



Comprometidos con la seguridad

Más allá de la gestión del tráfico: Gestión de la seguridad y el fraude en el sector de las telecomunicaciones

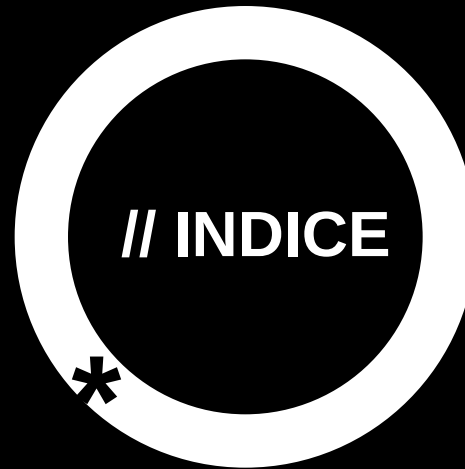
Conferencia Universidad de Granada

ETS Ingenierías Informática y de Telecomunicación



Autor: Álvaro Del Hoyo

Fecha: 14 Mayo 2012



1

Introducción

2

Algunos
problemas de
seguridad

3

Algunos
problemas de
fraude

4

Evolución, a
peor, del
problema

5

Obligaciones
de los
operadores

6

Gestión
seguridad y
lucha contra
fraude

//01

Introducción

*

En una sociedad hiperconectada...



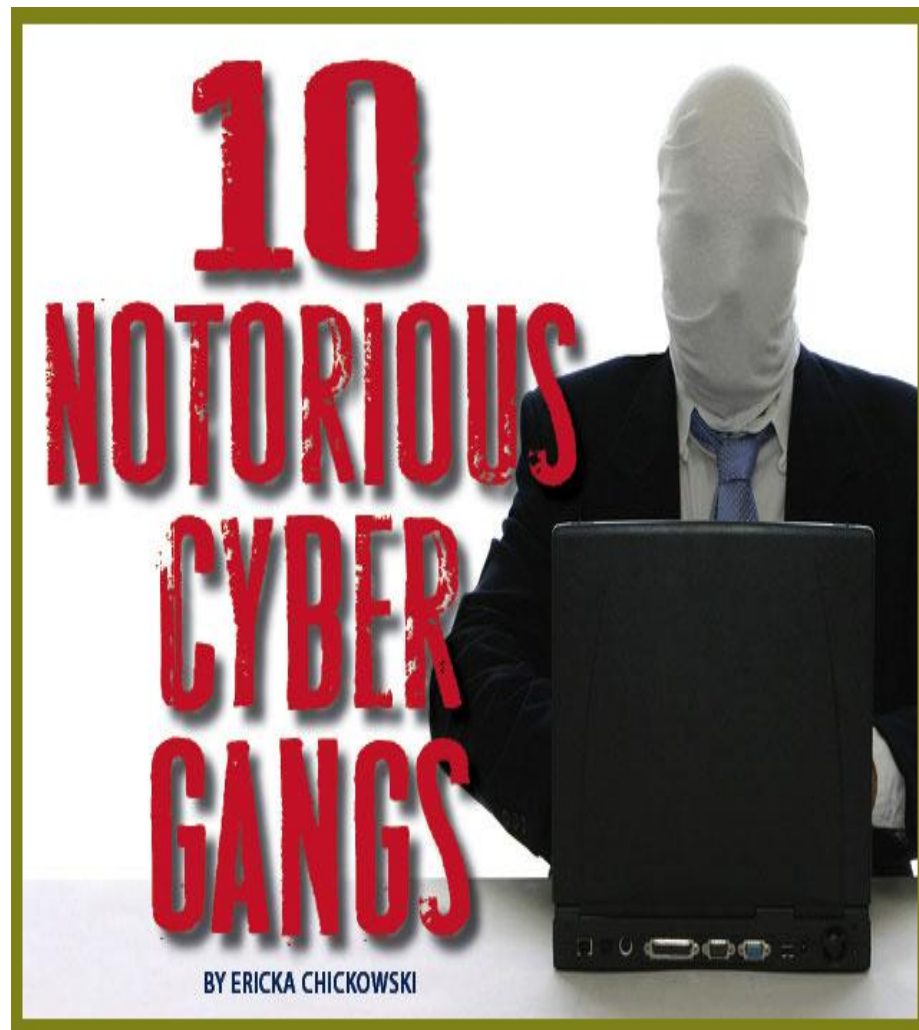
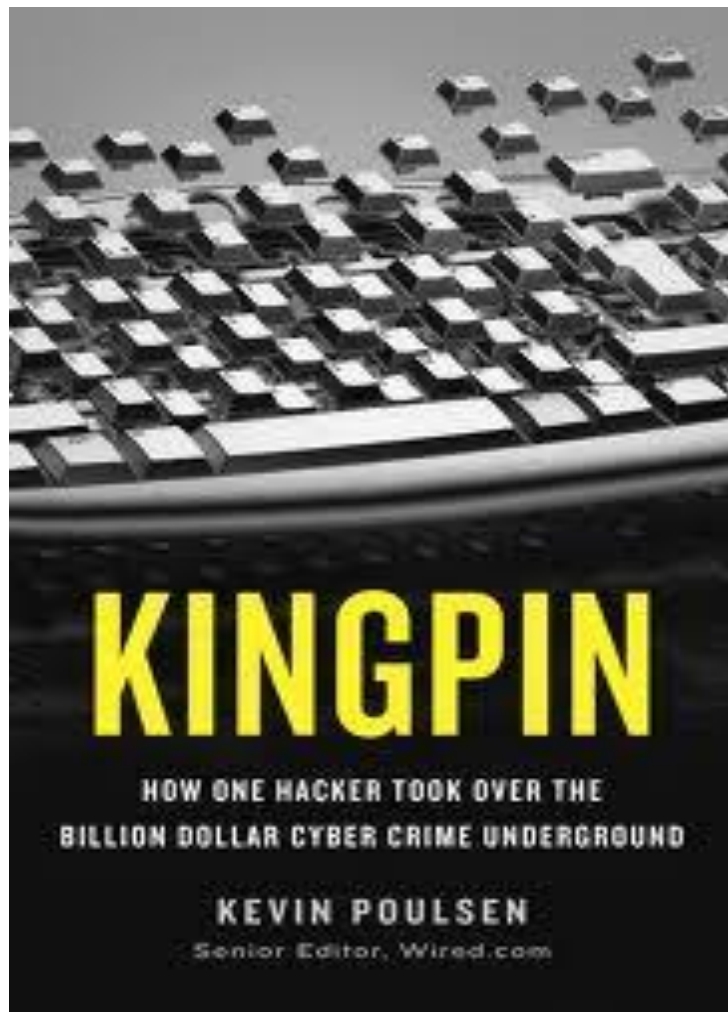
...donde la información es clave...



