971 John T. Draper (**Captain Crunch**) y Joe Engressia se hacen famosos por sus técnicas de **Phone Phreaking** mediante **Blue Boxes** (dispositivo electrónico para reproducir la marcación por tonos); tapando con pegamento uno de los agujeros del silbato se produce una frecuencia de 2600 Hz, que casualmente es la misma que empleaba AT&T para entrar en modo operador.

Steve Jobs y Steve Wozniak comenzaron ensamblando **Blue Boxes** en el Homebrew Computer de California.





# Perspectiva histórica...



## Los papeles del Pentágono:

- En junio de 1971, el New York Times comenzó a publicar extractos de un estudio clasificado del departamento de defensa que detallaba la intervención militar de EE.UU. en el sudeste asiático. Los documentos, que se conoció como los Papeles del Pentágono, revelaron una larga historia de bombardeos, invasiones militares secretas, y deliberadas mentiras sobre la participación de Estados Unidos en la región desde la década de 1950.
- **Daniel Ellsberg**, analista militar que había fotocopiado el informe, fue acusado de robo y conspiración, pero el caso fue archivado cuando se encontró que los fiscales federales habían utilizado escuchas ilegales.

# Perspectiva histórica..



Bob Woodward y Carl Bernstein (Washington Post). Momento de la dimisión de Richard Nixon.

## Caso Watergate (1972-1974):

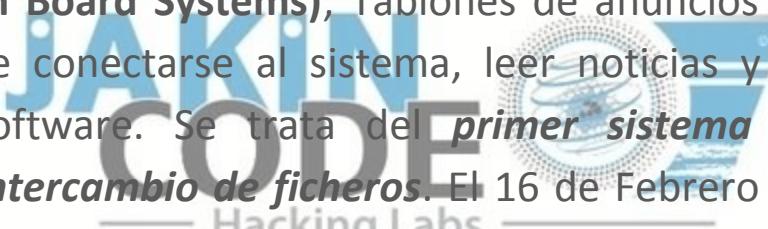
- Comienza con el arresto de cinco hombres por el allanamiento de la sede del Partido Demócrata en el complejo de oficinas Watergate, en Washington, D. C. el 17 de junio de 1972. Nixon y su equipo conspiraron para ocultar el allanamiento.
- Después de dos años reuniendo pruebas contra el entorno del presidente, que incluía a miembros de su equipo testificando contra él en una investigación del Senado de los Estados Unidos, se **reveló que Nixon tenía un sistema de grabación de cintas magnéticas** en sus oficinas y que había grabado una gran cantidad de conversaciones dentro de la Casa Blanca.



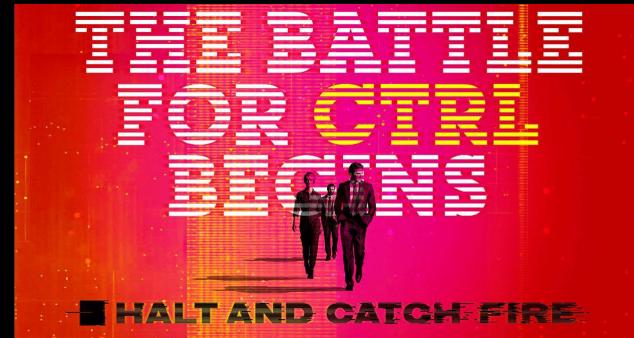
# Perspectiva histórica... Finales de los años 70:

Comienzan a existir hosts interconectados por módem.

- **BBS (Bulletin Board Systems)**; Tablones de anuncios desde donde conectarse al sistema, leer noticias y descargar software. Se trata del *primer sistema público de intercambio de ficheros*. El 16 de Febrero de 1978 Ward Christensen crea CBBC.
- **Wardialing**: Permite realizar llamadas automáticas a una serie de números de teléfono. Su objetivo es encontrar módems conectados para establecer una conexión con otro host.



# HALT AND CATCH FIRE



# WELCOME TO MUTINY

amc

HALT AND  
CAUGHT FIRE



© 2013 AMC Networks, Inc. All rights reserved.



# Comparing DES and AES

## Perspectiva histórica... Cifrado en los 70's:

Las grandes corporaciones necesitan **cifrado**.

	DES	AES
Developed	1977	2000
Key Length	56 bits	128, 192, or 256 bits
Cipher Type	Symmetric block cipher	Symmetric block cipher
Block Size	64 bits	128 bits
Security	Proven inadequate	Considered secure

- Hasta entonces, el cifrado era un tema exclusivo de gobiernos.
- En el 1972 el *US National Bureau for Standards* empieza una convocatoria para definir un nuevo cifrado.
- En el 1973 se selecciona la propuesta de IBM y la NSA aconseja hacer unas mejoras.
- En 1977 se declara el **DES** - Data Encryption Standard.



Se mantiene hasta el 2000, con la llegada del **AES** – Advanced Encryption Standard

# Perspectiva histórica... Criptografía de Clave Pública:

- Clave pública.
- Clave privada.



- Si cierro con la Pública, abro con la Privada.
- Si cierro con la privada, abro con la pública.

New Directions in Cryptography, W. Diffie M. Hellman, 1976.



Rivest, Shamir, Adleman, (La importancia de los primos) A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, Communications of the ACM 1978.

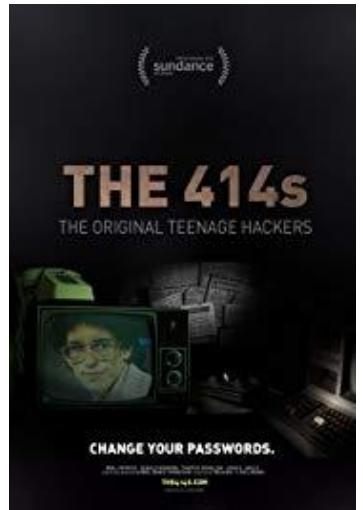
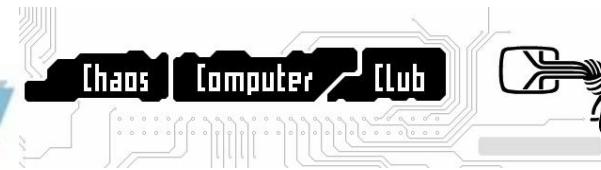
# Perspectiva histórica... Principios de los años 80:

1981: Fundación del **Chaos Computer Club** en Alemania y **The Warelords** en EEUU; compuesto por Hackers, Phreakers, Coders, geeks, black hat, underground, ...



1982: The 414s entran en 60 sistemas gubernamentales y aparecen en los medios. Se asocia el término hacker a la seguridad informática. Las primeras leyes surgen del congreso de EEUU al respecto.

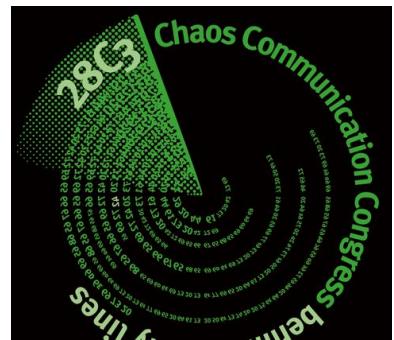
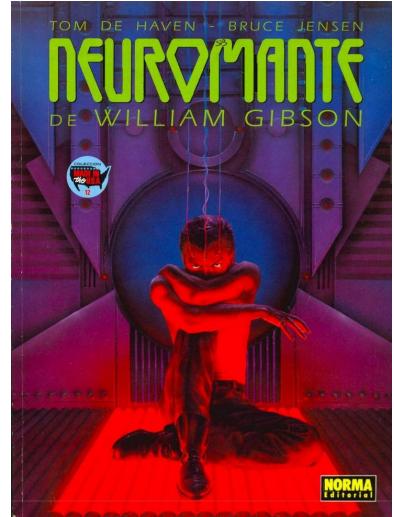
1983: Fundación del grupo **KILOBAUD**. El FBI captura a The 414s pero muchos no son acusados. La película "Juegos de Guerra" desata la paranoia en la opinión pública frente al fenómeno del hacking.



Perspectiva histórica... Mediados de los años 80:

1984:

- Fundación del **Legion of Doom**.
- **Cult of the Dead Cow** y comienza su e-zine. Publicación de la revista *hacker 2600*.
- Primer **Chaos Communication Congress** en Hamburgo.
- Publicación de la novela **Neuromante** para introducción de jerga hacker (cyberspace, the matrix, simstim, ICE, ...)



# Perspectiva histórica... Mediados de los años 80:

1985:

- El grupo *Kilobaud* se convierte en *The PHIRM* gestionando cientos de BBS en los EEUU, Canada y Europa.
- Publicación del e-zine *Phrack*. En Reino Unido se publica *Hacker's Handbook*.



1986:

- El congreso de EEUU aprueba la *Computer Fraud and Abuse Act*, convirtiendo en delito el ataque a sistemas informáticos.
- *The Mentor* es arrestado y publica el *Hacker's Manifesto* en la e-zine *Phrack*

Phrack Inc. presents Volume One, Issue One, Phile One of #8

Introduction...

Welcome to the Phrack Inc. Philes. Basically, we are a group of phile writers who have combined our philes and are distributing them in a group. This newsletter-type project is home-based at Metal Shop. If you or your group are interested in writing philes for Phrack Inc., you, your group, your BBSs, or any other credits will be acknowledged. We will also accept philes on telnet (phreaking), cracking, anarchy (guns and death & destruction) and hacking. Other topics will also allow to also to an certain extent. If you feel you have some material that's original, please call and we'll include it in the next issue possible. Also, you are welcome to use these philes on your BBS/AE/CCW/ETC. Etiquette and rules regularly available at Metal Shop. In the philes that your BBS will be sponsoring Phrack Inc., please leave feedback to me, Tarun King stating you'd like your BBS in the credits. Later on...

TARUN KING  
2660 CLUB!  
METAL SHOP SYSP

This issue is Volume One, Issue One, released on November 17, 1985. Included:

- 1 This Introduction to Phrack Inc. by Tarun King
- 2 SAM Security Article by Spitfire Hacker
- 3 Boot Tracing on Apple by Cheap Shades
- 4 The Fone Phreak's Revenge by Iron Soldier
- 5 How to Make a Micro Chip by Mr. Spud
- 6 How to Pick Master Locks by Gin Fizz and Ninja NYC
- 7 How to Make an Acetylene Bomb by The Clashmaster
- 8 School/College Computer Dial-Ups by Phantom Phreaker

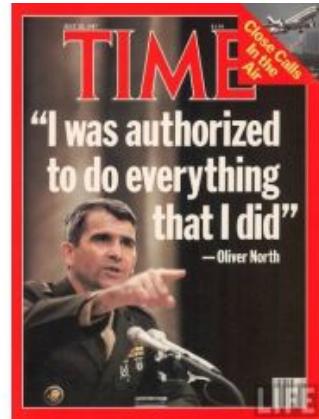
Call Metal Shop and leave feedback saying the phile topic and where you got these philes to get your article in Phrack Int.

Hacker's Manifesto by The Mentor

Damn kids, there's all alike...  
but did you in your three-week squalor and 95% technobrain, ever take a look behind the eyes of the hacker?  
Did you ever wonder what they think, what forces shaped them,  
what molded them?  
It's a world that begets with 95% similar than most of the other kids, this crap they teach us here me.  
Damn undisciplined...  
I've listened to teachers with the fifteen new hokey dokey... I understand...  
Damn kid...  
...you're not a computer... They're not  
I found a computer. What's it good for? What was it used to be, it's a silly noise, a computer won't do...  
Not because it doesn't like me... Or was threatened by me... Or didn't want me and abandoned here...  
I'm not a computer... They're not  
I'm not a computer... They're not  
This is it... THIS IS WHERE I BELONG...  
I've never seen the ocean, nor the sun, nor the moon, nor the stars, may never hear them again... I like you all...  
You get your ass, we're all alike...  
We've been spurned for body and a social life... We're the best that you can't stop through your closed and... tasteless  
We've been betrayed by society... We've been lied to... We've been lied to... We've been lied to...  
These forces like power and wealth... or wealth and status... or wealth and...  
We're not angry for what could be... We're not angry for what we've lost... We're not angry for...  
just being... We're not angry for...  
We exist without skin color, without nationality, without race...  
You built atomic bombs, you stage wars, you murder, cheat, lie to and try to make believe it's a lone bull's eye...  
My crime is that of judging people by what they say and think, I look up...  
I am a hacker, and THIS is my manifesto...  
You may STOP this individual, but you can't stop us all... after all...  
WE'RE ALL ALIKE!

# Perspectiva histórica...

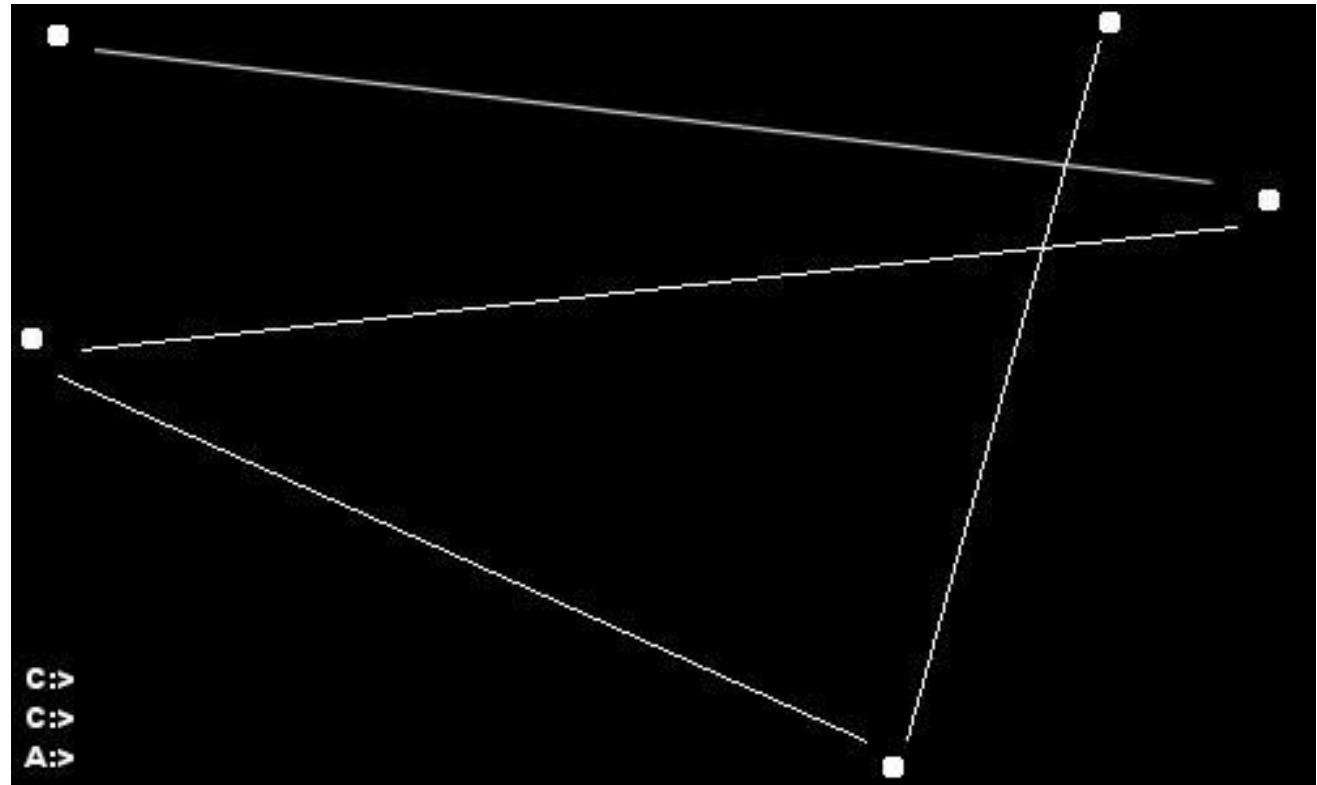
## Escándalo Irán-Contra (1986-1987):



- Gracias a la información filtrada por el clérigo chií Mehdi Hashemi, una revista libanesa publica el escándalo Irán-Contra.
- De manera clandestina, los funcionarios de la administración Reagan había vendido armas al gobierno iraní (a pesar del embargo existente) para lograr un intercambio de armas por rehenes.
- Las ganancias de las ventas se utilizaron para ayudar a financiar los rebeldes anticomunistas en Nicaragua, una violación directa de una prohibición del Congreso. Reagan negó inicialmente la venta, pero una semana más tarde lo admitió.



# Perspectiva histórica... 1988: Virus Ping-pong



# Perspectiva histórica... Finales de los años 80:

1987:

- Publicación en Italia de la e-zine Decoder.
- El gusano Christmas Tree EXEC worm provoca el caos en las redes VNET, BITNET y EARN.



1988:

- Robert T. Morris lanza un gusano en la red ARPAnet y es expulsado de la Universidad de Cornell, sentenciado a 3 años de libertad condicional y multa de 10.000 US\$.
- El First National Bank of Chicago es víctima de un robo informático de 70 millones de US\$.
- Creación del CERT (Computer Emergency Response Team) por DARPA.

1989:

- Lanzamiento de la revista Mondo 2000.
- El gusano con motivación política WANK en red DECnet.



# Perspectiva histórica... Gusano Morris:

- Se propagó el 2 de Noviembre de 1988.
- Afectó al 10% de Internet.
- Explotó vulnerabilidades de finger, sendmail y rsh/exec.
- Provocó la creación del primer CERT.
- Supuso la primera condena en EEUU por la Ley de Fraude y Abuso Informático.
- Pérdidas: 100 millones de \$.



# Perspectiva histórica... Principios de los años 90:



ELECTRONIC FRONTIER FOUNDATION

1990:

- Creación de la *Electronic Frontier Foundation*, tras la operación *Sundevil* la comunidad hacker se rompe (chivatazos) y se capturan numerosos sospechosos.
- La policía federal australiana es la primera en interceptar datos remotos como evidencia de ataques.



1992: Primer virus polimórfico 1260 del programador búlgaro *Dark Avenger*.

1993: Primera DEFCON en Las Vegas.

1994:



- 10 millones de US\$ robados al Citibank por crackers rusos (Vladimir Levin).
- Publicación de *AOHell* y una horda de scripts-kiddies tumba AOL.

# Perspectiva histórica... Principios de los años 90:

- Caso **PGP** - 1991

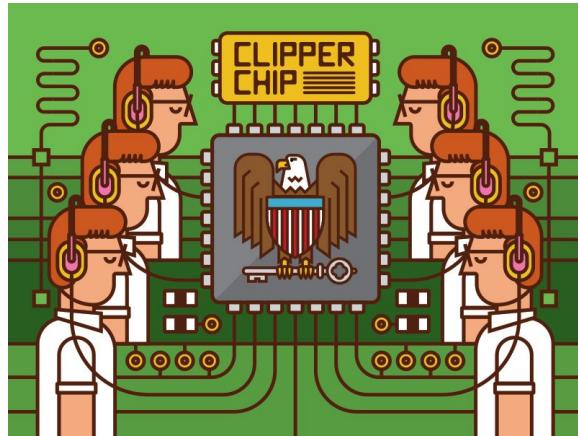
El cifrado tenía restricciones en la exportación. Su creador, estuvo a punto de ir a la cárcel.



Imprimió el código del Sistema de cifrado como un libro y lo exportó, amparándose en el derecho de libertad de expresión. Los libros no estaban sujetos en a los códigos de exportación.

- Caso **Clipper Chip** - 1994

La NSA quiso promover que todos los teléfonos cifrados usaran un chip que guardase todas las contraseñas.





**WANTED**  
**BY U.S. MARSHALS**

NOTICE TO ARRESTING AGENCY: Before arrest, validate warrant through National Crime Information Center (NCIC).  
United States Marshals Service NCIC entry number: COCO\_V721660021

NAME: ..... MITNICK, KEVIN DAVID  
AKA (s): ..... MITNICK, KEVIN DAVID  
..... KERBIL, BRIAN ALLEN

DESCRIPTION:  
Sex: ..... MALE  
Race: ..... WHITE  
Place of Birth: ..... TAN HUTS, CALIFORNIA  
Date(s) of Birth: ..... 04/06/63; 10/18/70  
Height: ..... 5'11"  
Weight: ..... 190  
Eyes: ..... BLUES  
Hair: ..... BLACK  
Skin: ..... LIGHT  
Scars, Marks, Tattoos: ..... SOME SPOTTY  
Social Security Number (s): ..... 310-39-3435  
NCIC Fingerprint Classification: ..... D09CQ0PM130CPH19PM09

ADDRESS AND LOCALE: KNOWN TO RESIDE IN THE SAN FERNANDO VALLEY AREA OF CALIFORNIA AND LAS VEGAS, NEVADA

WANTED FOR: VIOLATION OF SUPERVISED RELEASE  
CRIMINAL CHARGES: POSSESSION UNAUTHORIZED ACCESS DEVICE; COMPUTER FRAUD  
Warrant Issued: CENTRAL DISTRICT OF CALIFORNIA  
Warrant Number: 9312-2111-0154-C

DATE WARRANT ISSUED: NOVEMBER 10, 1992

MISCELLANEOUS INFORMATION: SUBJECT SUFFERS FROM A WEIGHT PROBLEM AND MAY HAVE EXPERIENCED WEIGHT GAIN OR WEIGHT LOSS

**FREE KEVIN**

# Perspectiva histórica... Mediados de los años 90:

Kevin Mitnick es detenido por el FBI el 15 de Febrero de 1995.

Este mismo año que se estrenan las películas *La Red* y *Hackers piratas informáticos*.

1996:

- Defacements en webs del Departamento de Justicia de EEUU, la CIA, US AirForce, ...
- *Brotherhood* es el grupo de hackers canadienses que entran en la Canadian Broadcasting Corporation.
- El 65% de los ataques contra el Departamento de Defensa fueron exitosos.



Pueden quebrantar cualquier código y entrar en cualquier sistema. Normalmente son solo adolescentes y ya se encuentran bajo la vigilancia de las autoridades. Son los piratas informáticos. Zero Cool, de nombre Wade Murphy, es una leyenda entre los de su clase. En 1988 provocó el solo la caída de 1.507 ordenadores en Wall Street y las autoridades lo prohibieron tocar un solo teclado hasta que cumpliera 18 años. Han transcurrido siete años sin probar un solo byte... y tiene hambre. Kate Libby, conocida como Acid Burns, tiene un potente ordenador portátil que en la autopista de la información pasa de 0 a 60 en un macrosegundo. Cuando ambos se enfrentan, la batalla de los sexos explota al disco duro.

Perdona la suerte esta achada cuando el maestro de los piratas The Plague, implica a Wade, Kate y sus amigos en una diabólica conspiración industrial. Ahora son los únicos que pueden evitar una catástrofe... la peor que jamás haya existido.



UNITED ARTISTS PICTURES Presenta IAIN SOFTLEY para THACKERS, JONNY LEE MILLER, ANGELINA JOLIE, FISHER STEVENS y LORRAINE BRACCO  
Música SIMON BOSWELL, Guión CHRISTOPHER BLUNDELL, MARTIN WALSH, Productor Ejecutivo JOHN DEARD, Director de Fotografía ANDRZEJ SĘKUŁA  
Fotógrafo IAIN SOFTLEY, De-productor JANET CRABBE, Writer RAFael MOREU, Produced by MICHAEL PEYSER, RALPH WINTER, Directed by IAIN SOFTLEY  
Read the Angelina Jolie Book

**características especiales**

- Folleto de 8 páginas con información sobre la producción.
- Pantallas de menú interactivas con una selección de 32 escenas.
- Trailer cinematográfico original.



