BIENVENIDOS

SESIÓN FORMATIVA

RIESGOS DE UN

CIBER ATAQUE

EN TU EMPRESA

ORGANIZA:

COLABORA:

clave i

www.elmundo.es/tecnologia/2017/05/12/59158a8ce5fdea194f8b4616.html

EM | Tecnología

TECNOLOGÍA

Hackean la red interna de Telefónica y de otras grandes empresas españolas

BRUNO TOLEDANO

12 may. 2017 | 12:31

165 Comentar

Hackean la red interna de Telefónica y de otras grandes empesas españolas

¿Quién nos ataca?

- Robots automáticos.
- Grupos Criminales.
- Países en “Ciberguerra”
- Hackers éticos.
- Empleados INTERNOS – EX EMPLEADOS.
- ¿La competencia?.

¿Quién nos ataca?

- Robots automáticos

¿Quién nos ataca?

- Países en “Ciberguerra”

hipertextual

Corea del Norte en el punto de mira por el ataque del WannaCry

TWITTEAR COMPARTIR Por A.S. 16/05/17 - 12:31

Las trazas de código y las similitudes de sus procedimientos sitúan el posible origen del WannaCry en Corea del Norte.

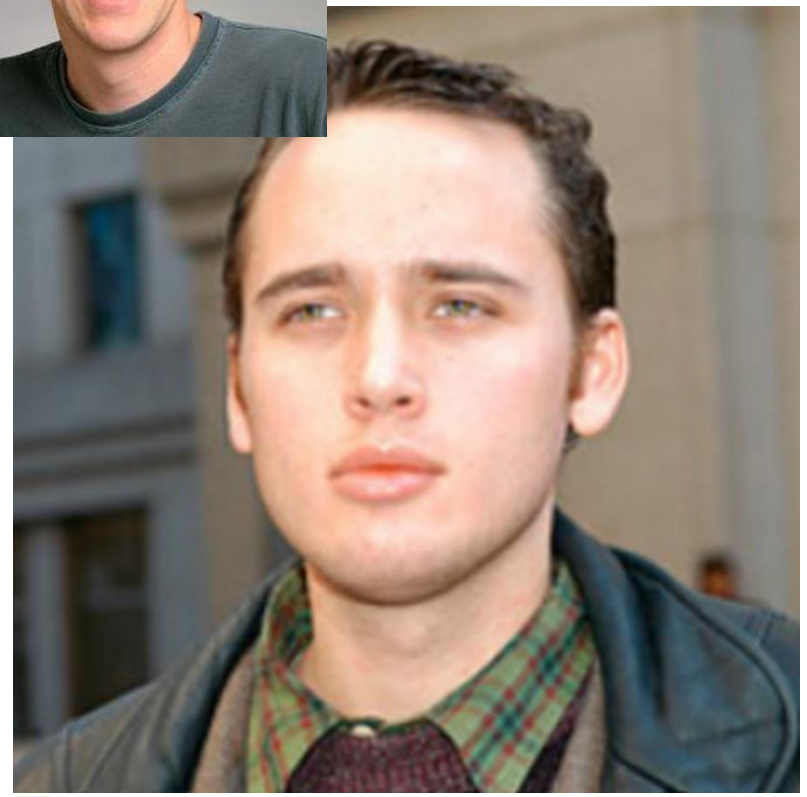
De momento no está confirmado al 100%, pero parece que las pesquisas de Estados Unidos respecto al ataque masivo con el malware WannCry residen en un origen ubicado en la cerrada Corea del Norte. Las sospechas existen sobre todo porque el ataque del viernes 13 de mayo, que ha dado la vuelta al mundo, comparte procedimientos similares con otros ataques informáticos cuyo origen, después de las investigaciones, se localizó en Corea del Norte.

¿Quién nos ataca?

- Grupos Criminales.

¿Quién nos ataca?

- Hackers éticos.



¿Quién nos ataca?

- Empleados INTERNOS –
  EX EMPLEADOS.

¿Quién nos ataca?

- La competencia?.

¿Pero… es mi empresa realmente un objetivo?


FISH McBites
HURRY. THEY WON'T LAST!
McDonalds
® USA official Twitter account. Just got sold to
McDonalds because the whopper flopped =[FREDOM IS FAILURE℠.
mcdonalds.com
In a hood near you ·
.com/press/sold-to-...
1,278
TWEETS
609
FOLLOWING
82,968
FOLLOWERS
Follow


FISH McBites
HURRY. THEY WON'T LAST!
McDonalds
@BurgerKing
BURGER KING® USA official Twitter account. Just got sold to McDonalds because the whopper flopped =[FREDOM IS FAILURE℠.
mcdonalds.com
In a hood near you · info.bk.com/press/sold-to-...
1,278
TWEETS
609
FOLLOWING
82,968
FOLLOWERS
Follow


CYBERTHREAT REAL-TIME MAP
KASPERSKY

clave i

¿Pero… es mi empresa realmente un objetivo?

MENÚ BUSCAR NEWSLETTER **El Confidencial** INICIA SESIÓN

Anonymous se cuela en El Corte Inglés para filtrar sus gastos

El grupo 'hacktivista' La Nueve, vinculado a Anonymous, ha publicado los gastos de patrocinio de El Corte Inglés en los últimos años. Destacan el golf, la religión, la vela y algunos periodistas

¿Pero… es mi empresa realmente un objetivo…?

Hello Kitty Hackeada: 3,3 millones de cuentas se han visto comprometidas

21 Dic 2015 Jeffrey Esposito Consejos, Featured Post, Noticias No hay comentarios

Con la temporada navideña a la vuelta de la esquina, deberíamos ir dejando a un lado el teclado y unirnos a la alegría característica de esta temporada. Por desgracia, los cibercriminales se han asegurado de que tengamos al menos una noticia más con la que advertiros sobre los peligros de la red antes de la llegada de Papá Noel.

¿Pero… es mi empresa realmente un objetivo…?

Fisher-Price's cuddly Smart Toy Bear was open to hackers

¿Pero… es mi empresa realmente un objetivo…?

¿Pero… es mi empresa realmente un objetivo…?

¿Pero… es mi empresa realmente un objetivo…?