..., de ahí, la llegada de la cibercriminalidad...



...y la profesionalización del cibercrimen...



..., donde las empresas TICs son esenciales...



...como lo es también la seguridad de las infraestructuras, servicios, aplicaciones e informaciones...



... para generar y retener confianza



//02

**Algunos
problemas de
seguridad**

*

Ataques de denegación de servicio

EL PAÍS.com | Tecnología

Jueves, 8/9/2011, 11:21 h

Inicio Internacional Política España Deportes Economía **Tecnología** Cultura Gente y TV Sociedad Opinión Blogs In English

ELPAÍS.com > Tecnología

CiberP@is volver a tecnología

El ataque de Anonymous contra Telefónica se salda con pequeños incidentes

La página de Movistar estuvo bloqueada o inoperativa cerca de media hora, pero a las cinco y media estaba restablecida

EL PAÍS - Madrid - 26/06/2011

Vota ☆☆☆☆☆ Resultado ★★★★★ 40 votos

Twitter 160

Recomendar 10

El ataque del [colectivo de ciberactivistas Anonymous](#) contra la página web de [Movistar](#), la marca comercial de Telefónica, se ha saldado con pequeños incidentes pero en la mayor parte del día ha funcionado correctamente, según ha constatado este diario hasta las seis y media de la tarde.