16:9 2.35:1	PAL	DVD FORMAT
Certificado de clasificación: 51.290		
No recomendada menores 13 años		
	VERSIÓN	PARA SORDOS
Castellano	Inglés	Alemán
Duración aprox. 1h 48 min • COLOR		

HACKERS © 1995 United Artists Pictures Inc. Todos los derechos reservados. Distribuidor © 1995 MGM Home Entertainment Inc. Todas las derechos reservados. "Duffy" y el símbolo Doblé D son marcas registradas de Duffy Laboratories Licensing Corporation. ADVERTENCIA: El ejercicio de los derechos de autor no concedidos o licenciados en este documento, sin la autorización escrita del propietario de los derechos de autor, es una violación de los derechos de autor. La difusión de este material sin la autorización escrita del propietario de los derechos de autor es una violación de los derechos de autor. Los derechos de autor incluyen, entre otros, la utilización de este DVD en lugares como salas, bibliotecas, hospitales, museos, plazas, ferias, exposiciones, reuniones y mitines. Copiar, editar, restringir, vender, transferir, publicar, difundir, utilizar para fines de exhibición pública o la realización de copias de este material sin la autorización escrita del propietario de los derechos de autor es una violación de los derechos de autor. El uso de este material para fines de exhibición pública o la realización de copias de este material sin la autorización escrita del propietario de los derechos de autor es una violación de los derechos de autor. Este DVD es vendido y ampliado con la condición de no ser objeto de importación, almacenamiento ni lugar o actividad privada o comunitaria.



DVD

571690

24

Pensabas que tus secretos estaban a salvo.  
Pensabas mal.

# HACKERS

(PIRATAS INFORMÁTICOS)

DVD

571690

24

# HACKERS

(PIRATAS INFORMÁTICOS)

# Perspectiva histórica... Finales de los años 90:

1997:

- Un hacker croata de 15 años entra en los ordenadores de la base militar de EEUU en Guam.
- La RIAA comienza su acoso legal a los distribuidores de MP3. Después de un año de fracasos surge Napster.



1998:

- Yahoo! es infectado en su página principal con un gusano y una bomba lógica que exige la liberación de Kevin Mitnick.
- El primer estudio de *Information Security* revela de  $\frac{3}{4}$  de las organizaciones ha sufrido un incidente de seguridad en el último año.



	Filename	Filesize	Bitrate	Frequency	Length
Online	< Zion I - critical.mp3	3,798,959	128	44100	3:51
	< Yuji Oniki - paper tigers.mp3	3,505,970	128	44100	3:33
	< Young Scott Perrie - everytime.mp3	4,957,964	320	44100	2:01
	< Wonderlick - right crazy rough mix.mp3	4,572,891	128	44100	4:39
	< Willard Grant Conspiracy - christmas in nevada.mp3	3,579,530	128	44100	3:38
	< Unknown - coconuts.mp3	4,856,236	128	44100	4:56
	< Wellwater Conspiracy - of dreams.mp3	3,466,264	128	44100	3:31
	< Waco Brothers - fox river.mp3	3,903,738	128	44100	3:58
	< Vivendo de Pao - riso de gilberto.mp3	3,377,656	128	44100	3:26
	< Vivendo de Pao - jacare.mp3	3,166,169	128	44100	3:13
	< Virgil Shaw - water cooler.mp3	4,988,928	128	44100	5:04
	< Virgil Shaw - volvo ff.mp3	3,220,086	128	44100	3:16
	< Unknown - next degree.mp3	4,062,125	128	44100	4:07
	< Unknown - are we people.mp3	2,932,736	96	44100	3:58
	< Trail of Dead - mistakes and regrets merge.mp3	3,631,104	128	44100	3:41
	< Tom Heyman - bottle full of wishes.mp3	4,008,229	128	44100	4:04
	< Tom Armstrong - thinking of him.mp3	2,671,723	128	44100	2:43
	< Tom Armstrong - looking forward to looking back.mp3	3,475,877	128	44100	3:32
	< tobyslater - the next life.mp3	3,089,870	128	44100	3:08
	< Unknown - sky is not crying.mp3	6,891,439	128	44100	7:00
	< The Rosenbergs - sucking on a plum.mp3	3,120,193	128	44100	3:10
	< The Rosenbergs - soaked in polyester.mp3	4,795,374	128	44100	4:52
	< The Rosenbergs - secret.mp3	4,147,955	128	44100	4:13
	< The Rosenbergs - overboard.mp3	6,839,612	128	44100	6:57
	< The Rosenbergs - little lie.mp3	2,911,214	128	44100	2:57
Offline					
	jonknibbs				
	t_kaura				

User: napster06062001 Total Files: 262 File Data: 1,014 megs Ping: N/A

[Get Selected Files](#) [Add User to Hot List](#)

# audiogalaxy



Music Search

go

Front Page

go

member login

**featured artist****Three 4 Tens**

These Philly based indie-rock kids are proud to be all about 60s psychedelia and have even opened up for the Who.

**Music News:**  
**Chubby Seeks Nobel Prize**

Early Rock n' Roller **Chubby Checker**, popularizer of "The Twist" (and its many variances), has sent an open letter to both the Rock n' Roll Hall of Fame and the Nobel Prize Committee.

**departments**[Rock/Alternative](#)[Electronica](#)[Metal](#)[inside audiogalaxy](#)[Punk](#)[Download Satellite](#)[Blues](#)[Users](#)[Folk](#)[Groups](#)[Jazz](#)[All Genres](#)[Hip-Hop](#)[Software / Hardware](#)[Country](#)[Feature Archive](#)[Record Labels](#)[Bulletin Board](#)**featured department****folk****Tom House**

Gruff and scary folksongs from a Nashville "poet and barroom singer." The combination of the extremely casual musical production and House's reedy, tuneless warble drives these bare, desolate songs right into the pit of your stomach.

Audiogalaxy: soundtrack - Microsoft Internet Explorer

Archivo Edición Ver Favoritos Herramientas Ayuda | Dirección e3dd86ce4084&searchType=0&searchStr=soundtrack | Ir a

Music Search  go — Jump To — go

Vínculos Google Dejanews AltaVista CNET e-Lingo

Found Exact Match:  
**soundtrack**

see all 7111 matches

Other listeners liked **theme, john williams, moby**

25 comments all songs

+ ADD TO FAVORITES 1270 FANS

All Songs 1-25 of 11338 songs sort by Popularity go

- soundtrack - gladiator
- soundtrack - blade
- soundtrack - gone in 60 seconds
- soundtrack - The Cast Of "My Best Friend's Wedding"-I Say A Little Prayer
- soundtrack - run lola run
- soundtrack - romeo and juliet-when doves cry
- soundtrack - x-men
- soundtrack - fifth element
- soundtrack - city of angels
- soundtrack - Charlie's Angels
- soundtrack - last of the mohicans

Audiogalaxy Satellite - v0.609W, logged in as: awmvannie...

File Options Display Settings Go Help

MP3-file	Size (kB)	%	Speed	Time left
fatboy slim - Moulin Rouge.mp3	200/4861	4%	15.38	7:26
ian pooley - cold wait.mp3	447/8986	4%	10.97	25:56

Recv: 0 files/0.20 MB Sent: 0 files/0.34 MB Enter searchstring:  
Time left: 7 min Time left: 25 min Go

Got response from master server Connected to server (257) 1051 0

Listo Internet



# **PIRATES of SILICON VALLEY**

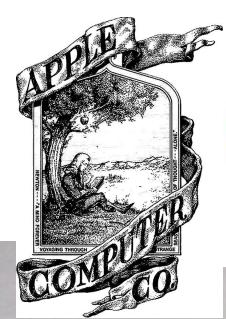
[PLAY MOVIE](#)

[SCENES](#)

[FEATURES](#)

[LANGUAGES](#)





1977 - 1998  
By Rob Janoff



1998  
Translucent Version



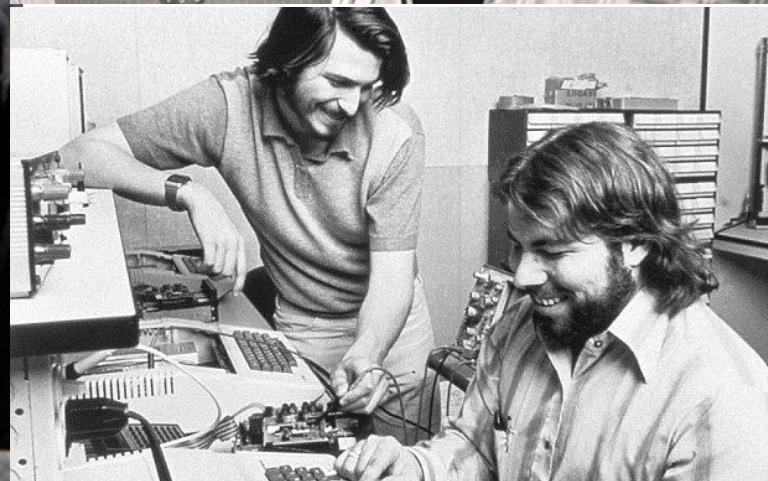
1998 - 2000  
Monochrome Version

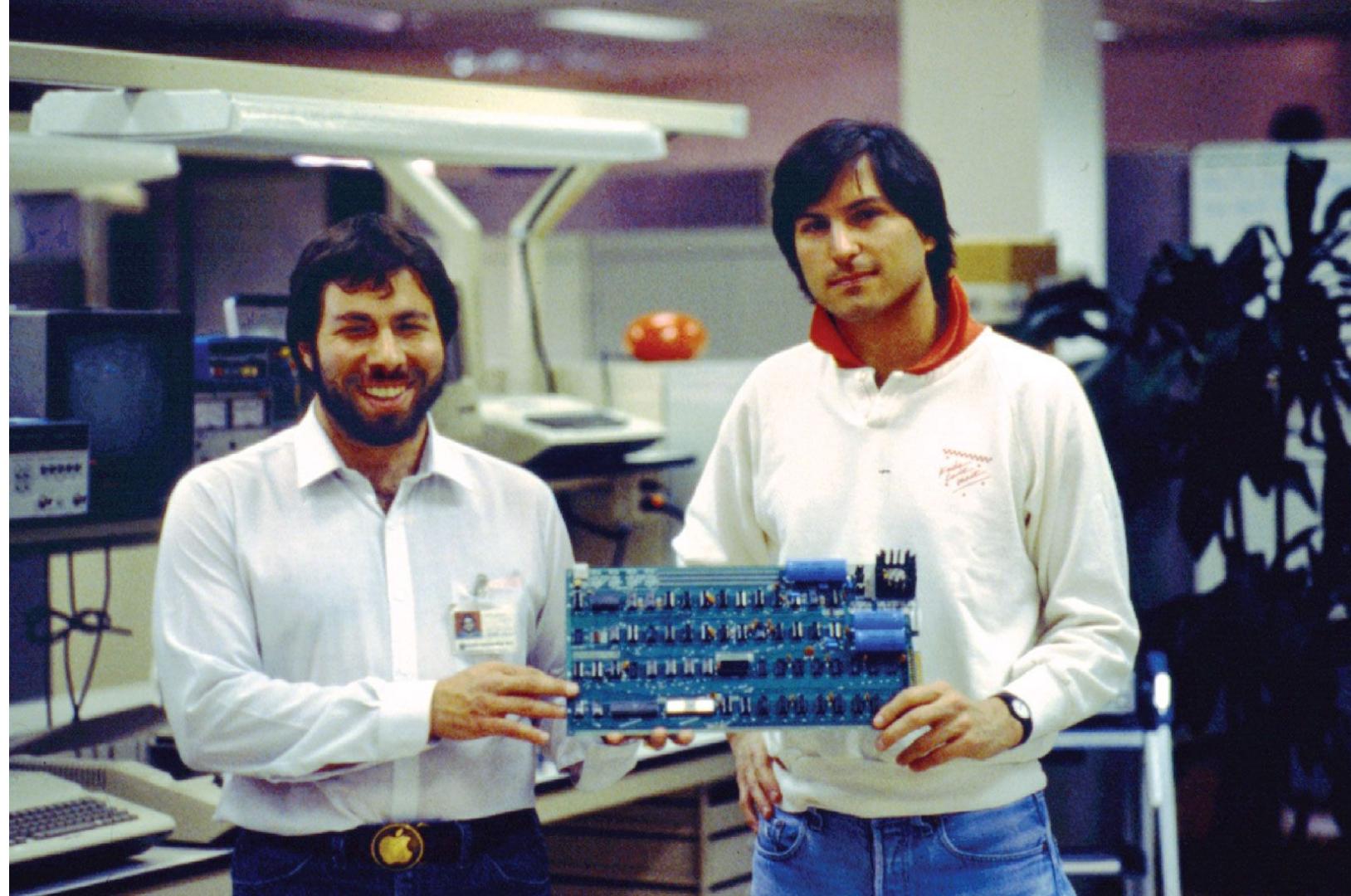


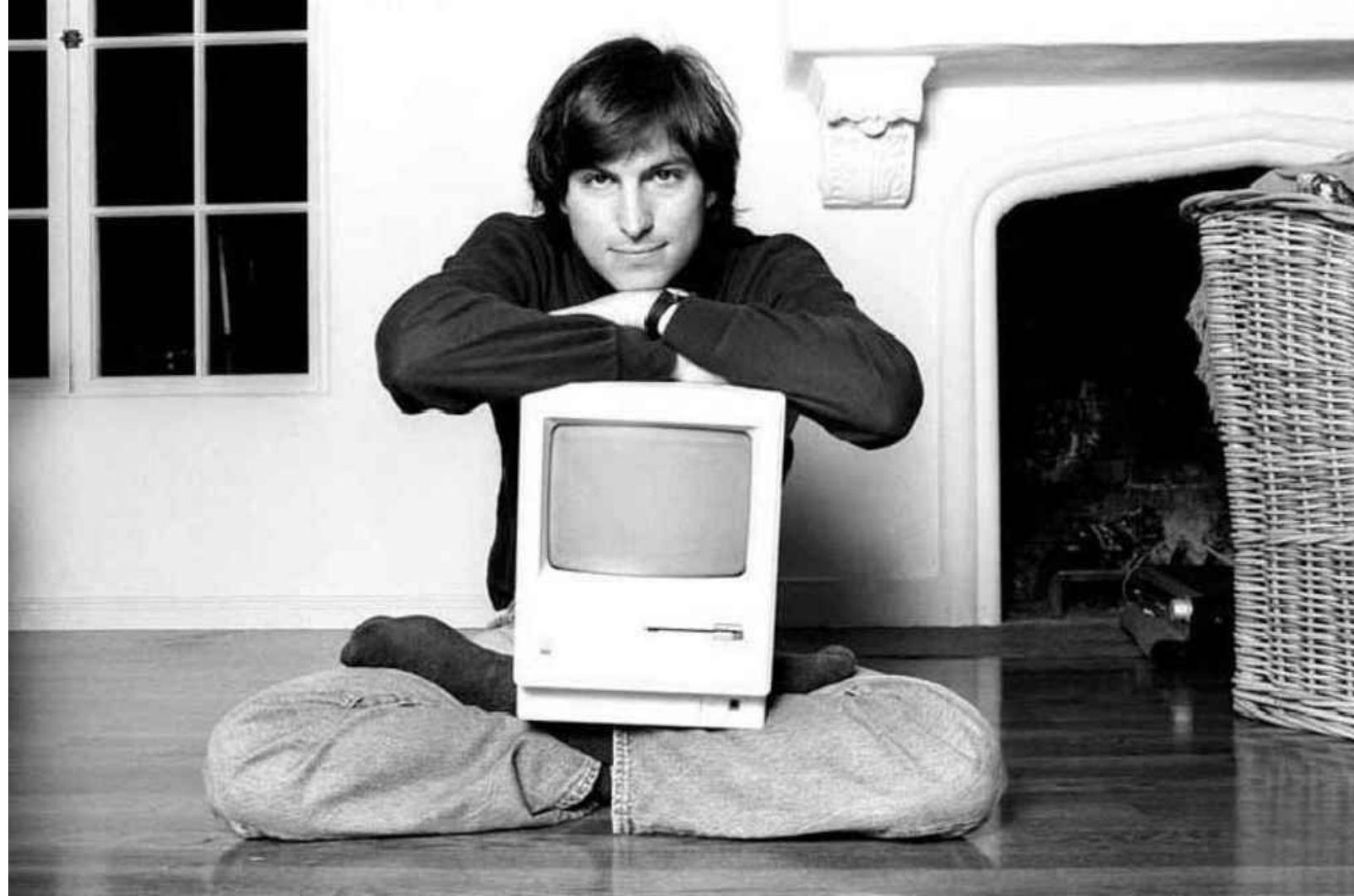
2001 - 2007  
Aqua Version



Current  
Chrome Version



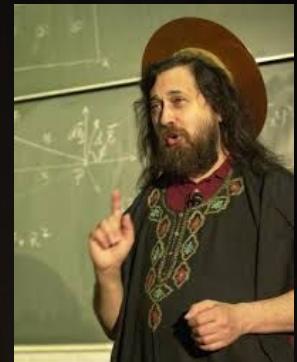
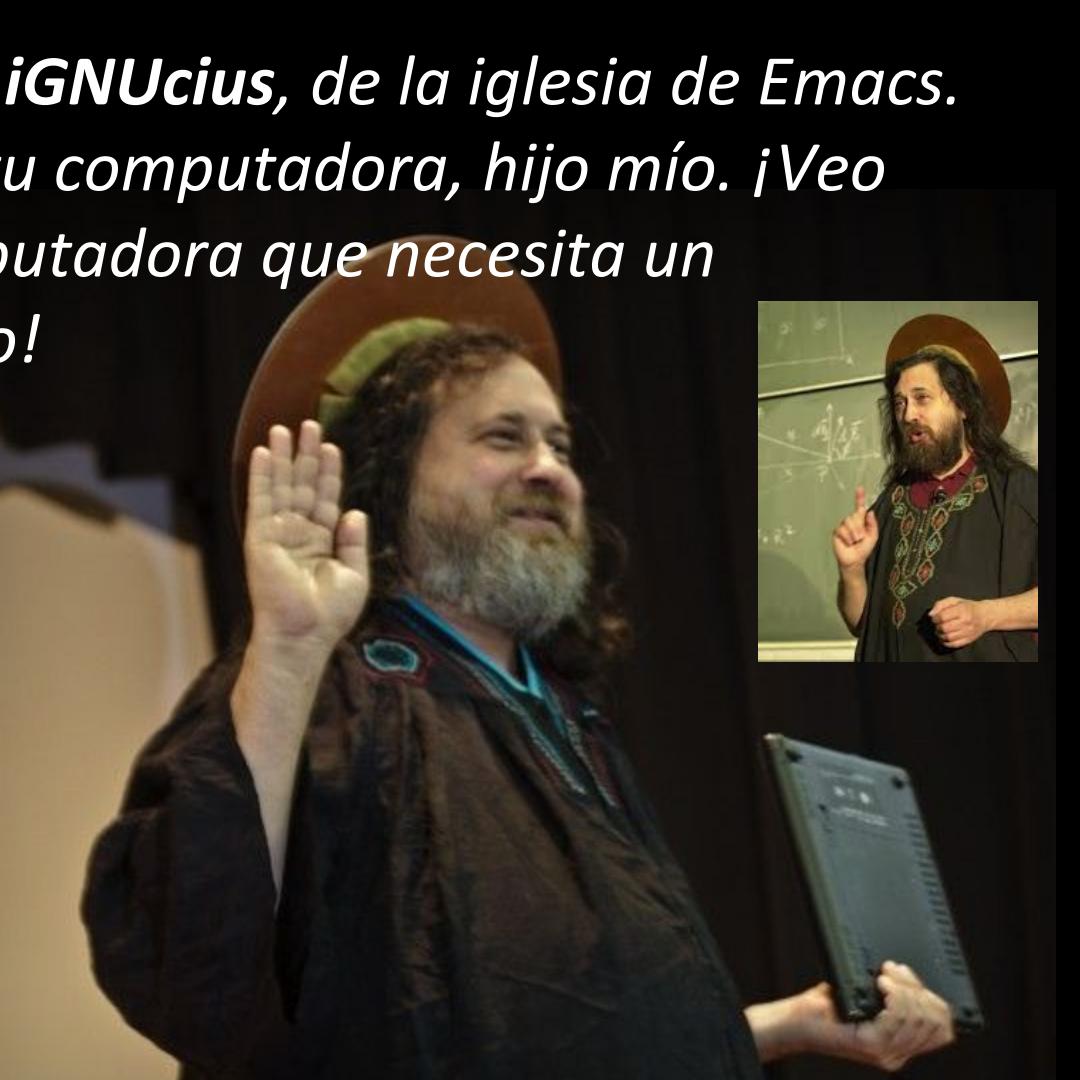


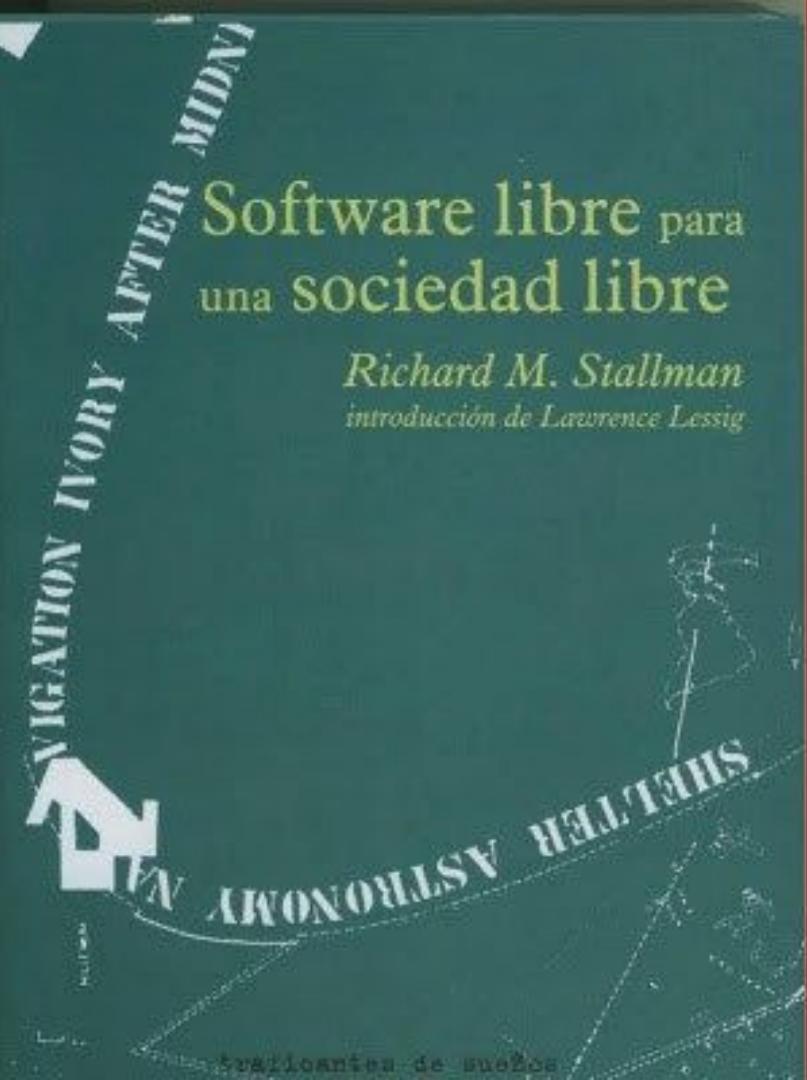






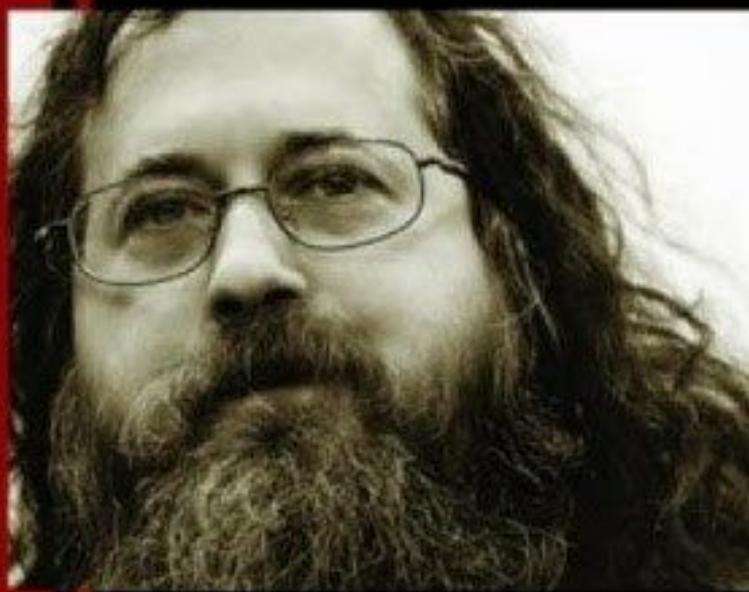
*- Soy **San iGNUcius**, de la iglesia de Emacs.  
Bendigo tu computadora, hijo mío. ¡Veo  
una computadora que necesita un  
exorcismo!*