¿Pero… es mi empresa realmente un objetivo?

¿Pero… es mi empresa realmente un objetivo?

¿Pero… es mi empresa realmente un objetivo?

¿Pero… es mi empresa realmente un objetivo?

¿Pero… es mi empresa realmente un objetivo?

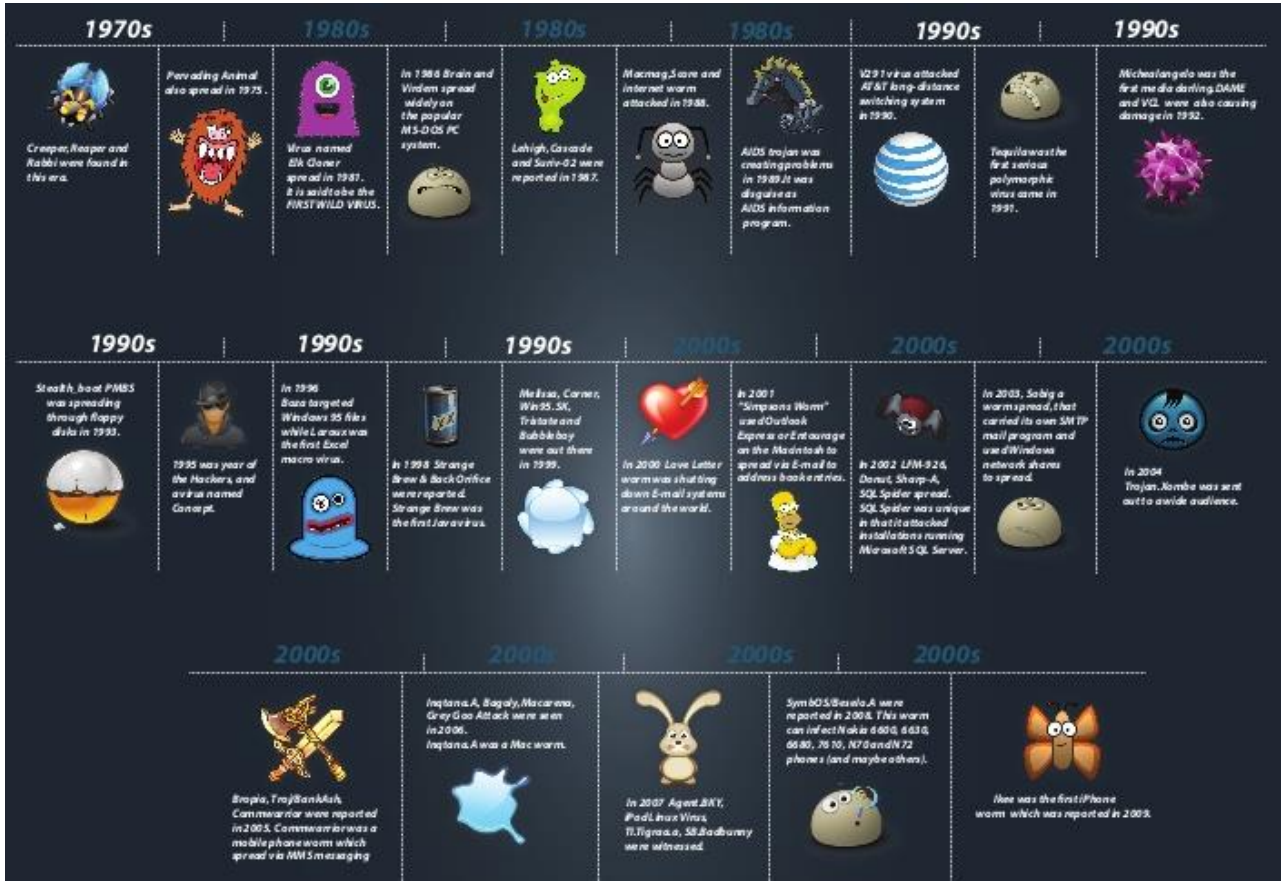
clave i

¿Pero… es mi empresa realmente un objetivo?

¿Pero… es mi empresa realmente un objetivo?

Evolución de las amenazas

- VIRUS.
- VIRUS LUCRATIVOS.
- PHISING-SPAM.
- DDOS.
- RANSOMWARE



VIRUS

- LOS CREABAN LAS EMPRESAS DE ANTIVIRUS EN LOS 90. (Leyenda Urbana¿?¿)
- LOS CREABA LA COMUNIDAD HACKER POR NOTORIEDAD.
- NO TENIAN IMPLICACIONES ECONOMICAS, MAS BIEN HUMOR.
- “FACIL” SOLUCIÓN.
- EL TIPO DISCO 3,5” DE MANO EN MANO…

VIRUS LUCRATIVOS

- LOS CREABAN Y CREAN LOS CIBERCRIMINALES.
- SU PROPÓSITO ES GANAR DINERO.
  - HABITOS DE NAVEGACION.
  - VENTA DE PRODUCTOS.
  - PAY PER CLICK
  - ETC…
- DIFICIL DETECCION.
- “FÁCIL” SOLUCIÓN.


Google - Windows Internet Explorer
google.com
File Edit View Favorites Tools Help
bing
Google
Search
Search Facebook
Quick Links
Login to Facebook
Images
Weather
News
Maps
Options
Duluth, GA (30097)
54° F Rain
Weekend
10 Day
Check traffic delays
WEB SEARCH
My Apps
Charter
Search
Options
Weather
Bookmarks
JobsInsider
SEARCH
AOL
Mail
Radio
eBay
Sign In
Norton
Cards & Log-ins
Favorites
Google
Page
Safety
Tools
Web Images Videos Maps News Shopping Gmail more
iGoogle | Search settings | Sign in
Google
Internet
100%
start


Personal Antivirus
Personal Antivirus
System is in Danger
Support
Home
Cleanup
Security
Updates
Settings
Security is at risk! Protection disabled
Computer automatic protection against viruses and other security threats not found.
Protection: Low
Low
Medium
Good
Virus protection
Not Found
Spyware protection
Not Found
Windows Protection
Not Found
Automatic update (Last Update 03/15/2009)
Not Found
Recommended: Click "Protect PC" to protect your PC
Protect PC Now
Application status: Trial
Application version
2.0.0.1
Database version
2.4.2.5
License expiry date: Get license key
Your security status: At Risk
Enter activation key
Action: Main window
Database: 2.4.2.5 12/24/2008 Update
OS: Windows XP
RAM: 1323 MBytes

PHISING- SPAM

- LOS CREABAN Y CREAN LOS CIBERCRIMINALES.
- SU PROPÓSITO ES GANAR DINERO.
  - ROBO DE CREDENCIALES.
  - TIMO NIGERIANO.
  - ETC
- DIFICIL DETECCIÓN.
- SOLUCION A VECES COMPLEJA.