Somos Anonymous

Anonymous descrito por un anonymous

La noticia en otros webs

- webs en español
- en otros idiomas

El mayor ataque se produjo a las cinco de la tarde y la página de Movistar estuvo bloqueada o inoperativa cerca de media hora, pero a las cinco y media estaba completamente restablecida y se podían realizar todo tipo de gestiones, tanto de consulta como comerciales, informaron fuentes de la operadora.

El ciberataque se produce [dos semanas después de la operación policial](#) que se saldó con la detención de tres personas como presuntos responsables de los chats desde los que se realizaron ataques de denegación de servicio (DDoS), envió masivo de peticiones a la web para su bloqueo, tanto a páginas web del Ministerio de Cultura como de la SGAE, entre otras.

Desde el pasado 23 de diciembre, los ataques de denegación de servicio están tipificados



Página web de Movistar.-

publicidad



Ataques a buzones de voz

[HOME PAGE](#) [TODAY'S PAPER](#) [VIDEO](#) [MOST POPULAR](#) [TIMES TOPICS](#)

Log In | Register Now | Help

The New York Times

Magazine

Search All NYTimes.com

[WORLD](#) [U.S.](#) [N.Y. / REGION](#) [BUSINESS](#) [TECHNOLOGY](#) [SCIENCE](#) [HEALTH](#) [SPORTS](#) [OPINION](#) [ARTS](#) [STYLE](#) [TRAVEL](#) [JOBS](#) [REAL ESTATE](#) [AUTOS](#)

**VALES DESCUENTO RESTAURANTES**
"Ejemplo de un próximo descuento"



GROUPON
► Descuento del día
Advertise on NYTimes.com

Tabloid Hack Attack on Royals, and Beyond



Laura Wink/Getty Images

Members of the royal household, including Princes Harry, left, and William, had their voice mail messages hacked into by News of the World employees.

By **DON VAN NATTA Jr.**, **JO BECKER** and **GRAHAM BOWLEY**
Published: September 1, 2010

IN NOVEMBER 2005, three senior aides to Britain's royal family noticed odd things happening on their mobile phones. Messages they had never listened to were somehow appearing in their mailboxes as if heard and saved. Equally peculiar were stories that began appearing about Prince William in one of the country's biggest tabloids, News of the World.

The stories were banal enough (Prince William pulled a tendon in his knee, one revealed). But the royal aides were puzzled as to how News of the World had gotten the

[RECOMMEND](#)
[TWITTER](#)
[LINKEDIN](#)
[COMMENTS \(137\)](#)
[SIGN IN TO E-MAIL](#)
[PRINT](#)
[SINGLE PAGE](#)
[REPRINTS](#)
[SHARE](#)

THE DNA ANCESTRY PROJECT

Discover your ancestry with DNA
www.DNAAncestryProject.com
Advertise on NYTimes.com

TicketWatch: Theater Offers by E-Mail

Sign up for ticket offers from Broadway shows and other advertisers.

[See Sample](#) | [Privacy Policy](#)

MOST E-MAILED **MOST VIEWED**



1. **DEGREES OF DEBT**
A Generation Hobbled by the Soaring Cost of College
2. **CHARLES M. BLOW**
Mean Boys
3. **OP-ED CONTRIBUTOR**
Diagnosing the D.S.M.
4. **GAIL COLLINS**
The Anatomy of a Jokerster

Anatomy of the Phone-Hacking Scandal


Robo de identidad...y de dinero



SECURITY ON THE MOVE



SECURE
BUSINESS
INTELLIGENCE

AUSTRALIAN EDITION ▼

SIGN IN JOIN

POPULAR: show , security , database

SEARCH

HOME NEWS IN DEPTH REVIEWS EVENTS SC AWARDS

WHAT WE'RE FOLLOWING: RSA 2012 • Print edition • Jobs • Fixer

Home / Security News / Hackers

\$45k stolen in phone porting scam



By Brett Winterford on Dec 6, 2011 8:47 AM
Filed under [Hackers](#)

Scammers steal identity, redirect banking verification codes.

Me gusta

13 Tweet

Share 6

3 Comments and 12 Reactions



Keywords

phone porting, fraud,
online banking,
commsalliance,
commbank, financeit

Related

Page 1 of 2 | [Single page](#)

Part one of a three part series into fraud.