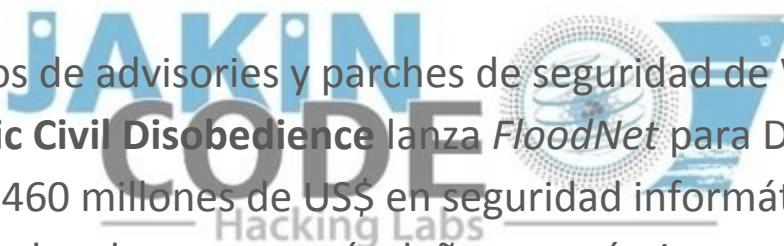
# Free Software, Free Society

Selected Essays of Richard M. Stallman  
Second Edition

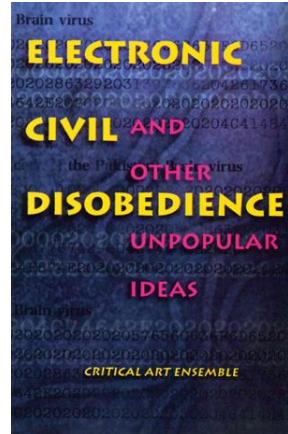


# Perspectiva histórica... Finales de los años 90:

1999:



- Publicación de cientos de advisories y parches de seguridad de Windows.
- El proyecto **Electronic Civil Disobedience** lanza *FloodNet* para DoS.
- Bill Clinton invierte 1460 millones de US\$ en seguridad informática.
- El gusano **Melissa** es el malware que más daños económicos causaba hasta la fecha.
- Sentencia de 5 años contra Kevin Mitnick, 4 de los cuales ya han pasado antes del juicio.
- Level Seven hackea la web de embajada de EEUU en China.
- American Express introduce la **primera tarjeta de crédito basada en chip**.

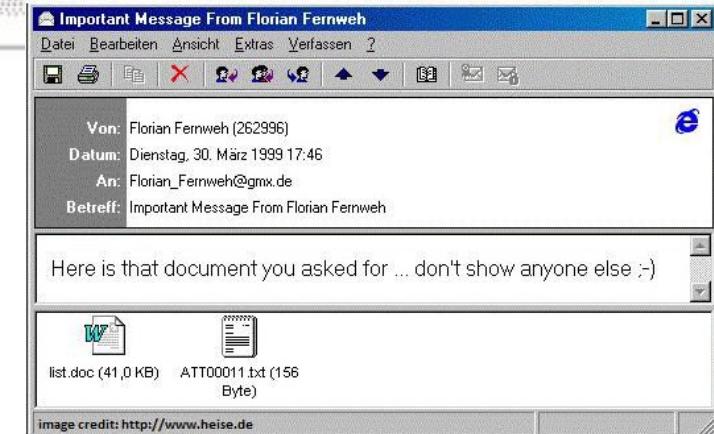


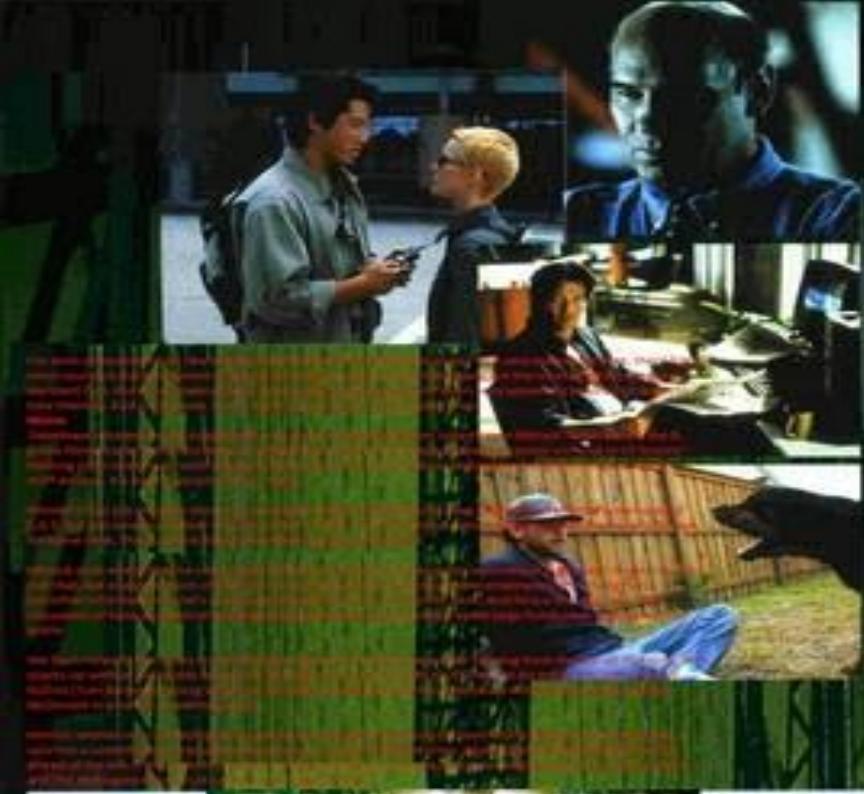
# Perspectiva histórica... Virus Melissa

El FBI busca al autor del virus 'Melissa', que afecta ya a 100.000 ordenadores

JAVIER DEL PINO | Washington | 31 MAR 1999

- El virus **Melissa** es descubierto el 26 de Marzo de 1999.
- Se reenvía a las 50 primeras direcciones de Outlook:
  - Asunto: Mensaje importante de ...
  - Texto: Aquí está el documento que me pediste... no se lo enseñes a nadie ;-)
  - Adjunto: Fichero con extensión .DOC
- Afecta a ficheros de MS Word 87/2000.
- Autor: David L. Smith.
- Pérdidas: 1200 millones de \$.





**TAKEDOWN**

LJUD	AC-3 5.1 CHANNELS	STEREO	MONO	CDS	DOLBY SURROUND
VISU	4:3 FULLSCREEN	LETTERBOX	WIDESCREEN	ANAMORPHIC	16:9 FULLSCREEN
DVD FORMAT	■	■	■	■	HYBRID

■ Visez denne DVD-en i specifikasjonene.

Operation Takedown

Ort. tit.: Takedown

Thriller

108 min.

Ungdomslinje 15 år

© 2000 SCANDOX  
Scandox International - SCANDOX ENTERTAINMENT AS  
Avsættende utgiver: Michael Madsen

DVD CLASSIC

SCANDOX

www.scandox.no  
Tlf. 03 444 70 00

Barcode: 1-00112-33509-6

DVD 5096

**Skeet ULRICH**  
"Scream"

**Russell WONG**  
"Proletian"

**Tom BERENGER**  
"A Murder of Crows"

**TAKEDOWN**

SCANDOX

Boxbuster

DVD VIDEO

The right side of the image shows the back cover of the same DVD case. It features a large, stylized portrait of two men's faces, one above the other, set against a background of green and blue grid patterns. The title "TAKEDOWN" is printed in large, bold, black letters at the bottom. The Scandox logo is visible in the top left corner, and the word "Boxbuster" is in the bottom right corner.



# Perspectiva histórica... Siglo XXI

El 13 de mayo de 2000 el gusano **ILOVEYOU** infecta (50 millones de host) el 10% de internet.

El 11 de febrero de 2001 Jan de Wit crea el virus **Anna Kournikova**.

- Ese mismo año Dmitry Sklyarov es arrestado en la DEFCON por violar la DMCA (*Digital Millennium Copyright Act*).
- El gusano **Code Red** infecta miles de máquinas.



2002: La variante **H** del virus **Klez** se convierte en el virus más infeccioso de la historia.

2003:

- Fundación de la comunidad hacktivista **Anonymous**.
- Autorización de los EEUU para exportar software con cifrado fuerte.



# Perspectiva histórica... Siglo XXI



2004: Corea del Norte afirma contar con un equipo de 500 hackers que han conseguido entrar en sistemas de Corea del Sur, Japón y otros países aliados.



2005: Cameron Lacroix es sentenciado a 11 meses por acceder a la red de T-Mobile y exportar el Sidekick de Paris Hilton.

2006:

- El hacker turco *iSKORPiTX* logra 21549 defacments de golpe.
- *Viodentia* publica *FairUse4WM* para eliminar el DRM de la música WMA.



2007: Estonia sufre DoS masivo. La operación *Bot Roast* del FBI encuentra un millón de víctimas de botnets.

# Perspectiva histórica... Siglo XXI



El 21 de junio de 2007 un **spear phishing** en la oficina del Secretario de Defensa roba datos sensibles de los EEUU obligando a introducir cambios significativos en la identidad y verificación de los mensajes de código.

Ese mismo año, las webs de la ONU, Trend Micro y Kaspersky fueron hackeadas por hackers turcos.

2008: Una veintena de hackers chinos aseguran haber accedido a los lugares más sensibles del mundo, incluído el Pentágono.

Anonymous lanza la operación *Chanology* para atacar los servidores de la Cienciología robando documentación.

# Perspectiva histórica...

- NSA Prism – 2008

El programa Prism promovió un sistema de vigilancia masiva.



A través de la Acta FISA 2008 se hacían peticiones a sistemas de proveedores de servicios de Internet como Google, etc.



- Heartbleed Bug - 2014

Era un bug de SSL y TLS que permitía que permitía robar las claves privadas de los servidores.



La NSA conocía la vulnerabilidad pero nunca la comentó.

# Perspectiva histórica... 2008: Rusia vs Georgia

Atribución:

- Invasión terrestre
- DDoS contra la web del presidente de Georgia: win+love+in+Russia. Inserción de fotos de Hitler
- DDoS y ataques contra prensa, bancos, empresas de Georgia
- Objetivo: Georgia

Más información:

<http://smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf>





# Perspectiva histórica... Siglo XXI

El 4 de abril de 2009 el gusano **Conficker** infecta hosts por todo el mundo, incluyendo máquinas de alta seguridad de muchos gobiernos.

El 23 de junio de 2009 se funda el *Cibercomando de EEUU* con sede en Fort Meade, Maryland.



El 12 de enero de 2010 la operación Aurora Google revela públicamente que Google ha sido objetivo de un ataque altamente sofisticado proveniente de China.

Este mismo año el gusano **Stuxnet** ataca las plantas nucleares iraníes con el objetivo de sabotear las centrifugadoras de enriquecimiento de uranio.

El 28 de noviembre de 2010 **Wikileaks** filtra 251187 cables del Dpto. de Estado de EEUU.



# Perspectiva histórica... - "Spain is different..."

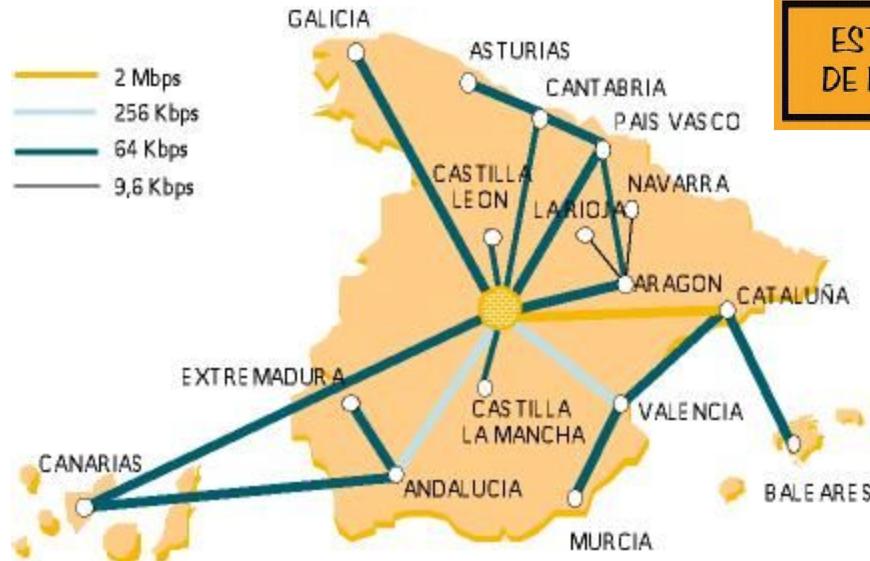




# Perspectiva histórica...

- "Spain is different..."

red Iberpac.



# SEAN VUESAS MERCEDES

Bienvenidas a

# ISLA TORTUGA DEL SIGLO XXI

el espacio libre de Internet



Pulsa en el banner para saber mas...

SOIS LA VISITA

242458

DESDE EL DIA QUE ABRIMOS ESTE CHIRINGUITO  
Y ESO FUE CON EL NUEVO ANO DEL SEÑOR DE 1997  
AL PRINCIPIO DEL MISMO VAMOS.

- POR CIERTO SI QUIERES UN CONTADOR TAN CHULU COMO ESTE VE A [WWW.CONTADEVES.COM](#) -

**CIBERESPACIO**

La empresa informática Vesatec está arruinada a causa de una dudosa actuación judicial. La Policía entró en su local, requisó sus materiales y paralizó su negocio. Aunque una tercera persona se autonómió del presunto delito atribuido a Vesatec, esta empresa aun no ha recuperado sus pertenencias y ha perdido mucho dinero.

**FOLLÓN LEGAL EN INTERNET**

**LA JUSTICIA ARRUINA UNA EMPRESA INFORMÁTICA**

El Juez ordenó la incautación de todos los sistemas informáticos de la empresa, incluyendo sus bases de datos y su software. Los sistemas fueron apoderados por la policía, que los llevó a su cuartel central. La empresa quedó sin acceso a sus sistemas y sin capacidad para realizar sus actividades. Poco a poco, la situación empeoró, ya que la policía no devolvió los sistemas ni permitió a la empresa restaurarlos. Esto llevó a la quiebra de la empresa y a la pérdida de muchos empleos.

Mientras tanto, la policía realizó una serie de audios y videollamadas entre los funcionarios de la empresa y sus clientes. Estos audios y videollamadas fueron utilizados como evidencia en el juicio.

Los funcionarios de la empresa se quejaron de la conducta abusiva y desproporcionada de la policía. Algunos de ellos fueron detenidos y acusados de delitos menores, lo que generó un gran escándalo en la opinión pública. La empresa finalmente logró recuperar sus sistemas y volver a funcionar, pero ya con una imagen dañada y una pérdida económica importante.

Este caso ilustra la importancia de la protección de los sistemas informáticos y la necesidad de establecer procedimientos legales más justos y equitativos para proteger a las empresas y a sus trabajadores.

**LISTAS WAREZ DE PowR**

**SCRIPTS PARA MIRC Y PIRCH**

**CITAS FAMOSAS**

## Indice de las paginas que estan en ISLA TORTUGA DEL SIGLO XXI

TITULO	AUTOR	DESCRIPCION	TIPO	VISITAS	FECHA DE
VIVA EL JAMON Y EL VINO II	Idea Original:FER13 Continuado por: Angelos y Maki Varios Autores	CANTIDAD DE CRACKS PARA PROGRAMAS COMERCIALES Y CANTIDAD DE NIÑAS PRECIOSAS, LIGERITAS DE ESPAÑA. ESTA PAGINA ES ACTUALIZADA POR EL AUTOR CADIA HAY Y ES UNA DE LAS MAS VISITADAS DE ESPAÑA RESPECTO A ESTE TEMA.	C/PN	1178263	23/09/96
JAWER 97	MASK	PAGINA OFICIAL DEL FAMOSO SCRIPT PARA MIRC, TE PERMITE MULTIPLES OPCIONES DE DEFENSA Y ATAQUE	C	37656	02/01/97
VIRTUAL SENTINEL	BOB-T	DECENAS DE LINKS A SITES EN INGLES SOBRE IRUP/CV Y UTILIDADES PARA LO MISMO	H/P/C/V	Inaccesible	02/01/97
MARUJONA	MAKI ANGELOS	PAGINA PARA DENUNCIAR LAS CALUMNIAS QUE SE LANZAN CONTRA INTERNET	R	22682	10/12/96
TARIFA PLANA	JONI HERBEROS MANUEL VINAGRE	PAGINA PARA RECLAMAR UNA TARIFA PLANA PARA INFOMA	R	43171	01/01/97
EMULADORES	ROGER	PAGINA DEDICADA A LOS EMULADORES DE ORDENADORES Y CONSolas	H	8	01/01/97
VIEJA GUARDIA	Vieja Guardia	PAGINA OFICIAL DE ESTE GRUPO DE HACKERS	H/P/C/V	5201	01/01/97
DARKSIDE	Rage 666	PAGINA OFICIAL DE ESTE GRUPO DE HACKERS	H/P/C/V	24413	22/02/97
MAILOBSCURO.ES	Malobscuro	EL WEB DEL CORRINO ANONIMO EN CASTELLANO	H	Inaccesible	12/03/97
QENDA	Qenda	PAGINA PERSONAL DE ESTE CONOCIDO NAVIGANTE	H/C	2	12/03/97
MAFIA MAGAZINE	Juanam	Cracks Script para IRC El crack del mundo Cheat codes Tables y otras cosas revolucionarias Manual del Cracker	H/C/V/R	1441	02/04/97
29A MAGAZINE	Mister Sandman	Página oficial del grupo de creadores de virus 29A	V	9311	15/04/97
DESCODIFICADOR DE SONIDO DE CANAL+ COMPANY OF PREAKING NACIONAL DE ESPAÑA	Eduardo Magaña	Página del descodificador de sonido de Canal +	H	8743	02/04/97
PAGINA DE APOYO A LOS OKUPAS DEL CINE PRINCESA	Maestri	Página para defender el derecho a la vivienda frente a la especulación inmobiliaria	H	Inaccesible	23/03/97
PAGINA OFICIAL DE RUIZ MATEOS	Ruiz Mateos	Desde se explica sobre el caso Ruano	H	Inaccesible	23/03/97
PAGINA DEL SALTEADOR DE LA WEB	Salteador	Página donde se muestra como la DGA tan valiente a la hora de patear puertas empresas como Vesatec, no se atreve a tocar a los contratos oficiales	H	Inaccesible	13/06/97
PAGINA DEL PADRE APILES	Okiode	Página (no oficial) sobre el Padre Apiles, el cura de las Iles; un personaje tan conocido como polémico	H/C	Inaccesible	19/06/97
PAGINA DE SICOTIC MAGAZINE	Big Brother	Página oficial de este grupo de hackers	H/C/PN	17906	20/06/97
PAGINA DEL CANAL #WAREZ DEL IRC HISPANO	#Warez IRC Hispano	Página del canal warez del IRC Hispano	H	Inaccesible	23/06/97
LA TABERNA DE VAN HACKEZ	Van Hackez	Página de este conocido hacker	H/C/V	23/06/97	
UNDERHACK	Schoddy Guy	Página de este conocido grupo	H/C/V	50011	23/06/97
PAGINA DE OCULTISMO	Yakomo	Comparte páginas sobre temas de ocultismo Crédito por uno de los autores del Mafia Magazine	Otros	Inaccesible	13/08/97
EL MUNDO DEL VALHALLA	Fco 97.	Famosas páginas sobre los temas que ocupan en la Isla	H/P/C/V	Inaccesible	13/08/97
SPANISH WEB HACK	ArctiSPH	Página Anti-HSA 100%, incluye todos los temas incluidos en la Isla y además una completa lista de LAMERS	H/P/C/V	5823	13/08/97
CALIMOTXO NEWS	Arlekin	Completo直到现在关于什么是黑客的所有东西,从简单的,到复杂的,不同的.	CH	2120	13/08/97
CIBERHACK FANZINE	Cyberhcky	Revista especializada en HACK	H/C	Inaccesible	13/08/97
PAGINA DEL SECRET TEXTURE	Mask	Patente script para Mirc en Castellano	C	1861	13/08/97
RECLAMAR A TELEFONICA	Albertor	Cómo Reclamar (Si eres Precio igual te confundes con defraudador) a la telefonera Timofonica	R	735	13/08/97
POWR'S LAIR	PowR	Página muy completa sobre las actividades de la Isla	H/P/C/V	Inaccesible	20/08/97
LISTAS WAREZ DE PowR	PowR	Las últimas listas warez actualizadas cada dia	W	Inaccesible	01/09/97
SCRIPTS PARA MIRC Y PIRCH	Dakkon	Todos los scripts para Mirc y PIRCH	C	Inaccesible	07/09/97
CITAS FAMOSAS	PowR	Citas de Chico de veraneo famosas Por una vez podías cultivar tu amor, my... CH	C/H	Inaccesible	07/09/97

### LEYENDAS DEL CAMPO TIPO

- H HACKING, sobre los servicios e interacciones de los sistemas informáticos
- C Como descubrirlos y como sacarlos provecho
- P Como engañarlos y como protegerte contra los engaños
- C/CRACKING, sobre los ataques debiles de los sistemas informáticos
- S Scripts, sobre los programas que realizan tareas sencillas
- V VIURSES, sobre temas de virus, como hacerlos y como protegerse de los mismos
- PORNOGRAFICAS, páginas con un contenido altamente sexualizado
- PS peligroso para niños, míticos del open y demás
- C/CACHONDIA, páginas cuyo contenido puede provocar serios trastornos de salud a causa del ataque de risa

## Invasiones en ordenadores de América y Asia

El pasado 2 de marzo, 24 de los 25 centros informáticos de la central de Washington, sede de la NASA, sufrieron ataques de hackers. En aquella ocasión no se produjeron pérdidas. Los sistemas afectados funcionaban con Windows NT o Windows 95.

Para penetrar el sistema, los hackers usaron las técnicas conocidas como newtow, booby y bomb. Algunas de ellas se componían simplemente de reiniciar el ordenador. Al parecer, esta acción fue una respuesta por la detención de un grupo de hackers que pretendían obtener acceso a varios máquinas del Gobierno de EEUU que contenían información confidencial.