C & AIR DIPLOMATIC COURIER SERVICES

Treasurers & Security Deposit Bureau

LAGOS-NIGERIA

DEPOSIT CERTIFICATE

><N0. 03839817PSFTF-01><

C &DCS DESPATCHED

Certificate of Deposit

This is to Certify that

PRESIDENT SANI ABACHA

HAS DEPOSITED WITH DIPLOMATIC CARRIAGE SERVICES LTD. FOUR (4) TRUNK BOXES OF PERSONAL TREASURES

PURPOSE OF DEPOSIT: SAFE KEEPING

REFERENCE CODE: CD/ST-03/195018

SECURITY CHECK REPORT: CONFIRMED O.K

DEPOSIT NUMBER: 03839817PSFTF-01

RELEASE CODE: SECRET

GIVEN UNDER MY HAND THIS 10TH DAY OF JULY 19 97

ISSUING OFFICER IN CHARGE: MR. JOHNSON IBEH

Depositor's Signature: Sony Abacha

Authorised Signature:

THIS CERTIFICATE IS THE SPECIMEN AND VALID DOCUMENT FROM THE TREASURER SECURITY DEPARTMENT OF C & AIR DIPLOMATIC COURIER SERVICES THE AGREEMENT THEREIN ARE TRUE, CORRECT AND BINDING ON THE PARTIES. ANY ALTERATION(S) MADE ON THIS SPECIMEN AFTER IT HAS BEEN LEGALLY ISSUED AND ACCEPTED RENDERS THIS DOCUMENT VALUELESS, NULL AND VOID. THIS DOCUMENT MUST BE PRESENTED FOR CLAIM OF DEPOSITED ITEM(S).

De Cajamar <info@cajamar.es>
Asunto **Nueva pagina web!** 9:36
A [redacted]
Fecha 09 Nov 2015 09:36:37 +0100
Message ID <20151109093637.80DB9F819DBB81E2@cajamar.es>
Return-Path [redacted]

Estimado cliente:

Bienvenido a nuestra nueva pagina web.

Para poder acceder a nuestra pagina teneis que completar el formulario adjuntado a este correo electronico.

Vuestra cuenta empieza ser activa despues de completar el formulario adjuntado a este correo electronico .

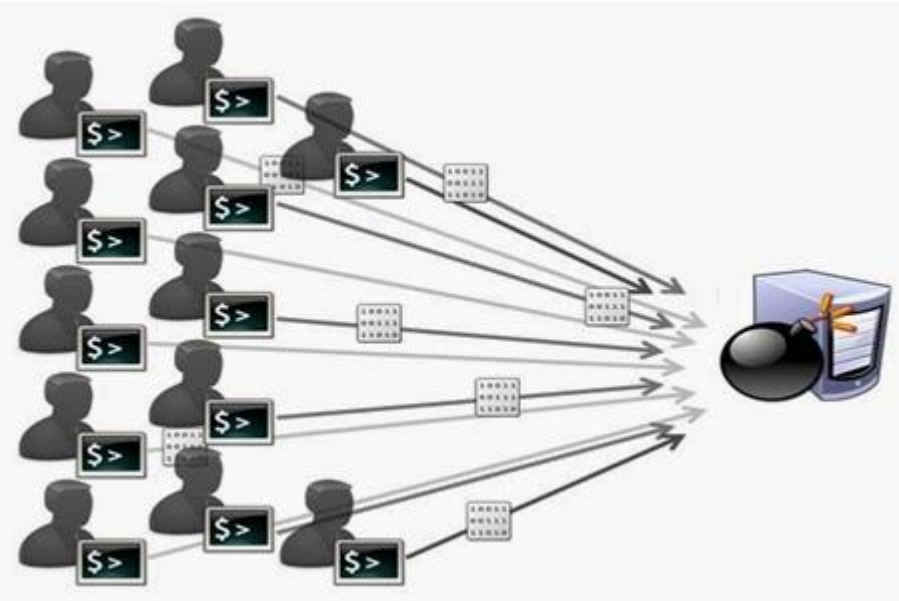
Esto solo le va a costar unos minutos de su tiempo y va a tener una seguridad mucho mas estable.

Para confirmar la reactivacion por favor descargue y complete el formulario adjuntado a este correo electronico.

DOS+DOS = DDOS

DOS: Denial Of Services –Denegación de servicio.

DDOS: Distributed Denial Of Services.



http://www.digitalattackmap.com/

DOS+DOS = DDOS

DOS: Denial Of Services –Denegación de servicio.

EFICIENCIA

Business Value Exchange Conoce Dell Movilidad empresarial Computerworld University

TENDENCIAS | NOTICIAS | 01 ABR 2016

El 68% de las empresas españolas expuestas a ataques DDoS

Tags: Bases de Datos Seguridad Informativo Ciberseguridad Amenazas

También te puede interesar:

- Disminuye el alcance de los ataques DDoS, pero aumenta su sofisticación
- El 12% de las empresas españolas atribuyen ataques DDoS a sus competidores
- Aumentarán los ataques DDoS utilizados como cortina de humo
- Los ataques DDoS experimentan una subida anual del 180%