Fraudsters are increasingly using social engineering techniques to steal mobile phone numbers and intercept their owners' online banking verification codes, according to an investigation published in the inaugural Australian print edition of *SC Magazine*.

With the country's police forces too stretched to investigate and telcos unwilling to accept responsibility for the problem, Australia's banks have been forced to wear the risk and cost of the fraud as they look to new methods of protecting online accounts.

The alarm

The scam is sophisticated, as one recent example illustrates.

Sign up to receive SC Magazine email newsletters

SIGN UP

FOLLOW US...



SECURITY ON THE MOVE



Thursday, 8th March
Intercontinental Melbourne

Most Read

- NSA builds Android phone for top secret calls
- Did Lulzsec's slip seal its fate?
- Infosec burn-out rate rising
- Security industrv "at serious risk of failino"

Fugas de información

[comparativa](#) [herramientas](#) [wiki](#)

hosting interdominios **BANDARROCHA.EU**
Información independiente
internet móvil / ADSL / FTTH / cable

20 usuarios 1.491 invitados
115.350 registrados

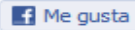
▶ Regístrate
▶ Entrar

LLEGA EL CALOR

**Orange revela tu número a las webs que visitas desde el móvil**

 votam

 27

 Me gusta

103

 Twittear

0

 +1

Actualización: Orange asegura que el problema está solucionado y que se trata de casos "residuales" que utilizan la "antigua plataforma de WAP".

Por la configuración de su servicio, **Orange está mostrando a cualquier web el número de teléfono del usuario que navega por WAP con su teléfono**, una práctica que ha detectado el [blog Certificate Error](#).

El blogger, que está elaborando un estudio sobre cómo los diversos operadores de telefonía móvil identifican a los usuarios en la red y las modificaciones que hacen para tal fin en las cabeceras del protocolo HTTP que se encarga de las peticiones web, ha comprobado que la división de Orange en España no está protegiendo bien la identidad de los clientes.

Tal y como comenta "xuf", hay dos métodos principales para la reconocer a los usuarios, basándose en qué tipo de webs se acceden.

Para los sitios internos seguros se hace con el número de teléfono real en una de las cabeceras de HTTP, pero para el resto de la red, se utiliza normalmente un identificador temporal generado que enmascara los datos reales del usuario.

Pues bien, según las pruebas que ha estado realizando, en **Orange España se utiliza para toda la red el número de teléfono real del cliente usando una conexión WAP**, con lo que cualquier administrador puede acceder fácilmente a este dato. Una consecuencia sería la posibilidad de empezar a recibir SMS o llamadas con publicidad que no nos interesa de una empresa a la que no hemos dado nuestros datos conscientemente.

Content-length: 0
Via: WTP/1.1 nwg2 (Nokia WAP Gateway 4.1/CD21/4.1.116)
X-Network-info: CSD,34xxxxxxxxxx,unsecured
X-Nokia-CONNECTION-MODE: TCP

Ausencia seguridad nuevos servicios



[CNET UK](#) > [Crave](#) > [Mobile Phones](#)

Femtocell security flaw puts Vodafone customers at risk of phone tapping

By [Luke Westaway](#) on 14 July 2011, 12:48pm [Follow](#) [@lukewestaway](#)

[ALERT ME](#) [Tweet](#) [9](#) [Submit](#) [Me gusta](#) [1](#)

Seguridad en la nube

rtve.es

Busca en rtve

NoticiasTVRadioDeportes

A la Carta | Programación | Telediario en 4* | Blogs | Mundo | España | Autonomías | Economía

DIRECTO**La Vuelta en directo - 18ª Etapa: Solares - Noja**
14:46 Sigue en directo la retransmisión de la decimoctava etapa de la Vuelta ciclista a España 2011

Noticias > Ciencia y tecnología

Imprimir

Sony investiga el ataque que mantiene cerrado PlayStation Network

- Se cumplen cinco días de corte en el servicio PSN
- Sony confirma que el 'apagón' se debe a una intrusión externa
- Se desconoce cuando volverá a estar operativo y la dimensión del ataque

Recomendar

Regístrate para ver qué recomiendan tus amigos.