Simpaticantes del Ejército Zapatista de Liberación Nacional EZLN protestan en Internet contra el presidente del Movimiento de Hacienda de México. Haciendistas manejaron rebeldes en la web de la Secretaría de Hacienda y Crédito Público. El ataque fue motivado por un grupo de piratas informáticos llamados "Liber". Los que atacaron pretendían al EZLN, establecer otras fuentes seguras de vinculación con el movimiento zapatista. El grupo reemplazó la página con imágenes del hemiciclo de la revolución mexicana de 1910. Además, Zapatistas y maestros del sur protestaron contra Marcos. La mayoría se prolongó durante toda la noche del 3 de abril.

En Japón, un grupo de piratas accedió en enero a los datos de clientes de un banco, pero no a sus cuentas. Los cibercriminales se apropiaron de la información durante una feria por las dependencias, viéndoseles de la entrada.

### EZA Barcelona

Ángel Badía, Argemiro y Francisco Salvador Montesquiu. Maki son los tres de la informática y el ordenador. Su actividad y trabajo es la lucha contra la explotación. Se siguen las páginas <http://www.islatortuga.com> (en uno de los más visitados). A través de sus enlaces distribuyen una página no controlada por ellos, denominada Viva el jamón y el vino. "Es una persecución, Somos inocentes", aseguran los dos informáticos, que han denunciado la expulsión de uno de sus sitios. Maki y Argemiro difieren y un proceso para lo siguiente en

paralelo se han iniciado en las facultades de Informática. Hace poco más de un mes, Argemiro y Francisco fueron detenidos y se les imputó el delito de intrusión en los ordenadores de la universidad.



Maki (queriendo) y Argemiro continúan con su página presente en Internet.

# Jamón, vino y Timofónica

'Webs' de protesta contra Telefónica llevan al juzgado a varios internautas

un lugar de la red y la propia abr. Así se abrieron las horas de ye ya he gastado en buscar barrios jamón".

Argemiro y Maki comparten el primer aniversario de su actividad el pasado 27 de mayo. "nos invadieron ordenadores y nos dejaron en la miseria", ponían en su Carta abierta. "Nosotros, sin embargo, no controlamos la página, sino que fue otra persona que solo declarante ante el juez. Lo que hacemos es legal", señalan los dos jóvenes, a los que ya obligado, el perniciosa Manuel Arias.

La policía, dentro el 6 de marzo en Barcelona (Gujar) y en Leganés, Madrid a Juan Antonio M. R., de 33 años, y Albert R. de 27, enmarcado con este asunto. En una nota oficial, se reconoce que se ha investigado a Francisco Salvador Montesquiu. Maki, que sigue en libertad, "era ajeno a los numerosos hechos detectados".

A pesar de todo, Argemiro y Maki están

## LA TERMINOLOGÍA

### Una jerga para la comunicación entre iniciados

Los hackers tienen una serie de términos para comunicarse entre ellos. Es como un diccionario, con conceptos como estos:

► BUG. Defecto de sistema. Un bug es un fallo del disco duro de un sistema que sus creadores no han detectado. Puede producirse por errores en una fórmula matemática o por un defecto en la forma de leer y tratar la información que se recibe. Consecuencias: errores de contabilidad y acceso a información restringida.

► EXPLOIT. Programa que utiliza un bug para provocar determinados efectos, como conseguir información privada mediante un servidor dañado electrónico.

► WAREZ. Término que define la recepción de intercambio de software comercial sin comprar y sin pagar derechos de autor.

► GAMEZ. Warez de videojuegos.

► HACKER. Tradicionalmente se considera hacker al aficionado a la informática cuya afición es buscar defectos y pueras traseras para entrar en los sistemas. Por extensión, la definición correcta sería: experto que puede conseguir de un sistema informático cosas que sus creadores no imaginan.

► CRACKER. Hacker cuya ocupación es buscar la forma de romper sistemas y las bolas de seguridad de programas.

► PHREAKER. Hacker especializado en telefonía. Su propósito es reducir al máximo su factura de teléfono por el procedimiento de robar y utilizar cualquier truco que le permita rea-

Dos personas fueron apresadas en Cádiz y otra en Asturias — Los agentes afirman que de la Nasa y de la Universidad de Oxford — Uno de los detenidos asegura que

## Hispahack: tres «cerebros» en la cárcel

*La Guardia Civil detiene a tres «intrusos» informáticos españoles e impone a otros diez*

MIREIA DRAGO

MADRID — Tresen 21, 22 y 26 años. Entre el miércoles y el jueves fueron detenidos por invadir los sistemas informáticos de la Nasa, de la Universidad de Oxford y de diversos centros españoles. Forman

una manada en incursiones ilegales en sistemas informáticos y en daños a proveedores de Internet, si bien la Guardia Civil, hasta ahora, sólo admite que han resultado pruebas contra los tres detenidos.

El teniente Amador del Moral cuenta que la investigación partió de la denuncia de un proveedor de



### La «red Hispahack»

Dos expertos en informática operaban desde Gibraltar, otro desde un pueblo asturiano y otra docena de personas desde distintas localidades de Cataluña.

► **Definición de «hacker»:** Gran aficionado a la informática, que accede a sistemas de ordenadores ajenos sin ánimo de lucro.

# Cuatro piratas españoles burlan el control de la NASA y acceden a su red informática

## SUCESOS

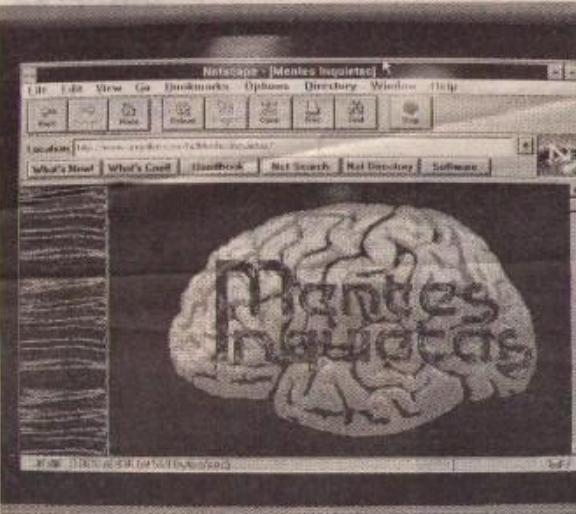
■ Tres de los detenidos son de Barcelona. El mayor no supera los 26 años. La Guardia Civil los considera unos genios

CARLOS NOVO  
DOMINGO MARCHEÑA

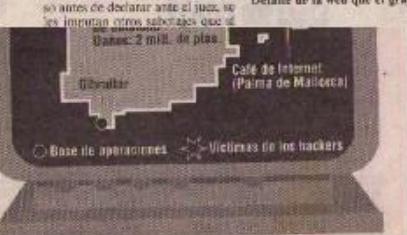
BARCELONA — El grupo español Os Resistentes tiene una canción titulada "Hay un hacker en la Luna". Si quieren, podrían cantar también "Hay un pirata español en la NASA". Hasta ahora, películas como "Jugos de guerra" o "La red", con genios capaces de robar los sistemas informáticos —supuestamente— más seguros del mundo, tenían protagonistas angloajunas. Dentro de poco, podrán ser latinos. El próximo viernes, va bien. La Guardia Civil ha detenido a cuatro jóvenes vascos de los ordenadores, de entre 18 y 26 años, acusados de acceder a la red informática de la agencia espacial estadounidense.

No hay constancia de que esa acción causara el más mínimo daño, pero a los acusados, que quedaron en libertad sin embargo, algunos incluso antes de declarar ante el juez, se les imputan otros delitos que sí lo hacen: 2 mil 2 plazas.

Entre los detenidos figura un menor de edad, que ya ha sido puesto en libertad. La Guardia Civil ha detenido a otros diez jóvenes, entre ellos un menor de edad, que permanecen en prisión. Los acusados pertenecen a un grupo que se considera la banda de hackers más activa de Europa.



Detalle de la web que el grupo Mejores Inquietos tenía en la red



pensad en las consecuencias". Pero más adelante se dan recomendaciones en caso de ser sorprendidos por la policía: "Nunca estés de más con tu presencia. Los consejos porque aunque no nos guste, algún día los piaremos necesitar".

Las detenciones se practicaron en la localidad barcelonesa de Sant Joan Despí, donde se detuvo a un joven de 18 años, el presunto autor material de los hechos mantenidos en la UPC; en la Línea de la Concepción (Cádiz) fueron detenidos jóvenes de 21 y 22 años, ambos naturales de Mataró; también de Barcelona, y la imbatible banda de una empresa informática de Gijón, la cuarta detención, la de un profesor de informática de 26 años, se produjo en Avilés (Asturias). Los in-

vestigadores, que han contado con ayuda de guardias civiles de las ciudades citadas, han localizado un importante número interno de la red, gracias a la Guardia Civil, ya que se trataba de un codiciloso frío en el que residía en Lyon. Otras policías, como New Scotland Yard o el FBI han participado en las pesquisas.

Según la Guardia Civil, "algunos de los ataques realizados a sistemas informáticos utilizados en España fueron realizados desde aquí, poniendo en la red de ordenadores conectados a Internet que estaban en Ho-

mIRC - [Urls List [urls.ini]]

File View Favorites Tools Commands Window Help

Join channel Part channel Query user Send notice Whois user Send CTCP Set Away Invite user

Barcelona Urls List

News

Lunes, 1 de junio de 1998 el Periódico

2 TEMA DEL DÍA

Intrusos en la red Tema del día

Vacio legal

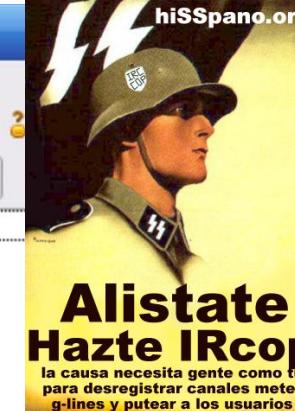
Abergados y jueces consideran que todavía existe un vacío legal en España para perseguir algunos delitos específicos que pueden cometerse a través de Internet.

## Los 'ciberpiratas' españoles se cuelan en la NASA y el Pentágono

Un estudiante de la Politécnica entró en un satélite y movió sus placas solares

Otro 'hacker' manipuló el simulador de guerra atómica de Estados Unidos

Los saboteadores han espiado a importantes proveedores de Internet



—En Barcelona, siendo las 16:30 horas del 25 de Marzo de 1.998, el Instructor de las presentes hace constar el siguiente informe a SS:

—Con fecha de 2 de noviembre de 1.997 se recibió en la sede de este grupo de delincuencia informática en Madrid un mensaje de correo electrónico a través de Internet, en el cual se adjuntaba la dirección de Internet donde podían verse diversas fotografías de los miembros de un grupo de "hackers" o intrusos informáticos que se autodenominan HISPAHACK, los cuales al parecer habían accedido de forma ilegal al ordenador del Congreso de los Diputados en Madrid.

—Puestos en contacto con el responsable técnico de dicho ordenador, éste confirmó los hechos, manifestando que, él o los atacantes habían modificado diversa información firmando los autores del acceso no autorizado como !HISPAHACK o !HISPAHACK. Dicha persona, tras ser informada de la posibilidad de denunciar los hechos, participó que estudiaría las posibles acciones legales y en caso de querer denunciar se pondría en contacto con esta Unidad, no habiéndose producido tal circunstancia hasta el día de la fecha.





www.internautas.org

**InfoVírria**

LA GRAN VÍRRIA DE ACCESO A LOS  
CAMINOS DE CABRAS DE LA  
INFORMACIÓN



Telefónica

**Timofónica**



# Perspectiva histórica... Siglo XXI

Gürtel (2009):

- La investigación iniciada en noviembre de 2007 por la **Fiscalía Anticorrupción** y denunciada en febrero de 2009 ante la Audiencia Nacional, sobre una red de corrupción política vinculada al **Partido Popular**, que funcionaba principalmente en las comunidades de Madrid y Valencia.
- La trama estaba encabezada por el empresario **Francisco Correa Sánchez**, cuyo apellido Correa en alemán dio nombre al caso. Se abrió el caso tras la denuncia realizada por el exconcejal de Majadahonda José Luis Peñas.

LAS CONVERSACIONES MÁS GOLPAS DE LA GÜRTEL

“¿Has follado en Colombia?”  
INTERVÍU ACCDE A LAS GRABACIONES ORIGINALES DE LAS ESCUCHAS TELEFÓNICAS MÁS IMPORTANTES DEL CASO, INCLUIDAS LAS MÁS FRIVOLAS

“Si, dos veces”

El primer de los tres episodios de la serie 'Gürtel' combina un sexito con una vida de jogos caro, en la que no faltan fastidios viajes y amores exóticos. Las conversaciones más golpas de la Gürtel tienen acceso íntimo, dan una perfecta idea de la dulce vita de Correa y sus hijos.

“Tengo una buena vida... LAS GRACIOSAS”

Playas y montañas

Correa y su familia se pasan las vacaciones en la playa. Allí se conocen las relaciones más íntimas entre los miembros de la familia, así como las peleas y los momentos de risa. Los amigos y las relaciones profesionales también juegan un papel importante en la vida de Correa.





# Perspectiva histórica... Siglo XXI

WikiLeaks (2010):

- En julio de 2010, la organización WikiLeaks envió al New York Times, The Guardian y Der Spiegel más de 91.000 documentos secretos relacionados con la participación militar EE.UU. en Afganistán.
- Los documentos revelaron que el conflicto había sido mucho más sangriento y costoso de lo inicialmente planteado. En él se detallaban numerosos casos de bajas civiles y de fuego amigo, así como pruebas de que la agencia de inteligencia de Pakistán había ayudado a los Talibán.



# Perspectiva histórica... 2010: Ataque a Baidu

Atribución:

- 4 horas caído. *Iranian Cyber Army*.  
Registros DNS.
- 2009 Twitter. Registros DNS.

Más información:

<http://www.telegraph.co.uk/technology/news/6974129/Baidu-hacked-by-Iranian-Cyber-Army.html>

Counter Craft



# Perspectiva histórica... 2010: Stuxnet



A.B.C  
El «gusano» Stuxnet ataca el sistema Scada, el software habitual en oleoductos y plantas nucleares

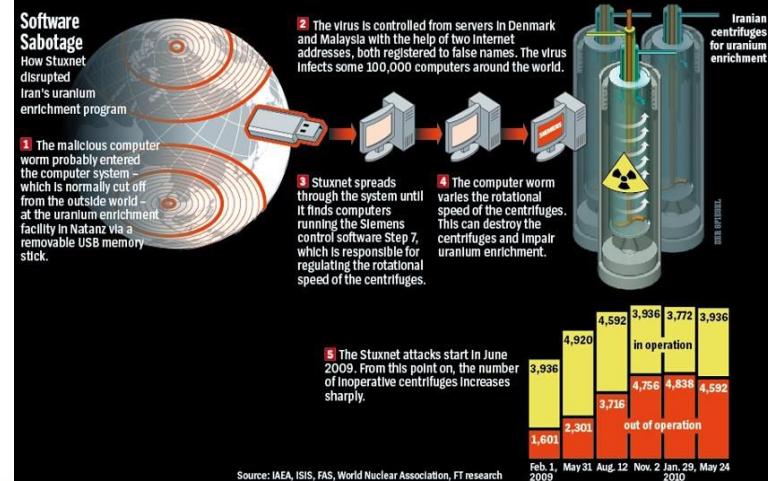
- Primer virus conocido que espía y reprograma sistemas industriales SCADA.
- Objetivo PLCs de Siemens para sabotear las centrifugadoras de enriquecimiento de uranio.
- Detectado el 17 de Junio de 2010 en la planta nuclear de Bushehr.
- Primera infección por memoria USB y posterior propagación a través de la red.
- Empleó un total de 4 vulnerabilidades de día cero.
- Primer gusano en incluir un rootkit.
- Hasta la fecha fue el malware más sofisticado del mundo.



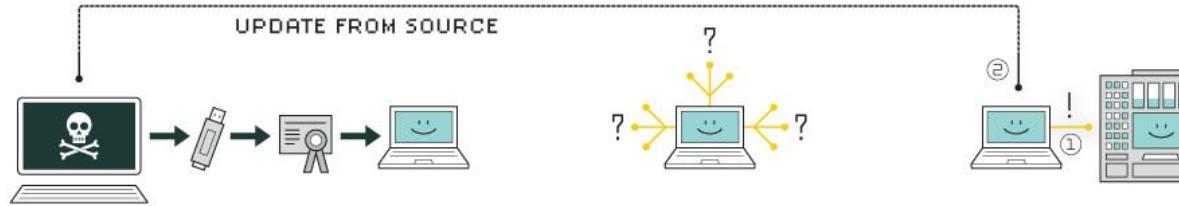
<https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet>

# Perspectiva histórica... 2010: Stuxnet

- Sólo funciona en dispositivos Siemens S7-300 y S7-400.
- Interviene las órdenes enviadas desde un sistema Siemens SimaticWinCC SCADA a un variador de frecuencia, y las modifica para alterar las velocidades del motor para que varíe de forma descontrolada en diferentes momentos.
- Sólo ataca a las centrifugadoras si funcionan entre los 870 y 1210 Hz.
- Al afectar la velocidad de los variadores de frecuencia, se sabotea el proceso de enriquecimiento dando como resultado un uranio de mala calidad.
- Unos investigadores infectaron un sistema conectado a una bomba de aire con un globo programado para funcionar por 3 segundos, pero Stuxnet lo prolongó hasta los 140 segundos.



# Perspectiva histórica... 2010: Stuxnet



## 1. infection

Stuxnet enters a system via a USB stick and proceeds to infect all machines running Microsoft Windows. By brandishing a digital certificate that seems to show that it comes from a reliable company, the worm is able to evade automated-detection systems.

## 2. search

Stuxnet then checks whether a given machine is part of the targeted industrial control system made by Siemens. Such systems are deployed in Iran to run high-speed centrifuges that help to enrich nuclear fuel.

## 3. update

If the system isn't a target, Stuxnet does nothing; if it is, the worm attempts to access the Internet and download a more recent version of itself.



## 4. compromise

The worm then compromises the target system's logic controllers, exploiting "zero day" vulnerabilities—software weaknesses that haven't been identified by security experts.



## 5. control

In the beginning, Stuxnet spies on the operations of the targeted system. Then it uses the information it has gathered to take control of the centrifuges, making them spin themselves to failure.



## 6. deceive and destroy

Meanwhile, it provides false feedback to outside controllers, ensuring that they won't know what's going wrong until it's too late to do anything about it.

# Perspectiva histórica... 2010: Stuxnet

Atribución técnica:

- Cadena MYRTUS-> My RTUs vs Myrtus -> Hadassah en hebreo, nombre de la Reina judía de Persia
- b:\myrtus\src\objfre\_w2k\_x86\i386\guava.pdb
- Cifrado 19790509 -> Habib Elghanian, un judío persa, fue ejecutado en Tehran
- Cadena 24 sep 2007 -> Presidente de Irán cuestiona el Holocausto en EEUU
- Multitud de declaraciones de ser una operación conjunta de EEUU + Israel

CounterCraft

Atribución:

- Objetivo: Programa nuclear de Irán

<http://www.goodreads.com/book/show/18465875-countdown-to-zero-day>





# Perspectiva histórica... Siglo XXI

2011:

- Fundación del grupo **Lulz Security**, obteniendo más de 1 millón de cuentas de usuario sony en un ataque contra PlayStation Network, y comprometiendo ordenadores del Senado de EEUU.
- Detección de **Duqu** (software con tecnología similar a Stuxnet, pero dedicado al robo de información) en sistemas industriales europeos.



2012: Detección de **Flame** en oriente medio, cuyo objetivo es rastrear de forma secreta redes de Irán y obtener control en ordenadores de funcionarios iraníes.

El 19 de febrero de 2013 el Ministerio de Defensa promulga la orden 10/2013 para la creación del *Mando Conjunto de Ciberdefensa de las Fuerzas Armadas*.

# Perspectiva histórica... Siglo XXI

15 de Agosto de 2012:

Caso: Saudi Aramco



# Perspectiva histórica... 2012: Shamoon

False Flags:

- C:\Shamoon\ArabianGulf\wiper\release\wiper.pdb
- Irán lo llama Persian Gulf
- 15 de agosto: Lailat al Qadr (la noche del poder – celebra la revelación del Corán a Mahoma)
- Wiping a las 11:08am
- El nombre Wiper se usaba también en Flame (ataque a empresas de petróleo de Irán)
- Ataque similar contra RasGas 2 semanas después (Qatar)
- Objetivo: Arabia Saudí – Saudi Aramco

<http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html>





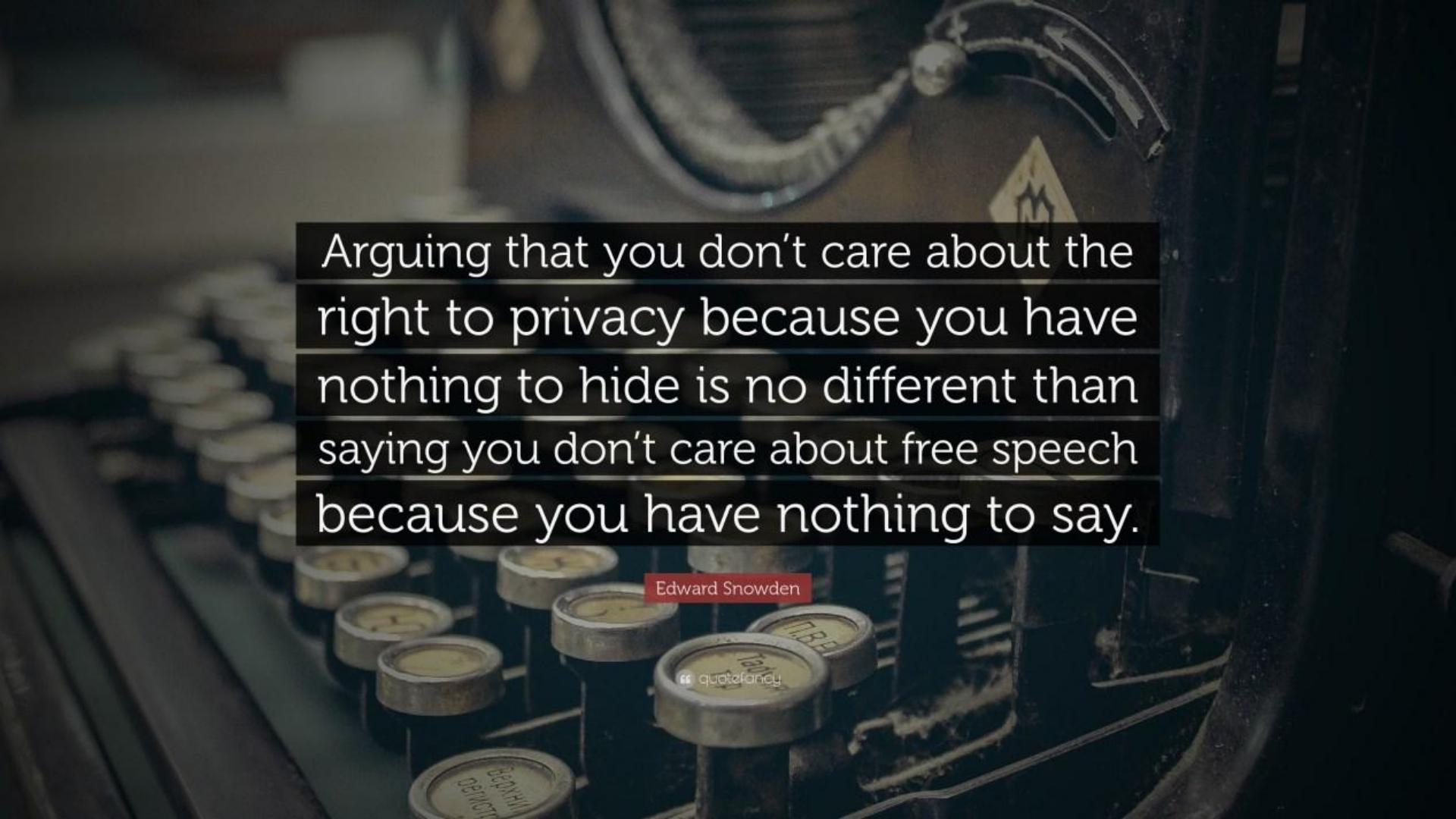
# Perspectiva histórica... Siglo XXI



Los secretos de la NSA (2013):

- A principios de junio, The Guardian y The Washington Post publicaron historias sobre la NSA sobre pinchazos en secreto en millones de llamadas telefónicas y comunicaciones por Internet.
- La información se filtró por **Edward Snowden**, de 29 años de edad, contratista de la NSA, que reveló su identidad diciendo que se sintió obligado a hablar sobre lo que llamó "mala conducta".