Aunque la mayoría de las compañías conocen la importancia de tener sistemas a

solo un 31% cuentan con un sistema completo de protección

MEJORAR LA EFICIENCIA

Login con o Crea una nueva cuenta

Business Value Exchange Conoce Dell Movilidad empresarial Computerworld Univer

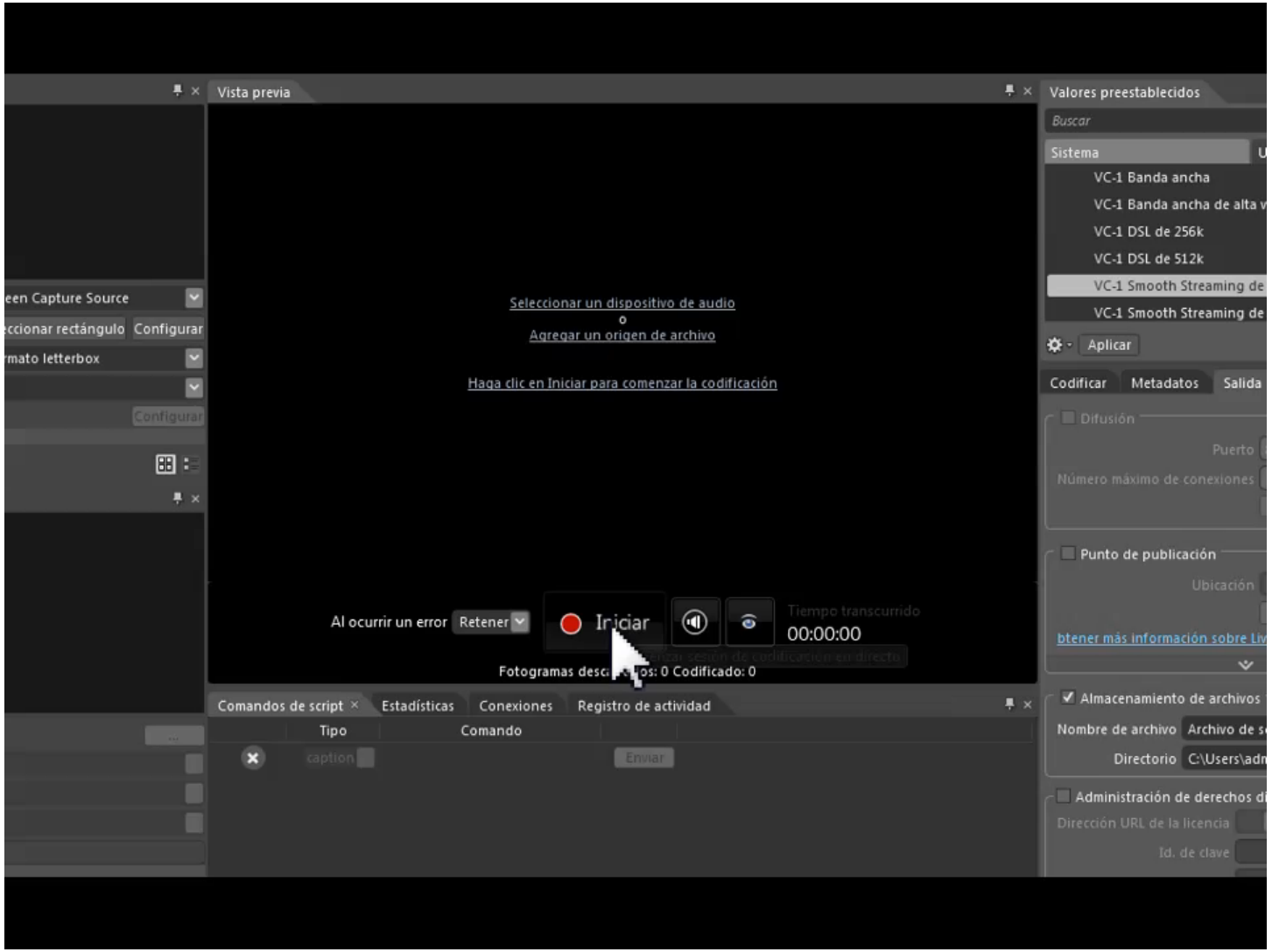
CIBERCRIMEN | NOTICIAS | 26 ENE 2016

El 12% de las empresas españolas atribuyen DDoS a sus competidores

Tags: Seguridad Amenazas

También te puede interesar:

- Aumentarán los ataques DDoS utilizados como cortina de humo
- Los ataques DDoS experimentan una subida anual del 180%
- ¿Qué sectores son objetivo de los ataques DDoS?
- Crecen las amenazas de ataques DDoS contra proveedores de hosting
- El 95% de los ataques DDoS son de corta duración


Vista previa
Seleccionar un dispositivo de audio
o
Agregar un origen de archivo
Haga clic en Iniciar para comenzar la codificación
Al ocurrir un error
Retener
Iniciar
Tiempo transcurrido
00:00:00
Comandos de script
Estadísticas
Conexiones
Registro de actividad
Tipo
Comando
Enviar
Valores preestablecidos
Buscar
Sistema
VC-1 Banda ancha
VC-1 DSL de 256k
VC-1 DSL de 512k
VC-1 Smooth Streaming de
Aplicar
Codificar
Metadatos
Salida
Difusión
Puerto
Número máximo de conexiones
Punto de publicación
Ubicación
Almacenamiento de archivos
Nombre de archivo
Directorio

RANSOMWARE

- LOS CREAN LOS CIBERCRIMINALES.
- SU PROPÓSITO ES GANAR DINERO. SECUESTRO
- DIFICIL DETECCIÓN.
- CASI IMPOSIBLE SOLUCIÓN UNA VEZ PRODUCIDO EL ATAQUE.

clave i

GOBIERNO DE ESPAÑA | MINISTERIO DEL INTERIOR

Cuerpo Nacional de Policía
Dirección General de la Policía

Se bloquea el proveedor de servicios de Internet

El trabajo del equipo ha sido suspendido por motivos de cyberactivity autorizado

Su dirección IP: [redacted]

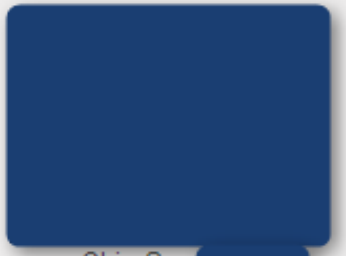
Su Proveedor: [redacted]

Ubicación: [redacted]

Todos los actos ilegales cometidos por el equipo que han sido almacenados para su posterior identificación en la base de datos de la policía, incluyendo fotos y videos de webcam. Del mismo modo, no se encontró el juego de la pornografía con menores de edad.