Twitter 2

+1 0

Enviar



Ampliar foto

La compañía nipona todavía no ofrece plazos sobre cuándo puede estar reestablecido el servicio PSN

Noticias relacionadas

- Los 'tablets' S1 y S2 de Sony, una apuesta distinta
- Nintendo anuncia nueva consola para 2012 en plena caída de ventas
- La PS3 vuelve a circular libremente en Europa

RTVE.es

26.04.2011

Se cumplen cinco días desde que la empresa japonesa Sony se viera obligada a apagar PlayStation Network, los servicios *on-line* de la PlayStation y la PSP en los que unos **75 millones de usuarios** juegan conectados, navegan y descargan contenidos multimedia. La compañía continúa investigando el ataque a sus servidores, pero por el momento se desconoce la naturaleza del mismo y la fecha en que PSN volverá a estar operativo.

Las explicaciones de la compañía se reducen a que hacen todo lo posible "para restablecer los servicios ante esta intrusión externa" detectada **el pasado día 21 de abril** y por la que Sony decidió apagar los servicios PlayStation Network (PSN) y Qriocity (servicios online de música y películas).

Sony pide paciencia a los usuarios vía Twitter, afirmando **« Seguimos**

Espionaje industrial...que salta fronteras



[Australian edition](#) | [NBN](#) | [Telstra](#) | [Government](#) | [Filter](#) | [Security](#) | [Android](#) | [Apple](#) | [Mobile Ph](#)

BREAKING NEWS: [Femtocells cause coverage holes: Telstra](#)

[ZDNet](#) / [Security](#) / [Story](#)

Telecom NZ data breached by rival: report

By Darren Pauli, ZDNet.com.au on January 18th, 2011

Topics

[security](#), [data breach](#), [telecom nz](#), [telcos](#), [vodafone](#)

 Recommend

 Sign Up to see what your friends recommend.

 Tweet

7

 Share

A telecommunications company has been accused of using leaked identity credentials to poach Telecom New Zealand customers in a [breach](#) that mirrors a similar theft which [hit Vodafone Australia weeks earlier](#).

Análisis forenses



[Registro](#) [Hemeroteca](#) BUSCAR en [elcorreo](#)

[PORTADA](#) [ÚLTIMA HORA](#) [ECONOMÍA](#) [DEPORTES](#) [OCIO](#) [PARTICIPACIÓN](#) [SERVICIOS](#) [C](#)

LA BOLSA

La sesión
al minuto

Acciones

Índices bursátiles

Personalización de
valores

ECONOMÍA

EL CORREO EDICIÓN IMPRESA

ECONOMÍA

Euskaltel acusa de espionaje a un empleado que acaba de fichar Orange

La operadora presenta una denuncia por la apropiación de datos confidenciales de su red comercial y sus clientes

Al servicio de la ley

PORTALTIC.es | INTERNET

domingo, 13 de mayo 2012 editado por europa press

INTERNET | GADGETS | VIDEOJUEGOS | SOFTWARE | EMPRESAS | MOVILIDAD | ADMINISTRACIÓN | SECTOR | BLOGS | VÍDEOS | JUEGOS

El Software más premiado en Europa:
Simple. Seguro. Ligero.

TRAS REINO UNIDO Holanda se une al bloqueo a The Pirate Bay

[Directorio](#) [The Pirate Bay](#) [Internet](#) [Partido Pirata](#) [Tribunal Superior Justicia Reino Unido](#)

Deja tu comentario

COMPARTE ESTA NOTICIA

The Pirate Bay

Foto: THE PIRATE BAY [Ampliar foto](#)

Tribunal Superior de Justicia de Reino Unido para que los principales

MADRID, 11 May. (Portaltic/EP) -

Un tribunal de La Haya en Holanda ha ordenado a los principales proveedores de servicios del país que dejen de facilitar el acceso a la página web. Además, el tribunal ha atendido una petición del grupo BREIN para solicitar al Partido Pirata de Holanda que deje de ofrecer soluciones alternativas para el acceso a la página.