Arguing that you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say.

Edward Snowden

quotefancy

# Perspectiva histórica... 2013: Red October

Atribución:

- Idioma cirílico
- Cadenas en slang ruso dentro de los binarios
- Utilización de direcciones de e-mail rusos
- Servidores en Rusia, Alemania (Hetzner)
- Registros de dominios en reg.ru, webdrive.ru, webnames.ru, timeweb.ru
- Objetivo: Europa del Este, Asia, antigua URSS, embajadas

# CounterCraft



<https://securelist.com/red-october-diplomatic-cyber-attacks-investigation/36740/>

# Perspectiva histórica... 2013: APT1/Comment Crew

Atribución:

- Identificación de personas: UglyGorilla, DOTA, SuperHard. Estudiantes universitarios.  
Reutilización de nicknames.
- Reutilización de dominios, Ips, direcciones de email
- Número de teléfono real a 600 metros del HQ de la Unit 61398 (habitación en alquiler)
- Lunes a viernes de 8am a 6pm en UTC+4
- Objetivo: EEUU

<https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf>



# Perspectiva histórica... 2013: Corea del Norte vs Corea del Sur

Atribución:

- Dark Seoul
- 20 de marzo a las 2pm: Wiping MBR en varias TVs y bancos. Palabras en MBR: Príncipes y Hastati (infantería romana). Ataques al BGP de esas empresas
- 1 semana antes: Corea del Norte estuvo 36 horas sin Internet
- 25 de junio: 63º aniversario de la guerra de Corea
- DDoS contra gobierno de Corea del Sur
- Objetivo: Corea del Sur



<https://arstechnica.com/security/2013/03/your-hard-drive-will-self-destruct-at-2pm-inside-the-south-korean-cyber-attack/>

# Perspectiva histórica... Lazarus Group (2007-\*)

Atribución:

- Código compartido con otros incidentes.
- Infraestructura reutilizada en otros incidentes.
- Utilización de alguna dirección IP de Corea del Norte en accesos a C2C.
- Objetivos: Corea del Sur, entidades financieras.

# CounterCraft



[https://securelist.com/files/2017/04/Lazarus\\_Under\\_The\\_Hood\\_PDF\\_final.pdf](https://securelist.com/files/2017/04/Lazarus_Under_The_Hood_PDF_final.pdf)

<https://www.operationblockbuster.com/wpcontent/uploads/2016/02/Operation-Blockbuster-Report.pdf>

# Perspectiva histórica... Siglo XXI

## Tarjetas "black" (2013):

- El caso de las tarjetas black saltó a la luz en diciembre de 2013, por el cual se desveló que la práctica totalidad de los consejeros de Caja Madrid, posteriormente Bankia, durante al menos las presidencias de **Miguel Blesa** y **Rodrigo Rato**, habían dispuesto de una tarjeta de crédito del tipo "Visa Black" otorgada por la entidad con la que habían llevado a cabo durante años cargos personales valorados en cientos de miles de euros con cargo a las cuentas de la caja de ahorros, y presumiblemente, sin declarar a Hacienda ninguno de ellos.



Elaboración: Belén Picazo y Alejandro Navarro

Fecha	Hora	Nombre	Descripción actividades	Nombre comercio	Importe
14/02/2003	19.34.50	Mariano Pérez Claver	TARJETAS ALQUILERES	IGAR DE LA CONCHA	6.000,00 €
04/04/2003	17.58.39	Ramón Ferraz Ricarte	AGENCIAS DE VIAJES	VIAJES HESPERIA, S.A.	5.998,36 €
29/04/2003	15.46.55	Carlos María Martínez Martínez	VIAJES BARCELÓ	VIAJES BARCELÓ S.L.	4.022,64 €
08/05/2003	12.39.58	Ricardo Morado Iglesias	AGENCIAS BANCARIAS/(ANTICIPO VENTANILLA)		4.000,00 €
29/07/2003	14.14.58	Carmen Contreras Gómez	EL CORTE INGLÉS	VIAJES ECI	3.441,22 €
31/07/2003	15.34.42	Juan Manuel Astorgui Portera	AUTOM / MOTOCICLETAS (VENTAS Y REPARAC)	NAUTICA BAUTISTA	3.836,42 €
05/08/2003	13.39.60	Ricardo Morado Iglesias	AGENCIAS BANCARIAS/(ANTICIPO VENTANILLA)		3.500,00 €
	15.33.40	Carlos Vela García	LÍNEAS AÉREAS	TIKAL VIAJES	6.052,10 €
29/08/2003	15.35.15	Maria Elena Gil García	JOYERAS Y RELOJERIAS	JOYERA SUAREZ	6.000,00 €
24/10/2003	13.53.46	Juan Manuel Astorgui Portera	Costes mensual	SALA RETIRO CAJA DE MADRID	4.050,15 €
22/12/2003	09.58.32	Ildefonso José Sánchez Bacoj	AGENCIAS BANCARIAS/(ANTICIPO VENTANILLA)		5.450,00 €
24/12/2003	09.14.50	Enrique de la Torre Martínez	AGENCIAS BANCARIAS/(ANTICIPO VENTANILLA)		5.000,00 €
29/12/2003	15.33.00	Carlos Vela García	JOYERAS Y RELOJERIAS	JOYERA SUAREZ	4.090,00 €
09/01/2004	12.40.28	Ildefonso José Sánchez Bacoj	AGENCIAS DE VIAJES	VIAJES TIKAL S.A.	5.293,34 €
	18.45.04	Juan Manuel Astorgui Portera	CONFECION TEXTIL NIVEL 2	YVES SAINT LAURENT	3.535,00 €
31/03/2004	15.36.55	Maria Elena Gil García	JOYERAS Y RELOJERIAS		6.905,72 €
26/05/2004	10.38.56	Maria Elena Gil García	AGENCIAS BANCARIAS/(ANTICIPO VENTANILLA)		8.000,00 €
16/08/2004	11.08.49	Carmen Contreras Gómez	HOTELES 4 Y 5 ESTRELLAS,BALNEARIOS,CAMP	HOTEL BARROS PARK	6.299,24 €
19/10/2004	14.04.37	Mariano Pérez Claver	AGENCIAS DE VIAJES	MILLAN TRAVEL SA	6.000,00 €
07/12/2004	09.47.23	Enrique de la Torre Martínez	AGENCIAS BANCARIAS/(ANTICIPO VENTANILLA)		5.390,00 €
17/12/2004	08.17.03	Enrique de la Torre Martínez	AGENCIAS BANCARIAS/(ANTICIPO VENTANILLA)		0.577,00 €
10/03/2005	14.28.38	Carmen Contreras Gómez	EL CORTE INGLÉS	VIAJES ECI	5.626,00 €
12/03/2005	12.53.11	Mariano Pérez Claver	FERRETERIA,BRICOLAJE,MENAJE DEL HOGAR	LUZ & AMBIENTE	3.500,00 €
29/03/2005	16.05.36	Miguel Blesa de la Parra	HOTELES 4 Y 5 ESTRELLAS,BALNEARIOS,CAMP		5.574,25 €
14/04/2005	15.23.50	Carlos Vela García	LÍNEAS AÉREAS	TIKAL VIAJES	3.483,20 €

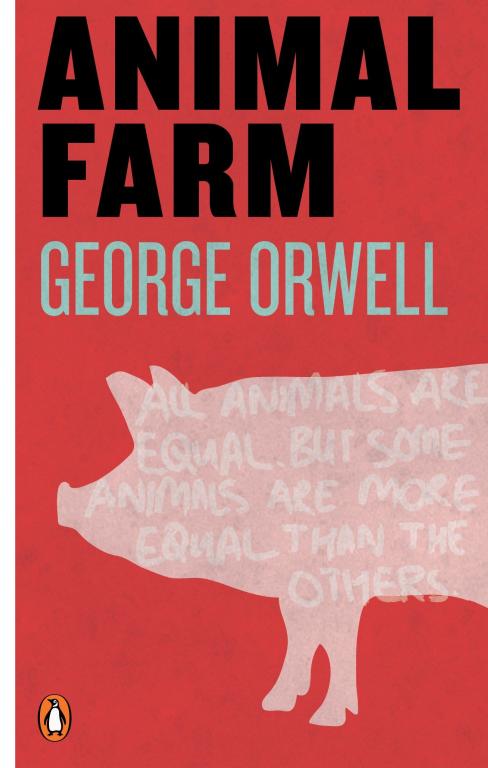
eldiario.es

# Perspectiva histórica... 2014: Animal Farm

Atribución:

- Tafacalou -> nombre interno del 1st stage.
- Babar
- Nombre del desarrollador: titi (diminutivo de Thiery)
- Idioma de la parte servidora 'fr\_FR'
- Inglés extraño
- Zonas horarias de compilación GMT+2 o GMT+3
- Buen inglés pero fallos de no nativos: Exceeded
- Objetivo: Siria

Counter Craft



<https://www.gdatasoftware.com/blog/2015/02/24270-babar-espionage-software-finally-found-and-put-under-the-microscope>

# Perspectiva histórica... 2014: Rocket Kitten



Atribución:

- Dominios registrados por grupos que se dedicaban al defacement (Ajax Security Team).
- Gholee (nombre de función exportada) es un cantante famoso de Irán.
- Cadena: 'bos bos'. Boos es beso en iraní, con lo que pudiera ser xoxo.
- Wool3n.H4T es un usuario de un blog iraní.
- Logs del autor que estaba infectado con su keylogger. Se conecta a AOL con el usuario 'yaserbalaghi'. Experto en C++ que escribe en foros de programación. Realiza un video tutorial de SQL Injection en farsi donde expone su identidad.

<https://blog.checkpoint.com/wp-content/uploads/2015/11/rocket-kitten-report.pdf>

# Perspectiva histórica... Siglo XXI

2014: Troyano Careto

Para espiar en Marruecos, Cuba, España, Francia y Suiza.

<https://www.osi.es/es/servicio-antibotnet/info/careto>

<https://www.elmundo.es/tecnologia/2014/02/12/52fb2ac5268e3e134e8b456c.html>

<http://blogs.lainformacion.com/zoomboomcrash/2014/02/16/careto-el-nuevo-virus-informatico-mundial-una-creacion-del-espionaje-espanol/>

[https://www.eldiario.es/turing/vigilancia\\_y\\_privacidad/careto-ciberespionaje\\_0\\_228527853.html](https://www.eldiario.es/turing/vigilancia_y_privacidad/careto-ciberespionaje_0_228527853.html)



# Perspectiva histórica... Siglo XXI

2014: Troyano Careto...

Atribución:

**CounterCraft**

- Dominio registrado por “Victoria Gomez”.
- Clave de cifrado RC4 Caguen1aMar
- Referencia al directorio `c:\Dev\CaretoPruebas3.0\` y `c:\Dev\CaretoPruebas3.0\release32\CDIIUninstall32.pdb`
- Cadena de lenguaje: **Accept-Language:es**
- Propagación mediante suplantación de periódicos: *El País, El Mundo, Público.*
- Objetivos: Marruecos, Cuba, España, Francia y Suiza.

[https://kasperskycontenthub.com/wpcontent/uploads/sites/43/vlpdfs/unveilingthemask\\_v1.0.pdf](https://kasperskycontenthub.com/wpcontent/uploads/sites/43/vlpdfs/unveilingthemask_v1.0.pdf)



# Perspectiva histórica... 2014: Inception/Cloud Atlas

Atribución:

- De los creadores de Red October. Reutilización de ficheros, víctimas
- <https://www.symantec.com/connect/blogs/blue-coat-exposes-inception-framework-very-sophisticated-layered-malware>



## Red Herrings

- In specific instances where the APT seemed to be under investigation by researchers the actors dropped another piece of malware that is clearly attributable to a previously known Chinese APT: Suggests ties to China
- A large majority of the hacked home routers are in South Korea: Suggests ties to South Korea
- The attackers are most active from 8:00AM to 5:00PM in the Eastern European Timezone: Suggests ties to areas in the GMT+200 timezone
- Some of the comments in the Android malware are in Hindi: Suggests ties to India
- Some text strings in the BlackBerry malware are Arabic: Suggests ties to the Middle East
- The string "God\_Save\_The\_Queen" was found within the Black Berry malware: Suggests ties to the UK
- The word documents show some resemblance to word documents used by the Red October APT: Suggests ties to Ukraine and/or Russia
- The iOS malware was developed by someone using the account name "JohnClerk": Suggests ties to the US or UK
- The encryption key for the iOS malware "fjkweyreruu665E62C:GWR34285U%^%^#\$%\$%^\$RXYEUFQ2H89HCHVERWJFKWEhjvvehhewfD63TDYDGTYEDT23Y" appears to be keyboard mashing on a US/US International keyboard: Suggests ties to the US

Perspectiva histórica... 2014: Duqu 2.0

## False flags:

- Cadena ugly.gorilla -> Wang Dong de APT1/Comment Crew
  - Cifrado Camellia -> APT1
  - Cadena romanian.antihacker -> apuntar a Rumanía
  - Algoritmo de compresión raro LZJB -> MiniDuke 2013

## Atribución:

- Apenas trabaja los viernes y no trabaja los sábados. Su semana empieza los domingos.
  - Binarios compilados el 1 de enero
  - Zonas horarias de compilación GMT+2 o GMT+3
  - Buen inglés pero fallos de no nativos: Exceeded
  - Objetivo: Kaspersky

[https://securelist.com/files/2015/06/The Mystery of Dugu 2.0 a sophisticated cyberespionage actor returns.pdf](https://securelist.com/files/2015/06/The_Mystery_of_Dugu_2.0_a_sophisticated_cyberespionage_actor_returns.pdf)

# ASHLEY MADISON®

Life is short. Have an affair.®

Get started by telling us your relationship status:

Please Select

[See Your Matches »](#)

Over **38,855,000** anonymous members!

# BE CAREFUL

# THINK BEFORE YOU ACT



**As seen on:** BBC News,  
Reuters, The Sun, The  
Telegraph, The Times

Ashley Madison is the  
world's leading married  
dating service for  
*discreet* encounters



Trusted  
Security  
Award



SSL  
Secure  
Site



# Perspectiva histórica... CASO: Ashley Madison

Al atacar una web se comprometen:

- Datos personales
- Pérdida de confianza de los usuarios
- Reputación
- El producto en sí mismo



En julio de 2015, un equipo de hackers denominado Impact Team robó datos de más de 37 millones de usuarios a la compañía amenazando hacerlos públicos si esta no cerraba inmediatamente su web.

En agosto de 2015 estos datos fueron publicados en BitTorrent conteniendo datos como nombre, apellidos, teléfono, correo electrónico y transacciones financieras realizadas por los usuarios.

Como consecuencia de este escándalo, el 28 de agosto dimite Noel Biderman, su fundador.

# Perspectiva histórica... CASO: Ashley Madison

Datos curiosos:

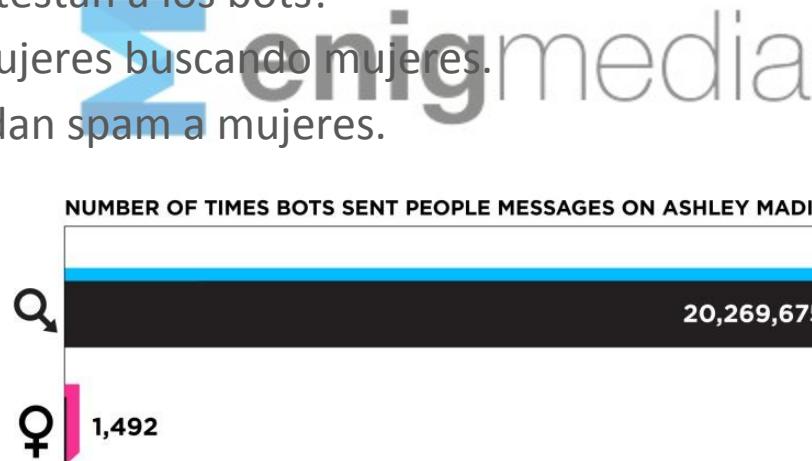
- El apellido más común entre mujeres era Doe.
- La dirección IP más común era 127.0.0.1 – más de 12.000 entradas.
- La distribución de fechas de cumpleaños (meses) era mayor en verano.
- Los usuarios pagaban \$19 por borrar los datos... y se guardan los datos con un campo <paid\_delete>



# Perspectiva histórica... CASO: Ashley Madison

Datos curiosos:

- \$250 Premium account > RunChatBotXmppGuarentee.service.php
- Los hombres contestan a los bots!
- Había 770.000 mujeres buscando mujeres.
- Los bots no mandan spam a mujeres.



[home](#) > [tech](#)**Tinder**

## I asked Tinder for my data. It sent me 800 pages of my deepest, darkest secrets

The dating app knows me better than I do, but these reams of intimate information are just the tip of the iceberg. What if my data is hacked – or sold?

- [Getting your data out of Tinder is really hard – but it shouldn't be](#)



35,983

**Judith Duportail**

@judithduportail

Tuesday 26 September 2017 07.10 BST



● A July 2017 study revealed that Tinder users are excessively willing to disclose information without realising it.  
Photograph: Alamy

### Most popular



Malta car bomb kills Panama Papers journalist



Men, you want to treat women better? Here's a list to start with



The Secret Actress: in Hollywood, Harvey Weinstein is not an anomaly



North Korean UN envoy says 'nuclear war may break out at any

# VICTIMA DE SEXTORSIÓN FACEBOOK?



T. +34 695 220 012 | brunoperez@evidenciesdigitals.cat  
Facebook /EvidenciesDigitals | Twitter @EvidenciesDigit  
www.evidenciesdigitals.cat



Asociación  
Stop! Violencia de  
Género Digital



## Solicita un Perito Informático

91 462 48 20  
659 082 631

INICIO LA ASOCIACIÓN ▾ HAZTE SOCIO SOLICITA UN PERITO FORMACIÓN ▾ ¿SUFRES ALGÚN TIPO DE VIOLENCIA? CONTACTO WEBINARS



Encarni Iglesias, presidenta de Stop Violencia de Género Digital: «Las chicas controlan más a su pareja»

16 diciembre, 2018



Detenido un menor por publicar en Whatsapp fotos eróticas de una niña

26 noviembre, 2018



«Sextorsión» en Galicia: «Vamos a empapelar Lugo con tus fotos»

13 noviembre, 2018



«Sextorsión» ¿Qué es y cómo evitar ser víctima de este tipo de chantaje?

7 noviembre, 2018

### Opinión de los Expertos



30 de Julio: Día Internacional contra la Trata; la esclavitud del siglo XXI

30 julio, 2018

En el año 2013, la Asamblea General de las Naciones Unidas se reunió, adoptando sus...



La prostitución: esto no va de sexo

1 febrero, 2018

Os invitamos a leer el artículo publicado en El País.com de nuestra compañera y amiga...



Opinión – Violencia de Género en los medios: de la información a la formación

7 agosto, 2017

Partimos de la base de que los medios de comunicación tienen como objetivo informar, formar...

### Síguenos Por las Redes Sociales



### Guías y Consejos contra la Violencia de Género Digital



CONSEJOS PARA PREVENIR UNA SEXTORSIÓN  
www.stopviolenciadegenerodigital.com



CONSEJOS PARA INTERVENIR EN UN CASO DE CIBERBULLYING  
www.stopviolenciadegenerodigital.com



CONSEJOS PARA EVITAR UNA SOPLANTACIÓN DE IDENTIDAD  
www.stopviolenciadegenerodigital.com



016

DELEGACIÓN A CORUÑA  
www.haysalida.org

# Perspectiva histórica... sexting, grooming, cyberbullying & revenge porn.

- **Sexting:** Básicamente, hacerse fotos eróicas y colgarlas en las redes sociales o enviarlas a través del móvil. Esta travesura o atrevimiento puede tener un efecto devastador, puede caer en manos a las que no iba dirigida.
- **Cyberbullying:** Es el acoso a través Internet, pero sin fines sexuales. Es decir, el uso de medios telemáticos (Internet, telefonía móvil, videojuegos on-line, etc.) para ejercer el acoso psicológico entre iguales. Se excluye el acoso o abuso de índole estrictamente sexual y los casos en los que intervienen personas adultas.
- **Grooming:** Es el acoso sexual de adultos a menores, utilizando las redes sociales. El primer paso lo dan utilizando esa imagen o vídeo erótico del menor que han conseguido previamente, a veces mediante perfiles falsos.
- **Revenge Porn (pornovenganza):** Difusión de fotos o videos íntimos de exparejas. (ej. casos: Olvido Hormigos y Karina Bolaños.)

# Una concejala del PSOE de Toledo dimite tras difundirse un video erótico suyo

Actualizado 05/09/2012 18:15:14 CET

TOLEDO, 5 Sep. (EUROPA PRESS) -

La concejala socialista Olvido Hormigos Carpio del Ayuntamiento de Los Yébenes (Toledo) ha presentado su dimisión como edil por "motivos personales", tras hacerse público a través de Internet un video erótico protagonizado por ella misma.

Según ha comentado a Europa Press el alcalde de Los Yébenes (Toledo), Pedro Acevedo, Hormigos registró su dimisión el pasado lunes y será en un pleno que la Corporación celebrará este jueves, a las 20.30 horas, cuando se haga efectiva la misma.

El edil, que ha definido como "escabroso" el tema, ha señalado que el video se conocía en la localidad "desde hace un mes". La concejala, casada y con dos hijos, entró en el Consistorio en junio de 2011.

A partir de este jueves, según el alcalde de Los Yébenes, se solicitará a la Junta Electoral la incorporación de la persona siguiente en la lista, el socialista Juan Diezma, para que asuma el acta de concejal.