Gabriela [redacted]
Fecha de nacimiento: 04-18-2002
Ciudadano de México

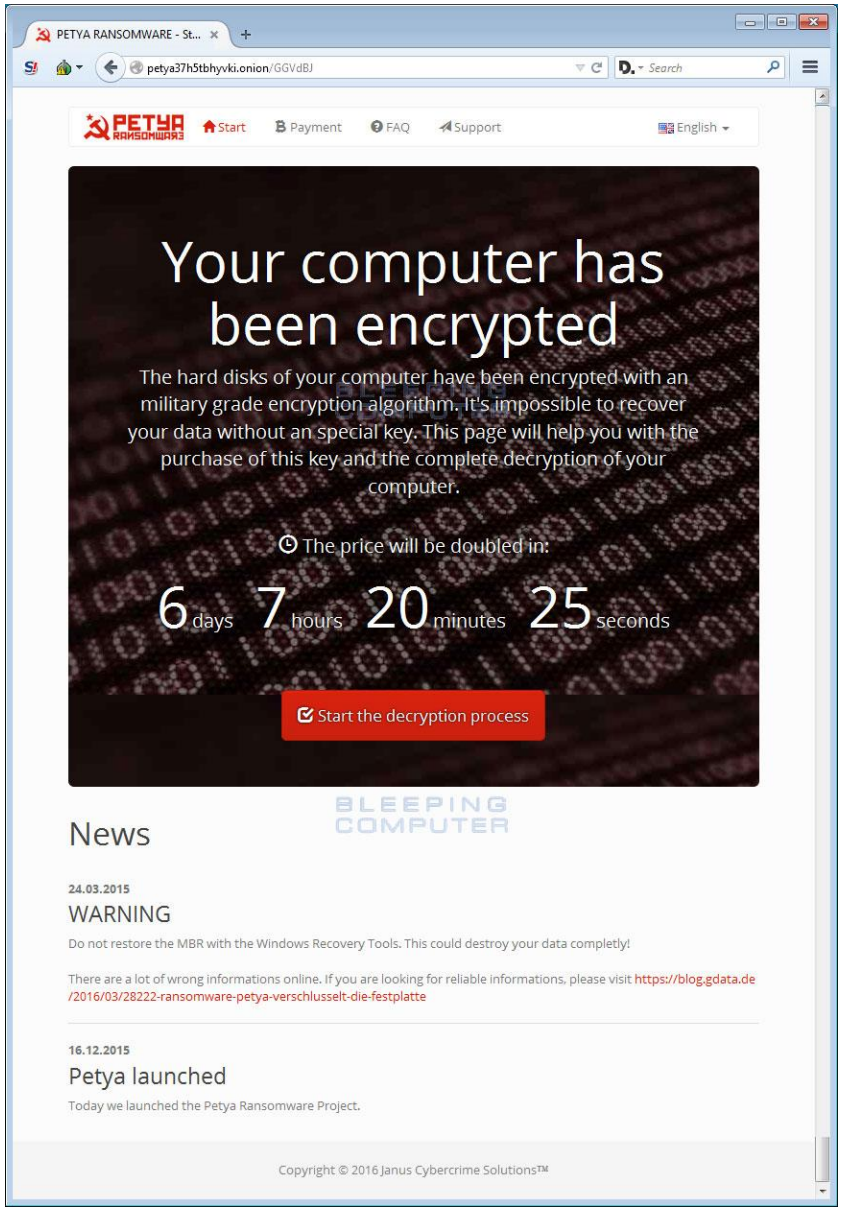
Linda [redacted]
Fecha de nacimiento: 03-24-2001
Ciudadanos de USA