RICA DESVELA LA TRAMA DEL VIDEO INTIMO POR EL QUE PERDIÓ EL CARGO

# Karina Bolaños

"La presidenta de mi país solo protege a los corruptos"

Foto: XANAS.EU

El 30 de julio, un video erótico recorrió las redes sociales y televisiones de todo el mundo. En él, la entonces viceministra de Juventud de Costa Rica aparecía en ropa interior instruyéndose a su amante. A las pocas horas fue destituida por la presidenta

interviu.es  
Z revista DEL 10 AL 16 DE SEPTIEMBRE  
2012. N° 1.898 CANARIAS 3.00€

**NIÑOS DE CÓRDOBA**  
**El día que Bretón perdió los nervios**

**DECLARACIONES EXCLUSIVAS**

**KARINA BOLAÑOS**  
**Cesada por un video erótico**  
**Era viceministra de Costa Rica**

**LA POLICIA INVESTIGA**  
**LA CAMORRA ENTIERRA BASURA EN MURCIA**

ESTA SEMANA CON INTERVIU  
**EL MEJOR Cine**



I can't be worried about  
that shit. Life goes on, man.

# Perspectiva histórica... 2015: Cyber Caliphate

# Counter Craft

False flags:

- Cadena TV5Monde fuera de línea
- Websites y redes sociales controladas por un tercero
- Grupo supuestamente de ISIS -> CyberCaliphate



Soldats de France! Vous avez la chance de sauver vos familles, profitez-en!  
#cybercaliphate

Soldats de France! Tenez-vous à l'ecart de l'Etat Islamique! Vous avez la chance de sauver vos familles, profitez-en! #CyberCaliphate

Au nom d'Allah le tout Clément, le Trois Monde et l'Europe. CyberCaliphate encourage (encourage) à monter son cyberjihad contre les ennemis de l'Etat Islamique.

Hollande m'a fait une liste impénitente ayant décidé à envoier les forces françaises pour nous aider à empêcher de kafirs musulmans dans cette guerre qui se met à rien. C'est pour ça que les français ont reçu les cendres de juif à Charlie Hebdo et à l'Hyper Casher de nos frères meurtriers Kouachi et Coulibaly.

Ensuite, au nom d'Allah, le CyberCaliphate est en train de rechercher les familles des militaires qui se sont vendus aux américains et servent à la base navale Camp de la Paix et à bord de Charles de Gaulle.

Les kafirs français, si vous vendez sauver vos familles, vous devrez abandonner l'idée de la paix et rejoindre l'opposition de l'Etat Islamique. C'est seulement comme ça que vous pouvez éviter le châtiment et sauvegarder vos vies et celles de vos proches.

Aljed d'Allah nous a donné perfirmer le travail de TV5 Monde et nous allons aussi exposer les documents confidentiels des départements qui contrôlent la France.

A l'aide d'Allah nous allons poursuivre la lutte contre l'Amérique et tous qui la soutiennent. CyberCaliphate et la Division des hackers de l'Etat Islamique préparent pour vous des surprises.

Il n'y a de Dieu qu'Allah et Mohammad est son message.  
Il n'y a de Dieu que Chacil.

[http://www.lexpress.fr/actualite/medias/piratage-de-tv5-monde-la-piste-russe\\_1687673.html](http://www.lexpress.fr/actualite/medias/piratage-de-tv5-monde-la-piste-russe_1687673.html)

# Perspectiva histórica... (2007-\*): Fancy Bear/APT28/Sofacy

Atribución:

- Binarios compilados en idioma ruso.
- Lunes a viernes de 8am a 6pm en UTC+4
- Objetivo: Georgia, Europa del Este, NATO

Counter Craft



<https://www.fireeye.com/content/dam/fireeye-www/global/en/currentthreats/pdfs/rpt-apt28.pdf>

# Perspectiva histórica... 2015: Yemen Cyber Army

False flags:

- Objetivos: Arabia Saudí
- En una cuenta comprometida, cambiaron el idioma a persa
- Nativos en farsi/persa
- Direcciones IP de Irán
- Utilizan la expresión “*Cutting Sword of Justice*” que se utilizó en Shamoon

<https://pastebin.com/HqAgaQRj>

<https://www.recordedfuture.com/iranian-saudi-cyber-conflict/>



# Perspectiva histórica... 2015: Yemen Cyber Army

 Untitled

A GUEST AUG 15TH, 2012 15,147 NEVER

[f SHARE](#) [TWEET](#)

 Pastebin PRO Accounts **SUMMER SPECIAL!** Until July 20th get 60% discount on a **LIFETIME PRO** account! *Offer Ends Soon!*

text 1.45 KB [raw](#) [download](#) [clone](#) [embed](#) [report](#) [print](#)

1. We, behalf of an anti-oppression hacker group that have been fed up of crimes and atrocities taking place in various countries around the world, especially in the neighboring countries such as Syria, Bahrain, Yemen, Lebanon, Egypt and ..., and also of dual approach of the world community to these nations, want to hit the main supporters of these disasters by this action.
2. One of the main supporters of this disasters is Al-Saud corrupt regime that sponsors such oppressive measures by using Muslims oil resources. Al-Saud is a partner in committing these crimes. It's hands are infected with the blood of innocent children and people.
3. In the first step, an action was performed against Aramco company, as the largest financial source for Al-Saud regime. In this step, we penetrated a system of Aramco company by using the hacked systems in several countries and then sended a malicious virus to destroy thirty thousand computers networked in this company. The destruction operations began on Wednesday, Aug 15, 2012 at 11:08 AM (Local time in Saudi Arabia) and will be completed within a few hours.
4. This is a warning to the tyrants of this country and other countries that support such criminal disasters with injustice and oppression. We invite all anti-tyranny hacker groups all over the world to join this movement. We want them to support this movement by designing and performing such operations, if they are against tyranny and oppression.
- 5.
6. Cutting Sword of Justice

# Perspectiva histórica... 2016: DNC Hack

Atribución:



- Crowdstrike y Fidelis: APT28 (FSB) y APT29 (GRU) están presentes
- Reutilización de herramientas, tácticas e infraestructura
- Misdepatrment.com -> 45.32.129.185 (APT28)
- C2C reusado: 176.31.112.10 (malware en el parlamento alemán)
- Certificado SSL reusado (parlamento alemán)
- Metadata de documentos: idioma en ruso, usuario Феликс Эдмундович, errores en cirílico
- Aparece Guccifer 2.0, que dice ser de Rumanía, pero utiliza todo de Francia (OVH, cuenta de AOL francesa, etc.)

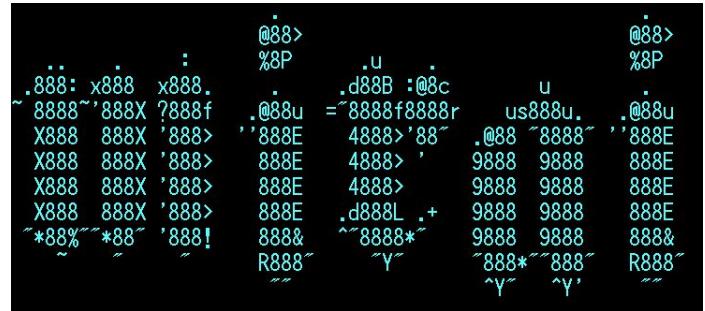
<https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/>

<https://guccifer2.wordpress.com>

# Perspectiva histórica... 21 de octubre de 2016: Malware Mirai.

Ciberataque a Dyn.

- Víctima: proveedor DNS Dyn.
- Ataque DDoS empleando una botnet.
- Empleó multitud de dispositivos IoT para su ejecución (SmartTVs, cámaras IP, etc.)



Lizia

te escribí cuando salió el artículo de lo de las tarjetas en la mierda de LOC y ya sabes lo que pienso Javier. Sabemos quién eres, sabes quiénes somos. Nos conocemos, nos queremos, nos respetamos. Lo demás, mierda. Un beso compi yogui (miss you!!!)

Os lo agradezco mucho. En el futuro extremare el cuidado, vivimos en un país muy difícil y sere aun mas consciente de mi conducta.

PF PT

Y tanto! Me uno al chat, pero prefiero tener un rato para charlar sin intermediación electrónica ni telefónica. Comemos mañana? Abrazos

PF PT

Ahi val Pues claro que no, hombre. Era por charlar con tranquilidad. Ya cuando vuelvas hablamos. Un abrazo y disfruta algo lejos de este barullo.

Gracias señor

# Perspectiva histórica... Siglo XXI



## Compi yogui (miss you!!!) (2016):

- En pleno escándalo de las tarjetas 'black' de Caja Madrid y Bankia, el empresario **Javier López Madrid** recibió el cariño y apoyo de varios amigos, entre ellos los reyes de España.
- En el momento del mensaje habían pasado cinco días desde que trascendiera el detalle de los gastos realizados por cada uno de los consejeros y directivos de **Caja Madrid y Bankia**.
- López Madrid había gastado 34.807 euros con el plástico que la entidad que **acabó siendo rescatada con 23.000 millones de dinero público**.





Payment will be raised on

5/15/2017 16:32:52

Time Left

02:23:58:49

### What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

### Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

Your files will be lost on

5/19/2017 16:32:52

Time Left

06:23:58:49

### How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

[About bitcoin](#)

[How to buy bitcoins?](#)

[Contact Us](#)



Send \$300 worth of bitcoin to this address:

12H9YD9gmcwZ9t4yMgvw41Sp7AABmugfS3Mw...

Copy

[Check Payment](#)

[Decrypt](#)

# Perspectiva histórica... 2017: Wannacry

## Vulnerabilidad del protocolo SMB de Microsoft CVE-2017-0144

 NVD  
National Vulnerability Database

CVE List      CUIs      Board      About      News & Blog

Search CVE List      Download CVE      Data Feeds      Request CVE IDs      Update a CVE Entry

TOTAL CVE Entries: 111064

Printer-Friendly View

**CVE-ID**  
**CVE-2017-0144** [Learn more at National Vulnerability Database \(NVD\)](#) • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

**Description**  
The SMBv1 server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT 8.1; and Windows 10 Gold, 1511, and 1607; and Windows Server 2016 allows remote attackers to execute arbitrary code via crafted packets, aka "Windows SMB Remote Code Execution Vulnerability." This vulnerability is different from those described in CVE-2017-0143, CVE-2017-0145, CVE-2017-0146, and CVE-2017-0148.

**References**  
Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- EXPLOIT-DB-42030
- URL-<https://www.exploit-db.com/exploits/42030/>
- EXPLOIT-DB-42031
- URL-<https://www.exploit-db.com/exploits/42031/>
- EXPLOIT-DB-41891
- URL-<https://www.exploit-db.com/exploits/41891/>
- EXP-DB-41987
- URL-<https://www.exploit-db.com/exploits/41987/>
- MISIC-<https://ics-cert.us-cert.gov/advisories/ICSM-18-058-02>
- CONFIRM-<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0144>
- CONFIRM-[https://cert-portal.siemens.com/productcert/pdf/ssa\\_701903.pdf](https://cert-portal.siemens.com/productcert/pdf/ssa_701903.pdf)
- CONFIRM-[https://cert-portal.siemens.com/productcert/pdf/ssa\\_966341.pdf](https://cert-portal.siemens.com/productcert/pdf/ssa_966341.pdf)
- BID-7074
- URL-<https://www.securityfocus.com/bid/95704>
- SECTRACK-1037991
- URL-<http://www.securitytracker.com/id/1037991>

**Assigning CNA**  
Microsoft Corporation

**Date Entry Created**  
20160909 Disclaimer: The `entry_creation_date` may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.

**Phase (Legacy)**  
Assigned (20160909)

**Votes (Legacy)**

**Comments (Legacy)**

**Proposed (Legacy)**  
N/A

This is an entry on the [CVE List](#), which provides common identifiers for publicly known cybersecurity vulnerabilities.

SEARCH CVE USING KEYWORD:    
You can also search by reference using the [CVE Reference Maps](#).

For More Information: [cve@mitre.org](mailto:cve@mitre.org)

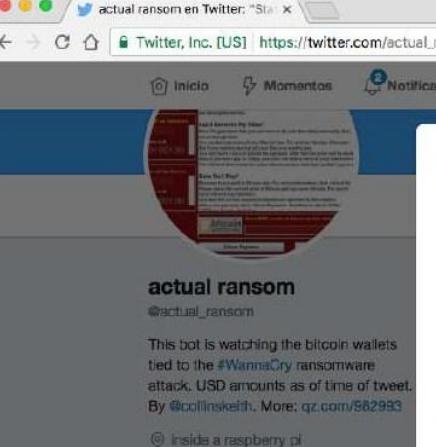
BACK TO TOP

# Perspectiva histórica... 2017: WannaCry

- Actualización de seguridad publicada el 14 de marzo de 2017.
- Empleo del exploit *EternalBlue*, supuestamente desarrollado por la NSA.
- Filtrado el 14 de abril de 2017 por el grupo de hackers *Shadow Brokers*.
- Ataque a escala mundial el 12 de mayo de 2017.
- Ha recaudado 116555 €.



NSA's Target List Leaked!	
orange.mplx.net	211.43.194.48
ortion.pipline.gov.vn	202.225.175.67
proton.dnsd.edu	202.297.6.105
natcisco.cau.ctu.edu.vn	202.175.36.180
butth-head.nos.ru	10.30.1.130
dproxy1.thurnet.com	210.117.65.44
heat.bjtu.edu.cn	202.120.399.1
dean.fsu.edu	121.160.195.54
doors.co.kr	211.43.193.9
enterprise.telesat.com.co	66.128.32.67
fb43.nic.ac	100.160.71.3
panberrol.cs.	179.154.62
gate.techno	179.9.148.61
hakuba.jst.go.jp	180.232.128.54
unsi.net	202.112.146.5
... (many more entries)	



actual ransom en Twitter: "Status of WannaCry wallets:  
51.98076422 BTC (\$132,984.34)  
337 payments, 0 withdraws  
Last payment:  
2017-06-28 at 05:50 AM ET  
[Traducir del inglés](#)  
5:07 - 30 jun. 2017

**actual ransom**  
@actual\_ransom  
  
Status of WannaCry wallets:  
51.98076422 BTC (\$132,984.34)  
337 payments, 0 withdraws  
Last payment:  
2017-06-28 at 05:50 AM ET  
[Traducir del inglés](#)  
5:07 - 30 jun. 2017

# Perspectiva histórica... 2017: WannaCry

Atribución:

- Código compartido con Lazarus Group
- De todos los idiomas, el mejor escrito es el chino



<https://www.flashpoint-intel.com/blog/linguistic-analysis-wannacry-ransomware/>

<http://blog.elevenpaths.com/2017/06/wannacry-chronicles-messi-coreano.html>

# Perspectiva histórica... 27 de junio de 2017: Petya

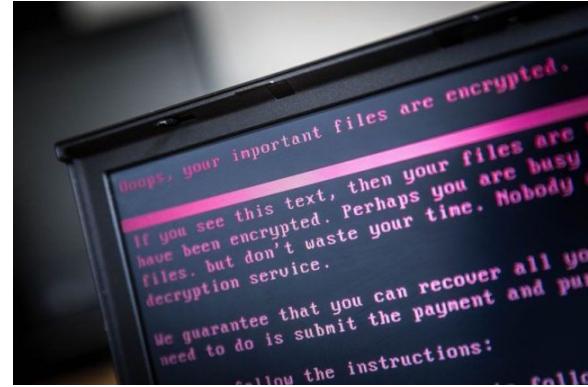


# Perspectiva histórica... 2017: Rusia vs Ucrania

Atribución:

- Atentado terrorista contra Coronel Maksym Shapoval
- Dia del 21<sup>a</sup> aniversario de la independencia
- Principal vector de infección: *MeDoc*, software financiero usado por muchas empresas en Ucrania.
- Visita en la semana pasada de Poroshenko a ver a Trump en Washington
- Objetivo: Ucrania

<http://dailysignal.com/2017/06/29/russias-hybrid-warfare-battlefield-ukraine-heats/>





# GreyEnergy: uno de los actores maliciosos más peligrosos cuenta con un arsenal actualizado

Una investigación de ESET revela la presencia del sucesor del grupo de APT de BlackEnergy apuntando a infraestructuras críticas; muy probablemente en la etapa previa a la realización de un ataque.



Anton Cherepanov and Robert Lipovsky 17 Oct 2018 - 11:55AM

Compartir



Una reciente investigación de ESET reveló nuevos detalles del sucesor del grupo de APT de BlackEnergy, cuya principal herramienta fue vista por última vez en diciembre de 2015 cuando por primera vez en la historia un ciberataque fue el responsable de provocar un apagón. Cerca de las fecha del incidente, cuando cerca de 230.000 personas quedaron sin electricidad, comenzamos a detectar otra infraestructura de malware que llamamos GreyEnergy. Desde ese entonces ha sido utilizada para atacar compañías de energía, así como también otros blancos de ataque de gran valor en países como Ucrania y Polonia a lo largo de los últimos tres años.

Es importante aclarar que cuando nos referimos a "grupos de APT" establecemos conexiones sobre la base de indicadores técnicos, como pueden ser similitudes de código, infraestructura C&C compartida, cadenas de ejecución de malware, entre otras características. Por lo general, no nos involucramos directamente en la investigación y la identificación de quienes desarrollan el malware y/o que luego lo implementan o interactúan con ellos. Dado que el término "grupo de APT" suele estar más asociado con los indicadores de malware anteriormente mencionados y frecuentemente se utiliza simplemente para categorizar, nos mantenemos al margen de la especulación con respecto a la atribución de ataques a países o gobiernos.

# New Shamoon V3 Malware Targets Oil and Gas Sector in the Middle East and Europe

December 13, 2018 | Anomali Labs



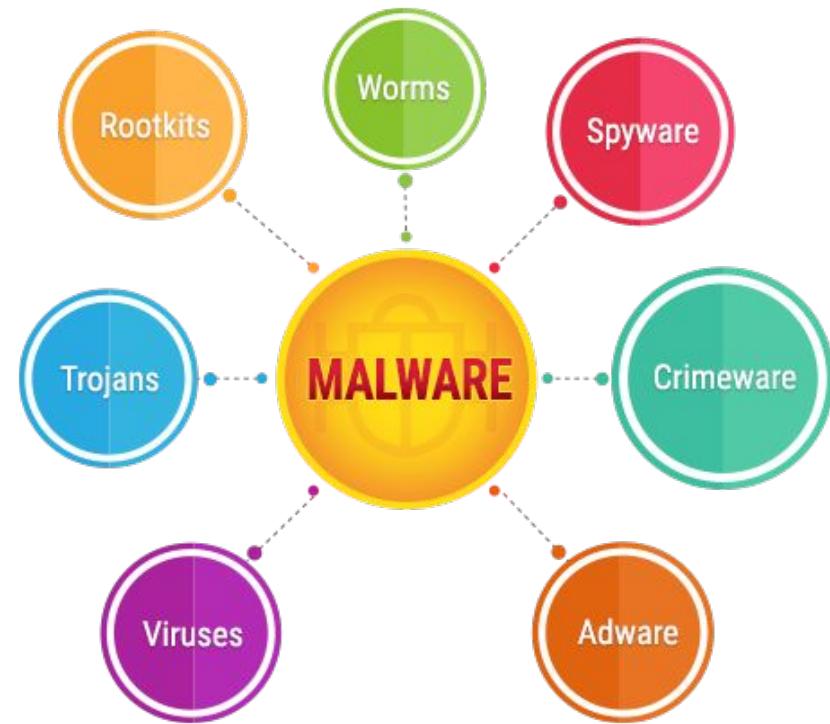
A new version of destructive wiper malware Shamoon was first identified by security researchers on December 5, 2018. This malware, dubbed Shamoon V3, appears to be a new version of the destructive malware, which has historically been associated with advanced persistent threat actors aligned with the interests of the Iranian state. It has targeted at least one European oil and gas company with operations in the Middle East and Asia. Unconfirmed reports also indicate possible entities in the UAE oil and gas industry are affected as well. A defining characteristic of this new Shamoon version is that it shares nearly 80 percent similarity with earlier versions of Shamoon and may use a historic trigger date, so that it can immediately perform destructive actions once infecting a user's machine. Although not confirmed to be the work of Iranian APT groups, the malware's codebase, targeted sector, and targeted geography have all been observed in historic attacks which were later attributed to adversaries from the region.

qj3rJvMq4tV,mpaUNKxRwqyIA9b1BQ3iMER3iWaceavubow1337nqLAmIzL7VA,V3an3qjg,y,r,21,NS38A,CWII,NNkgq4  
1wyua+616itPoZw1hPshGevmbC+MLjtTRYES5hOBM0FaOMo+Q+2nmU+4Pvhb33E2EW9iznayFjWQ0qcWvjUBQUYV/FuFyLPcdp1jk  
/CCbmpHye5RuaeOT/G6yPezgZFefqs2CE8nz9GBT+ab3Pbo90n2MMYGn1h1ztTNyzIBOKb01FqqFbsXCMgCKz4b+iQWIAtv6z1TFM  
ws6UJE/4jdrS1390q8q1cwmo37LYvvQThyzBt61KDPEX**N6vbRGz27RY**+6ntXFqs901XNREF3kIJnaKWiKzBSbvWleTxn12Hxt/g  
Db+geLNkXIR5T5BDR9ZLdr2s0M5WZXGp7j05EFFfqiS**V3jXO/K0pL4Iqouzo1lthHjFn1SBPUgoF/3GhmmYOC9dG0708qxz+v5e9**  
sFC/8myp//VPLFK0wx2sqA+SGbYLj9KAfveev5vD/**PRWGzE3NPWXT0v9b1zeCzhuTc+N7vkxi/pkmUA5YtBeHUG7OKTQt2tIQDM**  
ct6ywJ11ejuI3i1krje2Aj5ZiacGpRAP14KEhFRHf1z6wgYJ1Y30ax5**QKGohMPFsQ9b4AtTf1bgZtu1QGjfTV0q+jdzeAWBfcZ**  
7bhyiRKih8FuawqegyYLtSSD18PYKvtSWBFZ+1IZ0pjqgoD7wbqa4ndvp**UU0wdfdtG5yGMhbMdZRZ/hYv0IAprhi6kBosCdfEB**  
jeqNVgFLj4gc0eOdakww10cp40uSe7IGV/y6Pzhqv88uc2VBVG/JzpQk**z2ythFc5i2zhpbfCGWtpTwqf0v7jAHMmj2yg715n1**  
TPW5Fu2yyXC79YaasImkxc9xselu63G3Kx0k3m08dRtbhheQf4rM9TDLvLqteM2T2NTB15Hvnk8Thz40Z7F6Crnghtqzk0x1Rag  
z0tP1SmgX1/BEeRB4PKBG6fsufCOK/wgcDHExCuyeHX05+jtL/nkn14xTkse5cYM**GyDsCzrpDGFEiMeGcxtBw0+R0bqnup4fMyk7**  
k1k4Pi86uzv3z67CY10DIDgxoFyA3aws7Tdvdv3/b0P+qGA0wB+PGXPNiC9Ti0z6P3PFbusrf1GCCxe1ojKMFyncaAzqdh0rkF04  
KgIr0yqv2/uRVgMXg41xi5Tc4xDdAza+45Nw34PwVxcUPRJNgubbssxbTanJwlqvad06xu2N8m8jWYA/03hd8iKaIQjT+y43q/zz  
Ayg9wmuDfg00HLht4Gwj/6qLe0ofc1khjY6756**JQADKMXKDumbCTL6UgAMoeF2P5GXYQh31cb04n1Cy4ua3D3UjjsGe5U/YozY6e**  
waVPZT/Z6wow/G8I1aaK003Rqo8tL+HqyIHNCRMiul0pDEB+6XPzxqkuhnfpTyrzSGsv9ZpHi/h/eMNFl3xamtM6y/izox3d49re  
+Mpmi+pLq0pc9g3Jg38H6Puuzs0uox1Tgbelnx9u0Tbb8vo7ZrvjmdMrehv2lFI+wiplgrT3SuV1zz6rgc47pD6M3GvG4Vcm0MOB  
h4itLIX0093evudvwLoLUjZ0VzGro8UFN9G3Av**7Eo7nJflqYBit54HPF9TVXSIueGykkHnt2wuqfqd9F1JmgynvpsRiB3Su4Ez7r**  
sd8BkbqEB1Qv0qKv0tfjha0078KovcDkzbEDY/TpedLxfBjE3cyu6zhywCzx7zsxx5xc7mhqOBStc0B7aE29K0gtvrf/iRuILj1  
wiRXMPcFcgnaqGg1ZbsJbzTG+qoCKD03Nj1IzmnPvnlp7fnzjzyuFP5bjvb4jbFs6si1rnZh19Fd1f6s5dnzsh+Nw8xCL9j4pB3  
PiBVCDq4UuLEawlvxLaZe24FAEdbpDNgJT4BqtOarcvxHUOsTtU1qsARqud0Zmyf5a9YnByQGTI6rrICriAFZj1+teNjiA2T3nt  
+JCAtd0uyhx13ks/tcyIA6BBMW6Nvg/vLKnfFzyCPdkzfRLa7WujVqqxhASRXys7xR9677Mp37+nEafdbrwvIiN9hhG6HSJ9Ykv  
zonnlJHpP2GhLf8F-----  
AjS/FsgXHmK7+ftt  
bYE71yIIid/noyN93  
TOJB1y3IuPXETYS5  
R/vo8ye+4HPMLShv  
vd5TF571b42TK263,  
fk86q06ayaIblvrjo9dv5tzjL6xyygF4XiYj1gxkMCUyQZ9/d5ehMUPLo4c4hIXAXuKhfuuhvtXv2qdhbEGn1VycsYP9jrmxfqNM  
6e8vtLynwmj2SdoR1411hZYP9TgwJF00K2pCeQo4c8VpdTZNeqduaYPT3LtnJm17kaafOFg9ixokqnvOYmBg1NGUUTqHTK30xi21  
PW8tcglH+QuqY/b1MwgsAoFF835uZrmyCS7z9WNSfa0RPTyKizS6j6/RRTuqmHiKu8utg56F1tchek0LB9umUgfga4udm4QS90o2

# RANSOMWARE

# Evolución del Malware:

- 1986 Brain virus
- 1987 Christmas Exec
- 1988 Ping-pong virus
- 1992 Michelangelo
- 1999 I LoveYou
- 2003 SQL Slammer
- 2004 Cabir Worm (primer virus en Teléfonos móviles)
- 2008 Conficker



# Evolución del Malware:



- Primera generación; 1980-1990: Bromas y molestias.
- Segunda generación; 1990-1998: Virus de macro y polimórficos.
- Tercera generación; 1999-2001: Correo electrónico.
- Cuarta generación; 2001-2010: Difusión a través de internet y páginas web.
- Quinta generación; 2010-2015:
  - Malware personalizado y dirigido a objetivos concretos.
  - Cibercrimen: objetivos económicos.