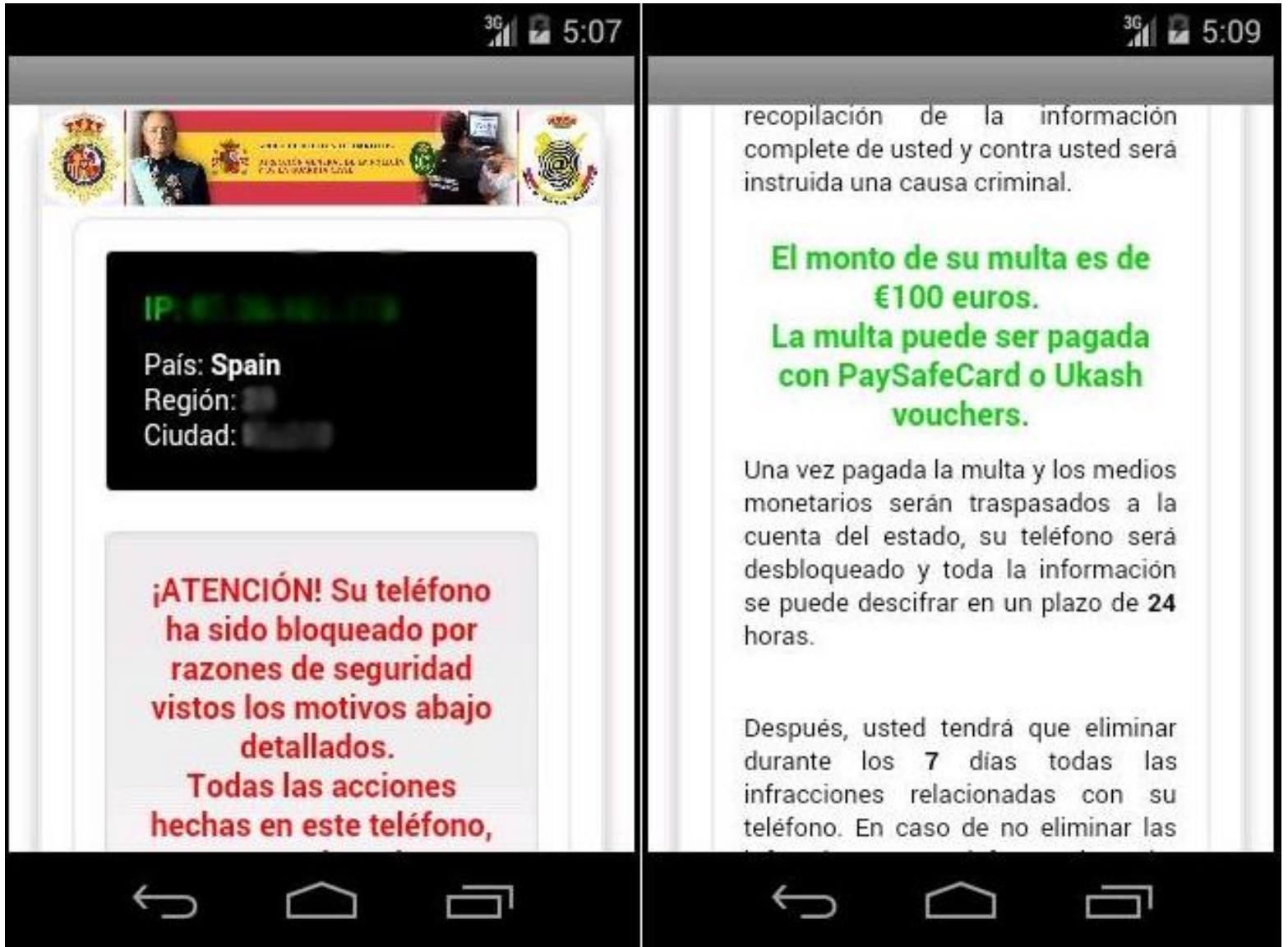


Chin-Sun [redacted]
Fecha de nacimiento: 08-11-2003
Ciudadanos de Korea

Ashlee [redacted]
Fecha de nacimiento: 12-04-2000
Ciudadanos de USA


GOBIERNO DE ESPAÑA
CUERPO NACIONAL DE POLICÍA
BRIGADA DE INVESTIGACIÓN TECNOLÓGICA
POLICIA
Atención!
Fue detectado un caso de actividad ilegal. El sistema operativo fue bloqueado por violación de las leyes de España! Fue detectada la siguiente infracción:
Desde su dirección IP bajo el número [redacted] fue efectuado un acceso a páginas de internet que contienen pornografía, pornografía infantil, zoofilia, asimismo como violencia sobre los menores. En su ordenador asimismo fueron encontrados archivos de video que contienen pornografía, elementos de violencia y pornografía infantil. Desde el correo electrónico asimismo se realizaba envío de spam con subtexto de terrorismo. El bloqueo del ordenador se realiza para suprimir la posibilidad de acciones ilegales por su parte.
Your details:
IP:[redacted]
Location:[redacted]
ISP:[redacted]
Para quitar el bloqueo del ordenador, usted debe pagar una multa de 100 euro.
Realizar el pago a través de Ukash:
Para ello, por favor introduzca el código recibido (en caso de necesidad junto con la contraseña) en la línea del pago, y posteriormente pulse OK (si usted tiene varios códigos, introdúzcalos uno detrás de otro, y después pulse OK).
Si el sistema le genera un error, usted deberá enviar el código al correo electrónico deposito@cyber-police.net
Ukash Donde conseguir Ukash?
Puedes adquirir Ukash en cientos de miles de establecimientos en todo el mundo, en línea, a partir de carteras, en quioscos y cajeros. A continuación encontrarás dónde puedes adquirir Ukash en tu país.
cajamar
Cajamar - A partir de ahora esta disponible Ukash en todos los cajeros de Cajamar.
CAIXAGALICIA
Caixa Galicia - A partir de ahora Ukash esta disponible en todos los cajeros de Caixa Galicia.
Telefónica
Telefonica - Ahora, Ukash esta disponible en las 80.000 cabinas de Telefonica.
Cuponesprepago
Cuponesprepago - Consiga tu Ukash online a traves de su Internet Bank o utilizando tu tarjeta de credito.
epay
CORREOS
TELECOR
conalrecargas
MundiRecargas
OK


PETYA RANSOMWARE - St...
petya37h5tbhyvki.onion/GGVdBJ
Search
PETYA RANSOMWARE
Start
Payment
FAQ
Support
English
Your computer has been encrypted
The hard disks of your computer have been encrypted with an military grade encryption algorithm. It's impossible to recover your data without an special key. This page will help you with the purchase of this key and the complete decryption of your computer.
The price will be doubled in:
6 days 7 hours 20 minutes 25 seconds
Start the decryption process
BLEEPING COMPUTER
News
24.03.2015
WARNING
Do not restore the MBR with the Windows Recovery Tools. This could destroy your data completly!
There are a lot of wrong informations online. If you are looking for reliable informations, please visit https://blog.gdata.de/2016/03/28222-ransomware-petya-verschlusselt-die-festplatte
16.12.2015
Petya launched
Today we launched the Petya Ransomware Project.
Copyright © 2016 Janus Cybercrime Solutions™



RANSOMWARE


Wana Decrypt0r 2.0
English
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.
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
Payment will be raised on
5/15/2017 16:32:52
Time Left
02:23:59:49
Your files will be lost on
5/19/2017 16:32:52
Time Left
06:23:59:49
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin ACCEPTED HERE
Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
Copy
Check Payment
Decrypt

¿QUEREMOS EVITAR EL RANSOMWARE?

- Sin Antivirus/ soluciones antiramsonware.
- Sin actualizaciones del Sistema.
- Sin Backup actualizado y comprobado (restauración).
- Sin plan de contingencia.

clave i


Email
Impresora
Móvil
¿TU EMPRESA TIENE
FUGAS DE INFORMACIÓN?
Web
PenDrive
Cloud
siemlab

clave i

CONTROL DE DISPOSITIVOS

Evita que se puedan conectar dispositivos no autorizados

PREVENCIÓN DE FUGAS POR EMAIL

Registra dónde se han enviado los archivos con información sensible

CONTROL DE APLICACIONES

Bloquea aplicaciones para conseguir un entorno más seguro

CONTROL DE IMPRESIÓN

Limita qué puede ser impreso y por quién

FILTRO WEB

Deniega acceso a páginas no deseadas bloqueando categorías, y filtrando palabras clave

ADMINISTRACIÓN DEL CIFRADO

Cifra el disco y unidades virtuales para almacenar los archivos con seguridad

CLASIFICACIÓN DE INFORMACIÓN

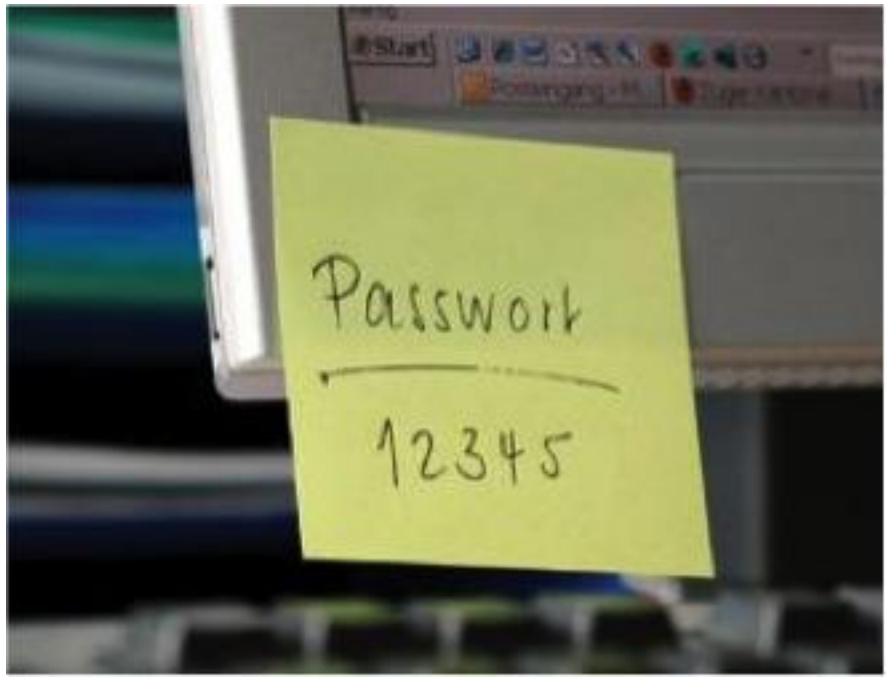
Protege la nueva información inmediatamente tras crear o recibir un archivo clasificado

MODO INFORMATIVO

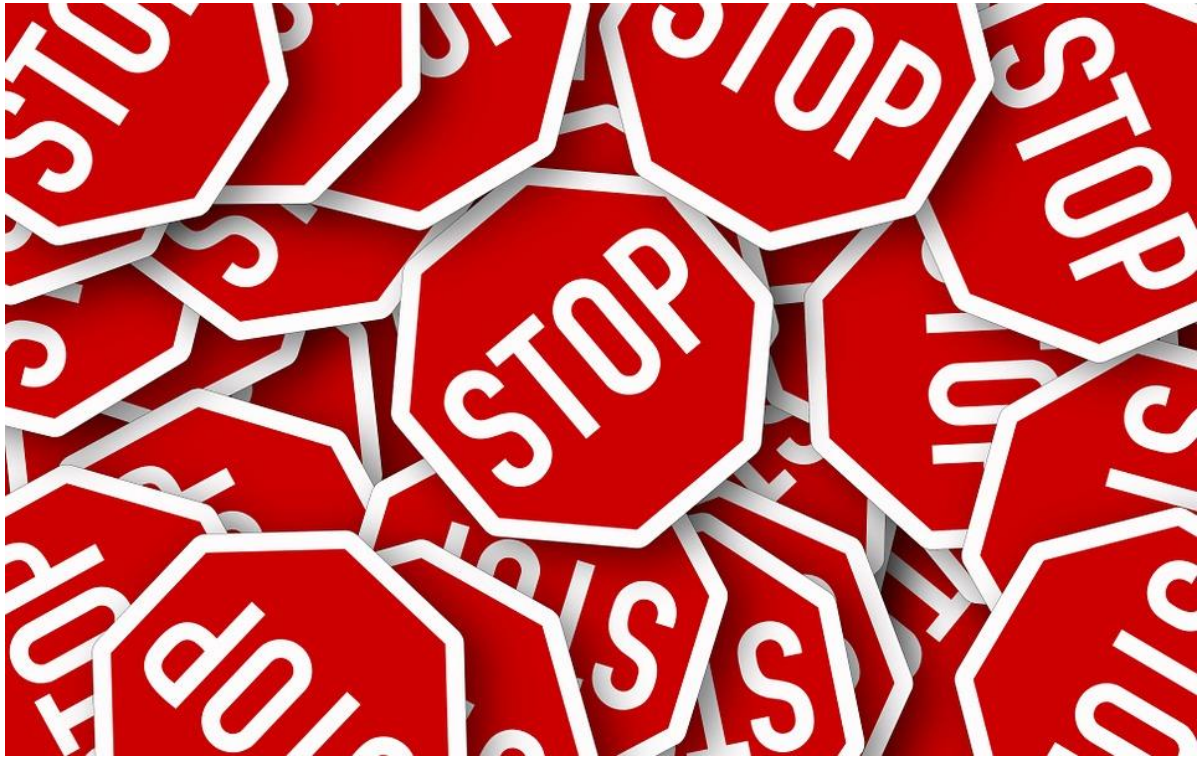
Integramos de forma progresiva la protección de información sin detenerlos procesos en la empresa

El principal culpable es el desconocimiento

"Cuando no ocurre nada, nos quejamos de lo mucho que gastamos en seguridad. Cuando algo sucede, nos lamentamos de no haber invertido más... Más vale dedicar recursos a la seguridad que convertirse en una estadística."



¿Cómo se puede proteger una Pyme frente al cibercrimen?