## Época Romántica (1996-2000)

- Virus destructivos
- Carácter local, sin propagación
- Creación de Virus
- Personas solitarias, muy localizadas

**MOTIVACIONES:**  
Superación personal  
Conocimientos técnicos

**Origen:**  
Personas individuales o grupos muy pequeños

**A destacar:**  
Alta calidad técnica  
No hay programación

## Edad Media (2001-2004)

- Primeros phishing (11S)
- Gusanos
- Botnets 1.0 (IRC)

**MOTIVACIONES:**  
Dinero rápido  
Infecciones masivas

**Origen:**  
Personas individuales o grupos muy pequeños

**A destacar:**  
Baja calidad técnica  
No hay programación

## Fraude (2005-2006)

- Milicias cibernéticas
- Múltiples objetivos
- Control del 50% de los ordenadores

**MOTIVACIONES:**  
Dinero de cualquier forma  
Extorsiones

**Origen:**  
Personas individuales o grupos muy medianos

**A destacar:**  
Phishing y malware  
100% fraude bancario

## e-crime (2007-2009)

- Ataques geopolíticos
- Botnets 2.0
- ISP a prueba de balas
- Infraestructura en venta
- Iframe businesss, pay per install, clickfraud, botnets, DDoS, infection kits, C&C, cyberwarfare, espionaje industrial...

**MOTIVACIONES:**  
Controlar Internet  
Dominación total

**Origen:**  
Grupos de crimen organizado

**A destacar:**  
Target: gobiernos, empresas  
Amenazas políticas

Common types of cyber incidents		Potential losses
	Data confidentiality breach (3rd party data)	Incident response costs Breach of privacy compensation Reputational damage Regulatory and legal defense costs Fines and penalties Directors and officers liability
	Data confidentiality breach (own data)	Intellectual property theft Directors and officers liability
	Operational technology malfunction	Business interruption Fines and penalties Physical asset damage Bodily injury and death Directors and officers liability
	Network communication malfunction	Business interruption Reputational damage Directors and officers liability
	Inadvertent disruption of 3rd-party system	Network security failure liability Regulatory and legal defense costs
	Disruption at external service provider	Contingent business interruption
	Deletion or corruption of data	Data and software loss Regulatory and legal defense costs Products liability Directors and officers liability
	Encryption of data	Cyber ransom and extortion Directors and officers liability
	Cyber fraud/theft	Financial theft and/or fraud Directors and officers liability

# Ciberseguridad en el mundo actual:

<https://cybermap.kaspersky.com/es>

<https://www.fireeye.com/cyber-map/threat-map.html>

<https://threatmap.checkpoint.com/ThreatPortal/livemap.html>

<https://threatmap.fortiguard.com/>

<https://sicherheitstacho.eu/start/main>

<http://map.norsecorp.com>

<http://www.digitalattackmap.com/>



# Ciberseguridad en el mundo actual:



**Sin denuncia no hay delito.**



## ACTA DE COMPARTECENCIA POR DENUNCIA PENAL

Fecha de la denuncia:

Asunto denuncia:

## DATOS DEL DENUNCIANTE

Sexo:  Tipo de documento:  Número docum.:

Nombre:  Apellido 1:  Apellido 2:

Nombre padre:  Nombre madre:

Fecha nacim.:  País nacimiento:  CCAA:

Provincia:  Municipio:  Nacionalidad:

### Datos del domicilio fijo

Tipo de vía:  Dirección:  Nº:  Piso:  Otros:

País:  CCAA:  Provincia:  Municipio:

Teléfono fijo:  Teléfono móvil:  Otros:

Fax:  Correo electrónico:

## CLAVE:

### A partir de 5.000 ciberataques

Madrid

Barcelona

### Menos de 5.000 ciberataques

Valencia Tarragona

Sevilla Vitoria

Bilbao Pontevedra

Málaga Jaén

Alicante Valladolid

Murcia Santander

Zaragoza Almería

Oviedo

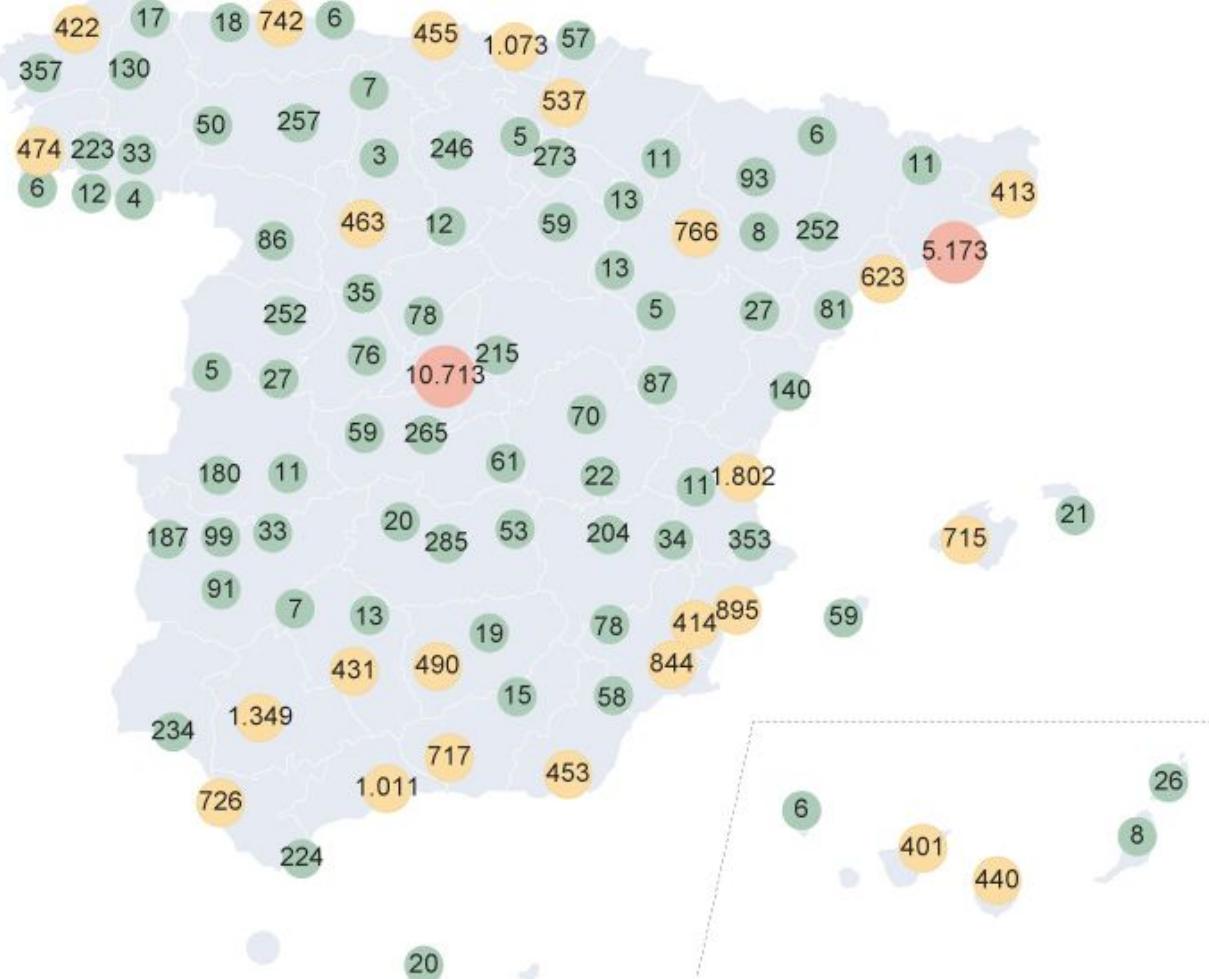
Cádiz Ferrol

Granada Elche

Palma Gerona

### Menos de 400 ciberataques

Resto



# Ciberseguridad en el mundo actual:

## Delito Informático

Definición: “Los actos dirigidos contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos”.



- **Abuso informático:** todo comportamiento ilegal o contrario a la ética o no autorizado que concierne a un tratamiento automático de datos y/o transmisión de datos.
- **Criminalidad informática:** la realización de un tipo de actividades que, reuniendo los requisitos que delimitan el concepto de delito, sean llevadas a cabo utilizando un elemento informático (mero instrumento del crimen) o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software.

# Ciberseguridad en el mundo actual:

## Tipos de Delito Informático:

- Delitos contra el derecho a la intimidad.
- Fraude informático.
- Sabotajes informáticos.
- Falsedades.
- Calumnias e injurias.
- Amenazas.
- Infracciones a la Propiedad Intelectual a través de la protección de los derechos de autor.
- Pornografía infantil.



# Ciberseguridad en el mundo actual:

## Clasificación Europea VS Clasificación según BIT.

Clasificación Europea	Clasificación BIT
Delitos contra la confidencialidad, la integridad y la disponibilidad de los daños y sistemas informáticos	Ataques contra el derecho a la intimidad
Delitos informáticos (falsificación y fraude)	Infracciones contra la propiedad intelectual
Delitos relacionados con el contenido (relacionados con la pornografía infantil)	Falsedades
Delitos relacionados con infracciones de la propiedad intelectual y derechos afines	Sabotajes informáticos
	Fraudes informáticos
	Amenazas
	Calumnias e injurias
	Pornografía infantil



# Ciberseguridad en el mundo actual:

- Clasificación según el “Convenio sobre la Ciberdelincuencia” de 1 de Noviembre de 2001

Con el fin de definir un marco de referencia en el campo de las tecnologías y los delitos para la Unión Europea, en Noviembre de 2001 se firmó en Budapest el “Convenio de Ciberdelincuencia del Consejo de Europa”. En este convenio se propone una clasificación de los delitos informáticos en cuatro grupos



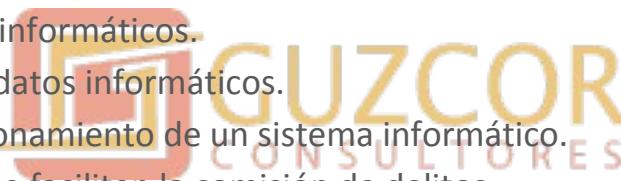
- Clasificación según **Brigada de Investigación Tecnológica** de la Policía Nacional:

[https://www.policia.es/org\\_central/judicial/udef/bit\\_quienes\\_somos.html](https://www.policia.es/org_central/judicial/udef/bit_quienes_somos.html)

# Ciberseguridad en el mundo actual... Clasificación Europea:

- Delitos contra la **confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos**:

- Acceso ilícito a sistemas informáticos.
- Interceptación ilícita de datos informáticos.
- Interferencia en el funcionamiento de un sistema informático.
- Abuso de dispositivos que faciliten la comisión de delitos.



Algunos ejemplos de este grupo de delitos son: el robo de identidades, la conexión a redes no autorizadas , la utilización de spyware y de keylogger.

# Ciberseguridad en el mundo actual... Clasificación Europea:

- Delitos **informáticos**:
  - Falsificación informática mediante la introducción, borrado o supresión de datos informáticos.
  - Fraude informático mediante la introducción, alteración o borrado de datos informáticos, o la interferencia en sistemas informáticos.
  - El borrado fraudulento de datos o la corrupción de ficheros algunos ejemplos de delitos de este tipo.
- Delitos relacionados con el **contenido**:
  - Producción, oferta, difusión, adquisición de contenidos de pornografía infantil, por medio de un sistema informático o posesión de dichos contenidos en un sistema informático o medio de almacenamiento de datos.
- Delitos relacionados con infracciones de la **propiedad intelectual** y derechos afines.

Un ejemplo de este grupo de delitos es la copia y distribución de programas informáticos, o piratería informática.

# Ciberseguridad en el mundo actual... Clasificación Europea:

- Con el fin de criminalizar los actos de **racismo y xenofobia** cometidos mediante sistemas informáticos, en Enero de 2008 se promulgó el “Protocolo Adicional al Convenio de Ciberdelincuencia del Consejo de Europa” que incluye, entre otros aspectos, las medidas que se deben tomar en casos de:
  - Difusión de material xenófobo o racista.
  - Insultos o amenazas con motivación racista o xenófoba.
  - Negociación, minimización burda, aprobación o justificación del genocidio o de crímenes contra la humanidad.

# Ciberseguridad en el mundo actual:

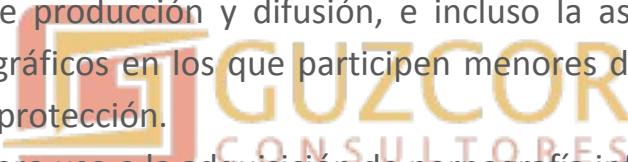
## URLs jurídicas:

- Ley "vieja" pero buen resumen:
  - <http://www.deic.uab.es/material/26118-ley.pdf>
- Ley "nueva" (CP y de 2015):
  - [http://noticias.juridicas.com/base\\_datos/Penal/549720-lo-1-2015-de-30-mar-modifica-la-lo-10-1995-de-23-nov-del-co-digo-penal.html](http://noticias.juridicas.com/base_datos/Penal/549720-lo-1-2015-de-30-mar-modifica-la-lo-10-1995-de-23-nov-del-co-digo-penal.html)
  - "fiscal"  
[https://www.fiscal.es/fiscal/PA\\_WebApp\\_SGNTJ\\_NFIS/descarga/ponencia%20Rodriguez%20Fernandez,%20Alberto.pdf?idFile=bd78e587-740d-4e30-abe4-ec7d2e0755dd](https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/ponencia%20Rodriguez%20Fernandez,%20Alberto.pdf?idFile=bd78e587-740d-4e30-abe4-ec7d2e0755dd)
  - "nuevos delitos"  
<http://web.icam.es/bucket/Faustino%20Gud%C3%ADn%20-%20Nuevos%20delitos%20inform%C3%A1ticos.pdf>
  - "trabajo universitario" [https://uvadoc.uva.es/bitstream/10324/13740/1/TFG-D\\_0124.pdf](https://uvadoc.uva.es/bitstream/10324/13740/1/TFG-D_0124.pdf)



# Delitos relativos a la pornografía infantil:

- Se presta especial atención al castigo de la **pornografía infantil**. Se ofrece una definición legal de pornografía infantil tomada de la **Directiva 2011/93/UE**, que abarca no sólo el material que representa a un menor o persona con discapacidad participando en una conducta sexual, sino también las imágenes realistas de menores participando en conductas sexualmente explícitas, aunque no reflejen una realidad sucedida.
  - Se castigan los actos de producción y difusión, e incluso la asistencia a sabiendas a espectáculos exhibicionistas o pornográficos en los que participen menores de edad o personas con discapacidad necesitadas de especial protección.
  - También se castiga el mero uso o la adquisición de pornografía infantil, y se incluye un nuevo apartado para sancionar a quien acceda a sabiendas a este tipo de pornografía por medio de las tecnologías de la información y la comunicación, en la conciencia de que las nuevas tecnologías constituyen una vía principal de acceso a los soportes de la pornografía.
  - Se faculta expresamente a los jueces y tribunales para que puedan ordenar la adopción de medidas necesarias para la retirada de las páginas web de internet que contengan o difundan pornografía infantil o, en su caso, para bloquear el acceso a dichas páginas.



# Delitos en relación con la libertad sexual y protección de menores:

- El **Artículo 189** incluye en **pornografía infantil** no sólo el material que representa a un menor o discapacitado participando en una conducta sexual, sino también las imágenes realistas de menores participando en conductas sexualmente explícitas, aunque no reflejen una realidad sucedida. Se penaliza el que para su propio uso adquiera o posea pornografía infantil y se incluye un nuevo apartado para sancionar a quien acceda a sabiendas a este tipo de pornografía por medio de las tecnologías de la información y la comunicación. También se faculta a los jueces para que puedan ordenar la retirada de las páginas web o aplicaciones de Internet que contengan o difundan pornografía infantil.
- El **Artículo 183** tipifica el nuevo precepto del **grooming**: “El que a través de Internet, del teléfono o de cualquier otra tecnología de la información y la comunicación contacte con un menor de dieciséis años y proponga concertar un encuentro con el mismo a fin de cometer cualquiera de los delitos descritos en los artículos 183 y 189, siempre que tal propuesta se acompañe de actos materiales encaminados al acercamiento, será castigado con la pena de uno a tres años de prisión o multa de doce a veinticuatro meses”, y “El que a través de Internet, del teléfono o de cualquier otra tecnología de la información y la comunicación contacte con un menor de dieciséis años y realice actos dirigidos a embauclarle para que le facilite material pornográfico o le muestre imágenes pornográficas en las que se represente o aparezca un menor, será castigado con una pena de prisión de seis meses a dos años”.

# Ampliación en la regulación del Grooming:

- Ya se tipificaba el **childgrooming** (art. 183 ter) que supone el acoso de adultos a través de las TIC hacia menores de 13 años para de obtener fotografías o vídeos de contenido íntimo y con el fin de conseguir un encuentro físico real en el que abusar del menor. Con la nueva regulación se aumenta la protección de los menores frente a los abusos cometidos a través de internet y las TIC, debido a la facilidad de acceso y el anonimato que proporcionan, con un nuevo apartado en el artículo 183 ter destinado a sancionar al que a través de medios tecnológicos contacte con un menor de 15 años y realice actos dirigidos a embaucarle para que le facilite material pornográfico o le muestre imágenes pornográficas.

### MODELO DE SOLICITUD DE CERTIFICADO POR DELITOS DE NATURALEZA SEXUAL

El que suscribe, cuyos datos se consignan a continuación, solicita de ese Ministerio la expedición de un certificado del Registro Central de Delincuentes Sexuales para cumplir los requisitos expresados en la Ley 26/2015, de modificación del sistema de protección a la infancia y a la adolescencia y la Ley 45/2015, de Voluntariado.

#### 1.- DATOS DEL TITULAR DE LA INFORMACIÓN (indicar nombre y apellidos completos):

N.I.F./N.I.E./PASAPORTE	NOMBRE		
<input type="text"/>	<input type="text"/>	<input type="text"/>	
PRIMER APELLIDO	SEGUNDO APELLIDO	SEXO	
<input type="text"/>	<input type="text"/>	<input type="text"/>	
FECHA DE NACIMIENTO	NACIONALIDAD *	LUGAR DE NACIMIENTO	PROVINCIA DE NACIMIENTO
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
NOMBRE DEL PADRE	NOMBRE DE LA MADRE	MENOR DE EDAD <input type="checkbox"/>	
<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	

Asimismo, solicita del Ministerio, que le remita vía SMS el código necesario para descargar el certificado a través de la sede electrónica.

\*\* TELÉFONO MÓVIL:

El solicitante recibirá en este teléfono un SMS un código de acceso que le permitirá descargar su certificado desde cualquier terminal con acceso a internet, tantas veces como necesite.

#### 2.- DATOS DE CONTACTO:

CALLE/PLAZA/AVENIDA	NÚMERO	ESCALERA	PISO	PUERTA
<input type="text"/>				
LOCALIDAD	PROVINCIA			
<input type="text"/>	<input type="text"/>			
CÓDIGO POSTAL	CORREO ELECTRÓNICO			
<input type="text"/>	<input type="text"/>			

En..... a..... de..... de.....

Firma:

\* En caso de nacionalidad distinta a la española deberá solicitar un certificado de antecedentes penales en su país.

\*\* El Real Decreto 1110/2015 indica que la expedición de certificados se hará preferentemente por medios electrónicos.



**MINISTERIO  
DE JUSTICIA**

### REGISTRO CENTRAL DE DELINCUENTES SEXUALES

#### CERTIFICA:

Que, en el día de la fecha, consultada la Base de Datos del Registro Central de Delincuentes Sexuales, **NO CONSTA** información penal relativa a:

D/D\*

con NIF n°

Conforme a lo dispuesto en la Decisión Marco 2009/315/JAI del Consejo de 26 de febrero, relativa a la organización y al contenido del intercambio de información de los registros de antecedentes penales entre los Estados miembros, **tratándose de ciudadanos españoles**, el presente certificado incluye, en su caso, las condenas impuestas por otros Estados miembros de la Unión Europea, en los mismos términos en que tales condenas hayan sido notificadas, sin que exista necesariamente una equiparación entre los tipos delictivos del Estado de condena y los tipos delictivos nacionales.



**Día Internet Segura 2019 | Martes 5 Febrero**

Una Internet mejor comienza contigo:  
conviviendo con respeto para una Internet segura

**SID 2019**

**SABER MÁS**

European Commission | INNOVAE Instituto | is4k INTERNET SEGURA FORKIDS



#### Guía de juguetes

La guía de juguetes conectados está formada por 7 fichas que recogen las principales recomendaciones para las familias antes y después de la compra de



#### Guía de Privacidad

La guía está formada por 18 fichas que recogen los principales riesgos a los que nos exponemos al hacer uso de Internet.