Buenas practicas Técnicas

- **Controles de acceso e identidad** Usuarios y passwords robustas para acceder al sistema. A partir de ahí, podremos controlar a base de políticas quien accede a la información.
- **Soluciones anti-malware y anti-fraude,** y obviamente, un buen antivirus actualizado.
- **Seguridad perimetral y control de las comunicaciones.** Cuantas empresas tienen conectado los servidores al router wifi de su proveedor de telefonía… segmentación de la red, firewalls, uso de DMZ (*zona desmilitarizada)* para aplicaciones web que dificulten el acceso a servidores, base de datos desde Internet, etc. etc.
- **Control de contenido, control de tráfico y copias de seguridad**
- **Actualizaciones de seguridad de sistemas operativos y software en general.** Normalmente las vulnerabilidades en el software y sistemas operativos son detectadas y utilizadas para tomar el control sobre nuestras infraestructuras y acceder a los sistemas. Estar al día con las actualizaciones es esencial.
- **La implementación de productos o servicios** destinados a la gestión del ciclo de vida de la información (ILM, del inglés *Information Life-Cycle Management)* o específicos para evitar la fuga de información (DLP, del inglés *Data Loss Prevention*).
- **El asesoramiento profesional**, no solo durante la gestión de un incidente (¡normalmente nos acordamos de Santa Bárbara cuando truena…error!!) sino para el diseño y mantenimiento de las medidas de prevención.

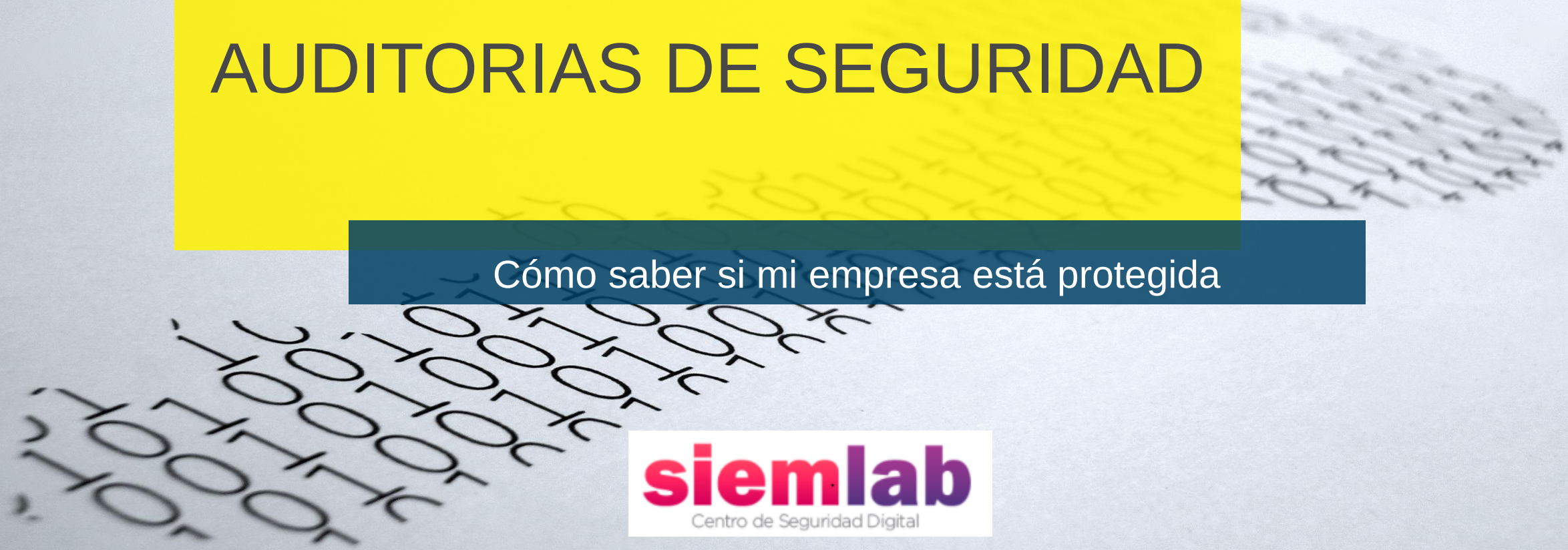
Buenas practicas organizativas

- **Clasificar la Información**: Esto es obvio. No podemos limitar el acceso a la información si no tenemos claro que es confidencial y quien debe acceder a ella. Esta confidencialidad puede establecerse dependiendo del valor que tenga para la organización, el nivel de sensibilidad, si tiene datos de carácter personal, etc.
- **Desarrollar políticas de acceso a la información**: como hemos dicho, un usuario solo debe tener acceso a la información confidencial estrictamente necesaria para su trabajo diario y debe ser informado de los límites de su trabajo diario y los procedimientos para disminuir el riesgo en aquellas actividades que puedan implicar fugas de información. Es muy importante que en las organizaciones existan acuerdos de confidencialidad con los empleados. Dichos acuerdos, además de otras medidas, pueden servir como elementos disuasorios para evitar usos malintencionados de la información.
- **La formación de los usuarios**: En este punto hay que tener dos conceptos muy claros. La ciberseguridad total no existe y la información es manipulada por personas. Existe el factor humano y, por consiguiente, el error humano. "*El usuario es el eslabón más importante de la cadena*". La fuga de información, voluntaria o no, tiene un componente humano, ya sea por motivaciones económicas, personales o el simple y el comentado **error humano**.

clave i

AUDITORIAS DE SEGURIDAD

Cómo saber si mi empresa está protegida



siemlab
Centro de Seguridad Digital

clave i

THE
ITALIAN JOB

Tipos de auditoría

- **Auditoría de seguridad interna:** En este tipo de auditoría se contrasta el nivel de seguridad y privacidad de las redes locales y corporativas de carácter interno.
- **Auditoría de seguridad perimetral:** En este tipo de análisis, el perímetro de la red local o corporativa es estudiado y se analiza el grado de seguridad que ofrece en las entradas exteriores.
- **Test de intrusión:** El test de intrusión es un método de auditoría mediante el cual se intenta acceder a los sistemas, para comprobar el nivel de resistencia a la intrusión no deseada. Es un complemento fundamental para la auditoría perimetral.
- **Análisis forense:** El análisis forense es una metodología de estudio ideal para el análisis posterior de incidentes, mediante el cual se trata de reconstruir cómo se ha penetrado en el sistema, a la par que se valoran los daños ocasionados. Si los daños han provocado la inoperabilidad del sistema, el análisis se denomina análisis postmortem.

clave i

ALGUNA PREGUNTA +

clavei

Carlos A. Rodriguez

carodriguez@clavei.es

@carlos_dhe

www.clavei.es/sistemas

siemlab Web de Seguridad Digital

Microsoft Partner Gold Desarrollo de aplicaciones

Preferred Partner