#### Guía para familias

Guía de mediación parental para ayudar a los hijos a hacer un uso más seguro y responsable de Internet.

## Chaval.es



**chaval.es**  
en la Red | La web que te conecta con el mundo

Programa de referencia para el buen uso de las TIC que forma e informa a padres, tutores y educadores sobre las ventajas y posibles riesgos del panorama tecnológico actual para menores y jóvenes

### Históricos de éxito

Ayudas Banda Ancha 30Mbps

Ciudades e Islas Inteligentes

Territorios Inteligentes

Pilotos 5G

Transformación digital en pymes

Profesionales digitales

Videojuegos

Escuelas Conectadas

'Cloud Computing'

Cultura digital

e-Salud

Datos Abiertos

Internacionalización

Turismo

Chaval.es

Tecnologías del Lenguaje

Fuentes abiertas y soluciones reutilizables

Servicio de Pago Telemático

Pabellones MWC & 4YFN

## Chaval.es

### Información general

Chaval.es responde a la necesidad de solventar la brecha digital entre padres, madres, tutores y educadores respecto al avance de los menores y jóvenes en el uso de las TIC. Nuestro objetivo es educar a los estímulos sobre las posibilidades de las TIC, enseñar el buen uso y promocionar roles y conferencias que les sean útiles en su relación con los jóvenes y menores.



El portal chaval.es se convierte en el lugar perfecto para encontrar consejos, guías y resolver dudas, pero también, para encontrar un listado de referencias útiles y de calidad.

Para desarrollar esta labor hemos contado con el apoyo y colaboración de organizaciones e instituciones públicas y del sector privado.

También puedes encontrar más información referente a menores en la red en <https://www.4yfn.es/>.

[Hazte socio](#)[Quiénes somos](#)[Programas](#)[Cómo ayudar](#)[Actualidad](#)[Documentación](#)

## OBJETIVO ANAR

Ayuda a Niños y Adolescentes en Riesgo

[Firma la petición >>](#)

### ANAR en España

- [Teléfono de Ayuda a Niños y Adolescentes](#)
- [Teléfono del Adulto y la Familia](#)
- [Teléfono para Casos de Niños Desaparecidos](#)
- [Chat Anar](#)
- [Email](#)
- [Colegios e Institutos](#)
- [Hogares de Acogida](#)

### ANAR en Latinoamérica

[Hazte socio](#)[Haz una donación](#)[Hazte voluntario](#)[Si eres empresa](#)

**OBJETIVO ANAR**  
Ayuda a Niños y Adolescentes en Riesgo

Cero Violencia contra la Infancia

[Firma la petición](#)



- Blog
- Mediateca
- Canal PantallasAmigas



#### RECURSOS DIDÁCTICOS PREVENCIÓN

Recursos didácticos prevención

#### ÚLTIMOS POST

La Policía de varios países combate la sextorsión con videos de PantallasAmigas

Videojuegos: Fortnite como eSport, talleres de Roblox y protagonismo femenino en el Fun & Serious Game Festival 2018

Día internacional de los derechos de la infancia, también en Internet, #20N



#### LA POLICIA DE VARIOS PAISES COMBATE LA SEXTORSIÓN CON VÍDEOS DE PANTALLASAMIGAS

Dic. 18, 2018 | Blog, Ciberdelitos, Información, Mediateca, Televisión, Video | 0  
La sextorsión, el chantaje realizado a partir de la posesión por parte de otra persona de una...

Videojuegos: Fortnite como eSport, talleres de Roblox y protagonismo femenino en el Fun & Serious Game Festival 2018

Dic. 13, 2018 | Blog, Ciudadanía Digital, Videogames / videojuegos | 0



#### USO SEGURO Y RESPONSABLE DE LAS NUEVAS

##### TECNOLOGÍAS EN MENORES

Nov. 23, 2015 | Entrevista, Información, Mediateca, Televisión, Video | 0  
Ficha Técnica: Televisión Canaria entrevista a Jorge Flores en torno a la charla ofrecida por...

¿Cómo se efectúa un chantaje sexual en Internet?  
Oct. 23, 2015 | Entrevista, Mediateca, Reportaje, Televisión, Video | 0

Analísisis sobre uso imprudente de las redes sociales en adolescentes y jóvenes en edades tempranas



PantallasAmigas es una iniciativa social

## The BeSmartOnline Project

The project is implemented through a consortium coordinated by the Malta Communications Authority (MCA) and brings together FSW5 Agenzia Appogg, the Office of the Commissioner for Children and the Directorate for Learning and Assessment Programmes (DLAP) particularly the PSCD Department. The consortium is supported by the expertise and experience of a number of strategic partners' who contribute through a purposely set up Advisory Board.

All partners work together to raise awareness and educate children and teens, parents/carers and educators on the safer use of the Internet. The partners also established and promotes [www.childwebalert.gov.mt](http://www.childwebalert.gov.mt), an online reporting facility for illegal online content, particularly child abuse material and offers support services to respective victims.



### Helpline

The internet helpline is an extension of Support line 179 and aims to offer support to individuals that reach them via telephone on free phone 179 or email 179.appogg@gov.mt

### Hotline

The Hotline is an online reporting system which provides a secure and confidential environment where members of the public can anonymously report websites that host content related to online child abuse. Reports are received through [www.childwebalert.gov.mt](http://www.childwebalert.gov.mt)

### Youth Panel

Young people have a right to participate and be involved in decisions and initiatives that concern them. The BeSmartOnline Awareness team rely on children and young people themselves to keep up to date with new trends and also to identify the most effective ways of creating awareness about online safety for children.

### Partners



### Supporting Partners



Directorate for Educational Services  
Secretariat for Catholic Education



# Delitos de hacking:

- Se modifican los delitos relativos a la intromisión en la intimidad de los ciudadanos (art. 197) con el fin de adaptar la legislación española a la normativa europea transponiendo la Directiva 2013/40/UE, de 12 de agosto, relativa a los ataques contra los sistemas de información y la interceptación de datos electrónicos cuando no se trata de una comunicación personal.
  - Se solucionan ciertos problemas de falta de tipicidad de algunas conductas que hasta el momento no aparecían recogidas de forma específica y suponían problemas de interpretación.
  - Se opta por la tipificación separada y diferenciada del mero acceso a los sistemas informáticos.
  - Con el mismo planteamiento, y de acuerdo con las exigencias de la Directiva, se incluye la tipificación de la interceptación de transmisiones entre sistemas, cuando no se trata de transmisiones personales: la interceptación de comunicaciones personales ya estaba tipificada en el Código Penal; ahora se trata de tipificar las transmisiones automáticas –no personales– entre equipos.
  - Se tipifica la facilitación o la producción sin autorización de programas informáticos o equipos específicamente diseñados o adaptados para la comisión de estos delitos.
  - Se regulan separadamente, de un modo que permite ofrecer diferentes niveles de respuesta a la diferente gravedad de los hechos, los supuestos de daños informáticos y las interferencias en los sistemas de información.
  - Finalmente, en estos delitos se prevé la responsabilidad de las personas jurídicas.

# Se penaliza la PORNOVENGANZA o **revenge porn**:

- Dentro de los delitos contra la intimidad (art. 197) se castiga de forma específica aquellos supuestos en los que se divultan sin consentimiento las imágenes o grabaciones de tipo íntimo de otra persona, aunque en su día se obtuvieran con el consentimiento de la víctima. Conducta que se ha convertido en una forma de venganza habitual entre ex parejas una vez acabada la relación y que puede suponer un grave lesión a la intimidad. De ahí que el legislador haya previsto dentro de este delito un tipo agravado cuando esta conducta se realice entre cónyuges o personas unidas por análoga relación de afectividad.

# Delitos contra la propiedad intelectual e industrial:

- Entre otros aspectos se tipifican expresamente la neutralización de las medidas tecnológicas utilizadas para evitar el plagio y demás conductas asociadas a estos delitos, la elusión o facilitación de la elusión de las medidas tecnológicas de protección de la propiedad intelectual llevada a cabo con la finalidad de facilitar a terceros el acceso no autorizado a las mismas, cuando esta conducta se ejecuta con intención de obtener un beneficio económico directo o indirecto.
  - Se tipifica la facilitación del acceso o localización de obras o prestaciones protegidas ofrecidas en internet en forma no autorizada. En estos casos, la orden de retirada de las obras o prestaciones objeto de la infracción dispuesta por la autoridad judicial estará referida tanto a los archivos que contengan las obras o prestaciones protegidas como a los enlaces u otros medios de localización de las mismas.
  - Las modificaciones anteriores no afectan a quienes desarrollen actividades de mera intermediación técnica, como los motores de búsqueda entendiendo que realizan una actividad neutral de búsqueda de contenidos o que meramente enlazan ocasionalmente a tales contenidos de terceros.

# Delitos de incitación al odio y a la violencia:

- Se prevé una agravación de la pena para los supuestos de comisión de estos delitos a través de internet u otros medios de comunicación social, así como para los supuestos en los que se trate de conductas que, por sus circunstancias, o por el contexto en el que se produzcan, resulten idóneas para alterar la paz pública o menoscabar gravemente el sentimiento de seguridad de los integrantes de los grupos afectados.
- *¿ley mordaza? Caso 15-M, asaltemos el Congreso.*

# En relación con la **intimidad**:

- El Artículo 197 sobre **descubrimiento y revelación de secretos**, distingue entre revelación de datos que afectan a la intimidad personal y los que afectan solo a la privacidad. Introduce la conducta delictiva de aquel que, con conocimiento de su origen ilícito y sin haber tomado parte en su descubrimiento, difunde, revela o cede a terceros los datos o hechos descubiertos o las imágenes captadas. También tipifica los supuestos en que las imágenes o grabaciones de otra persona se obtienen con su consentimiento pero luego se divultan contra su voluntad.
- El Artículo 197 bis tipifica el nuevo precepto de **ciberespionaje, black hacking, cracking, accesos no autorizados**: “El que por cualquier medio o procedimiento, vulnerando las medidas de seguridad establecidas para impedirlo, y sin estar debidamente autorizado, acceda o facilite a otro el acceso al conjunto o una parte de un sistema de información o se mantenga en él en contra de la voluntad de quien tenga el legítimo derecho a excluirlo” y “El que mediante la utilización de artificios o instrumentos técnicos, y sin estar debidamente autorizado, intercepte transmisiones no públicas de datos informáticos que se produzcan desde, hacia o dentro de un sistema de información”.
- El Artículo 197 ter establece asimismo que “será castigado con una pena de **prisión** de seis meses a dos años o **multa** de tres a dieciocho meses el que, sin estar debidamente autorizado, produzca, adquiera para su uso, importe o, de cualquier modo, facilite a terceros, con la intención de facilitar la comisión de alguno de los delitos a que se refieren los apartados 1 y 2 del artículo 197 o el artículo 197 bis: un programa informático, concebido o adaptado principalmente para cometer dichos delitos; o una contraseña de ordenador, un código de acceso o datos similares que permitan acceder a la totalidad o a una parte de un sistema de información”.

# En relación con los daños informáticos:

- Los **Artículos 264, 264 bis y 264 ter** tipifican el “sabotaje informático”: “El que por cualquier medio, sin autorización y de manera grave borrase, dañase, deteriorase, alterase, suprimiese o hiciese inaccesibles datos informáticos, programas informáticos o documentos electrónicos ajenos, cuando el resultado producido fuera grave”, “El que, sin estar autorizado y de manera grave, obstaculizara o interrumpiera el funcionamiento de un sistema informático ajeno”, y “El que, sin estar debidamente autorizado, produzca, adquiera para su uso, importe o, de cualquier modo, facilite a terceros, con la intención de facilitar la comisión de alguno de los delitos a que se refieren los dos artículos anteriores: un programa informático, concebido o adaptado principalmente para cometer alguno de los delitos a que se refieren los dos artículos anteriores; o una contraseña de ordenador, un código de acceso o datos similares que permitan acceder a la totalidad o a una parte de un sistema de información”.

## En relación a la **propiedad intelectual**:

- El Artículo 270.2 tipifica las **páginas de enlaces** castigando a quien, “en la prestación de servicios de la sociedad de la información, con ánimo de obtener un beneficio económico directo o indirecto, y en perjuicio de tercero, facilite de modo activo y no neutral y sin limitarse a un tratamiento meramente técnico, el acceso o la localización en Internet de obras o prestaciones objeto de propiedad intelectual sin la autorización de los titulares de los correspondientes derechos o de sus cesionarios, en particular ofreciendo listados ordenados y clasificados de enlaces a las obras y contenidos referidos anteriormente”.

# En relación al ejercicio de los **derechos fundamentales y libertades públicas**:

- El **Artículo 510** penaliza la **incitación al odio y a la violencia** agravada “cuando se hubiera llevado a cabo a través de un medio de comunicación social, por medio de Internet o mediante el uso de tecnologías de la información”.
- Desde el INCIBE se señala que, pese a ser una amplia reforma, parece que se ha perdido la oportunidad de incluir otras conductas como puede ser la **suplantación de identidad**. En cuanto a las indefiniciones y conceptos indeterminados existentes deberemos esperar a las distintas interpretaciones que hagan los jueces y tribunales.

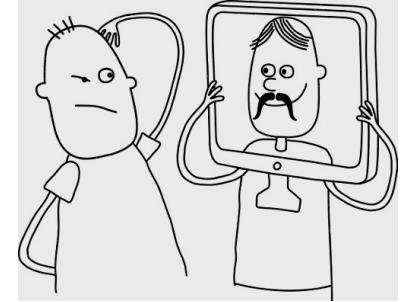
# Agrava las penas por el uso de software ilegal:

- Una de sus novedades es que se agravan las consecuencias penales derivadas del uso de software ilegal que se encuentre en los sistemas informáticos de las empresas, tanto para las organizaciones como para los administradores de las mismas.
- Las penas aplicables a las **personas jurídicas** pueden ser de multa de hasta 280.000 euros; disolución de la persona jurídica; suspensión de las actividades por un plazo que no podrá exceder de cinco años; prohibición de realizar en el futuro actividades en cuyo ejercicio se haya cometido, favorecido o encubierto el delito; inhabilitación para obtener subvenciones y ayudas públicas, o incluso intervención judicial para salvaguardar los derechos de los trabajadores o de los acreedores.
- En cuanto a los **administradores**, las penas previstas para los delitos contra la propiedad intelectual podrían alcanzar, en determinados caso, los cuatro años de privación de libertad, además de multas similares a las previstas para las personas jurídicas.
- Por tanto, “si se detecta que una organización dispone de software sin licencia, se arriesga a tener que pagar daños y perjuicios por las licencias de software que debería haber adquirido en primera instancia, además de las posibles consecuencias penales en caso de que se actué por vía criminal, y no solo civil. Además, las compañías también están obligadas a asegurarse de que todo el software está licenciado de forma adecuada de cara al futuro.

# Contenidos Inapropiados vs Contenidos Ilegales:

- Pueden ser de diverso tipo: violentos, relacionados con el consumo de sustancias estupefacientes, lenguaje soez, pornografía, pornografía con menores y contenidos pedófilos, racistas o xenófobos, la apología de terrorismo, fabricación de artefactos explosivos, armas, juegos online de adultos, juegos de azar, apuestas o, sencillamente, páginas de hábitos poco saludables ej. *Ana y Mía* (anorexia y bulimia).

# Suplantación de identidad:



- Consiste en la apropiación del nombre, contraseñas y/o patrimonio de otra persona con el fin de realizar actos delictivos.
- Sólo es delito, si lo que se usurpa es el estado civil de otro. Si me hago pasar por otra persona concreta y real van de 6 meses a 3 años de cárcel.
- Si lo que se hace es simplemente crear un perfil inventado o con datos falsos, la conducta no podría ser considerada delito.
- El hecho de que la usurpación de identidad hubiera sido una broma no exime de responsabilidad a su autor.

# Derecho al honor, a la intimidad personal y a la imagen propia:

- Protección legal:
  - Constitución (art 18.1)
  - Ley Orgánica 1/1982, de 5 de mayo, de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen.
  - Protección penal: Código Penal.

# Derecho al honor, a la intimidad personal y familiar, y a la imagen propia:

- Derecho al honor empresas y personas:
- Queda prohibida:
  - La divulgación de hechos relativos a la vida privada de una persona o familia que afecten a su reputación y buen nombre.
  - La captación, reproducción o publicación por fotografía, filme, o cualquier otro procedimiento, de la imagen de una persona en lugares o momentos de su vida privada o fuera de ellos sin su permiso (salvo excepciones).
  - La utilización del nombre, de la voz o de la imagen de una persona para fines publicitarios, comerciales o de naturaleza análoga.
  - La imputación de hechos o la manifestación de juicios de valor a través de acciones o expresiones que de cualquier modo lesionen la dignidad de otra persona, menoscabando su fama o atentando contra su propia estimación.
  - La utilización del delito por el condenado en sentencia penal firme para conseguir notoriedad pública u obtener provecho económico, o la divulgación de datos falsos sobre los hechos delictivos, cuando ello suponga el menoscabo de la dignidad de las víctimas.



# Derecho al honor, a la intimidad personal y familiar, y a la imagen propia:

## Uso de fotografías de personas:

- Norma general: sólo si tenemos consentimiento de la persona
- Uso permitido sin necesidad de permiso de fotografías de personas:
  - Imagen captada en acto público o lugar abierto al público de personas que ejerzan cargo público o profesión de notoriedad o proyección pública.
  - Información gráfica sobre suceso o acontecimiento público cuando la persona sea meramente accesoria en la imagen.
  - Caricatura de acuerdo al uso social.

Retirada en virtud de la ley de privacidad de la UE

Ayuda

## Formulario para solicitar la retirada de información personal

Por motivos de privacidad, tienes el derecho a solicitar que se retire determinada información personal sobre ti.

Este formulario sirve para solicitar que retiremos de la Búsqueda de Google resultados específicos de consultas en las que se incluya tu nombre. Si quieres solicitar la retirada de información personal de otro producto de Google, envía una solicitud a través del formulario correspondiente, que puedes encontrar en nuestra página [Cómo retirar contenido de Google](#).

Por ejemplo, si quieres retirar información personal de Blogger, envía una solicitud a través del formulario de Blogger.

Cuando envías una solicitud, en Google buscamos el equilibrio entre los derechos a la privacidad de los usuarios afectados, el interés público que pueda tener esa información y el derecho de otros usuarios a distribuirla; por ejemplo, es posible que rechacemos retirar cierta información sobre estafas financieras, negligencias profesionales, condenas penales o conductas de funcionarios.

Para completar este formulario, necesitas una copia digital de un documento de identidad. Si envías una solicitud en nombre de otra persona, tienes que facilitar su documento de identidad.

\* Campo obligatorio

### TU INFORMACIÓN

País de origen \*

Selección tu país o tu región

Nombre legal completo \*

Aunque envíes la solicitud en nombre de otra persona que te haya autorizado para representarla, debes indicar tu nombre. Si representas a otra persona, debes tener autoridad legal para actuar en su nombre.

Nombre:

Apellidos:

Dirección de correo electrónico de contacto \*

Actúo en nombre de... \*

Si envías esta solicitud en nombre de otra persona, tienes que especificar tu relación con ella (por ejemplo, "padre" o "abogado"). Es posible que te solicitemos documentación que confirme que estás autorizado para representarla.

Yo mismo

Cliente

Familiar

Amigo

Otros

Tu relación legal con la persona en cuyo nombre presentas esta solicitud \*

Adjuntar una copia legible de un documento que verifique la identidad de la persona en cuyo nombre se presenta la solicitud \*

Para saber quién se envían solicitudes de retirada de contenido fraudulentas procedentes de personas que se hacen pasar por otras, que intentan dañar la competencia o que quieren eliminar información legal de forma inadecuada, tenemos que verificar la identidad de la persona en cuyo nombre se realiza la solicitud (la persona correspondiente). No es necesario que sea un pasaporte ni otro documento de identificación oficial. Puedes adjuntar partes del documento que proporcionas (por ejemplo, el número de identificación), siempre que se pueda identificar a la persona correspondiente con el resto de la información. Asimismo, puedes adjuntar cualquier fotografía presente en el documento de identificación, excepto si estás solicitando que se retiren páginas con fotografías de esa persona. Google LLC solo utilizará esta información para evaluar y documentar la autenticidad de tu solicitud y eliminará la copia en un plazo de un mes una vez cerrada la solicitud, a menos que la ley establezca lo contrario.

Para subir varios documentos a la vez, mantén pulsada la tecla Ctrl o Comando al seleccionar los archivos.

No se han seleccionado archivos.

¿Has presentado una solicitud anterior?

Si tú (o la persona correspondiente) ya has solicitado que retiremos URLs con contenido similar, podremos ayudarte antes si, en lugar de enviarnos una notificación nueva, contestas a algún correo electrónico que te hayamos enviado a ti (o a la persona correspondiente).

Si prefieres enviar una notificación nueva, introduce el número de referencia de 14 dígitos que identifica tu solicitud anterior, con un formato similar a 1-1111000001111. Puedes encontrar este número en el asunto del correo electrónico que te enviamos como respuesta a tu anterior solicitud.

### IDENTIFICA LA INFORMACIÓN PERSONAL QUE QUIERES RETIRAR Y SU UBICACIÓN

Si esta notificación está relacionada con varios motivos que han sido objeto de una infracción, envía únicamente el primero aquí abajo. A continuación, haz clic en el enlace "Añadir un nuevo grupo" que aparece debajo de los cuadros de texto para añadir otro motivo.

Las URL del contenido que incluya la información personal quequieres retirar \*

[Haz clic aquí](#) para obtener ayuda con la búsqueda de la URL.

# Derecho al olvido:

- Es el derecho de la persona titular de un dato personal a que se borre, bloquee o suprima información personal que figure en internet que esté obsoleta o afecte al libre desarrollo de sus derechos fundamentales.
- Las reclamaciones se centran sobre todo en motores de búsqueda.
- St. Tribunal Superior de Justicia Europeo 13 de mayo de 2014. Caso Costeja:



Los buscadores de internet son responsables del tratamiento de los datos que recopilen de páginas web publicadas por terceros.

- Afecta a todos los buscadores.
- Afecta solo a datos de personas físicas.
- Se suprime la información de los buscadores, no de la página de destino.

# Derecho al olvido... Caso Costeja:



# Derecho al olvido:

[https://www.google.com/webmasters/tools/legal-removal-request?complaint\\_type=rtbf&visit\\_id=636821152994333903-2643050447&hl=es&rd=1](https://www.google.com/webmasters/tools/legal-removal-request?complaint_type=rtbf&visit_id=636821152994333903-2643050447&hl=es&rd=1)

Motivos para solicitarlo:



- Atenta contra el derecho a la intimidad de la persona.
- Contenido injurioso o difamatorio.
- Info sobre procesos judiciales.
- Robo de identidad.
- Presunción de inocencia.
- STS 964/2016, de 14 de marzo de 2016

# Derecho al olvido:

## Nuevo Reglamento Europeo de Protección de Datos:

- Mejora el derecho al olvido. Dentro del Derecho a la cancelación.
- Cuando nos demos de baja de un servicio podemos solicitar el borrado definitivo de nuestros datos personales excepto que exista una normativa que lo impida.
- Podremos solicitar a una página en Internet que elimine totalmente los datos que aparecen en su web o contiene en sus ficheros sobre nuestra persona.