La persecución legal contra The Pirate Bay continúa. A finales de abril se conocía una decisión del

ÚLTIMAS NOTICIAS

- 10:00 Google+ permite responder a las notificaciones directamente desde el correo
- 11/05 El Ayuntamiento de Madrid participa en el II Foro de la Gobernanza de Internet en España
- 11/05 RTVV estrena la webserie Desenterrats
- 11/05 Holanda se une al bloqueo a The Pirate Bay
- 11/05 Venden por Internet una pitón y la envían por correo en un tupperware
- 11/05 Microsoft rediseña Bing e incluye nuevas características sociales
- 11/05 Facebook permitirá compartir archivos entre los grupos
- 11/05 Easel permite crear infografías de forma gratuita
- 10/05 Acepta dos años de cárcel por descargarse 400 vídeos y 2.700 fotos de pornografía infantil
- 10/05 La plataforma Sibarit.us amplía capital con el apoyo de directivos de Telefónica

6Mb + TLF + TV

Comercio de divisas Fácil Únase a Easy-Forex: comercio

Anuncios Google

Medidas de seguridad en tela de juicio



THREAT LEVEL

PRIVACY, CRIME AND SECURITY ONLINE



[PREVIOUS POST](#)

[NEXT POST](#)

CIA, Mossad, Also Targeted in Massive DigiNotar Cert Breach

By Kim Zetter   September 6, 2011 | 3:22 pm | Categories: [Breaches](#), [Cybersecurity](#), [Hacks and Cracks](#)
[Follow](#) @KimZetter · 3,501 followers

The list of fraudulent certificates obtained by hackers who breached a Dutch certificate authority has grown to more than 500 and includes certificates for domains owned by three intelligence agencies: the CIA, Israel's Mossad and the UK's MI6.

DigiNotar, which is owned by Illinois-based Vasco Data Security, also lacked basic security safeguards, such as strong passwords, anti-virus protection, up-to-date software patches, according to a third-party audit conducted by security firm Fox-IT in the Netherlands, released Monday.

DigiNotar acknowledged last week that it became aware it had been breached on July 19, though it has never disclosed how long the hackers were inside its network before they were



DigiNotar®
A GDS VASCO COMPANY



//03

Algunos
problemas de
fraude

*

Fraude back-office, como en otro lugar

**REUTERS**

EDITION: U.S. ▼

Register | Sign In   

Search News & Quotes

Home Business ▼ Markets ▼ World ▼ Politics ▼ Tech ▼ Opinion ▼ Breakingviews ▼ Money ▼ Life ▼ Pictures ▼ Video ▼



TAP INTO WESTLAW NEXT

WestlawNext™ iPad™ App.
Access the world's most advanced legal research system via your iPad.

[LEARN MORE »](#)

ARTICLE



"IT HELPS ME ADDRESS MY CLIENTS' ISSUES ANYTIME, ANYWHERE."

TIM JOHNSON, PRINCIPAL ATTORNEY
MATTHEWS, LAWSON & JOHNSON, P.L.L.C.
HOUSTON



See what the WestlawNext iPad app can do for you ▶



THOMSON REUTERS™

Follow Reuters

Latest from My Wire ▲

"Back office" fraud seen rising after recession peak

 Recomendar  19 recomendaciones. [Regístrate](#) para ver qué recomiendan tus amigos.

By Barbara Liston
ORLANDO, Florida | Sat May 14, 2011 6:56pm EDT

(Reuters) - "Back office" fraud is draining corporate treasuries of billions of dollars a year, and the risk is growing as companies and employees struggle in the wake of the recession, **finance** managers and experts say.

 Tweet 31

 Share 23

 Share this

 +1 0

 Email



Tráfico falso, blanqueo dinero y fraude fiscal

[HOME PAGE](#) [TODAY'S PAPER](#) [VIDEO](#) [MOST POPULAR](#) [TIMES TOPICS](#) [Log In](#) [Register Now](#)

The New York Times **Global Business**

[WORLD](#) [U.S.](#) [N.Y. / REGION](#) [BUSINESS](#) [TECHNOLOGY](#) [SCIENCE](#) [HEALTH](#) [SPORTS](#) [OPINION](#) [ARTS](#) [STYLE](#) [TRAVEL](#) [JOBS](#) [REAL ESTATE](#) [AUTO'S](#)

Search Business **Financial Tools** **More in Business »**
[Global Business](#) [Markets](#) [Economy](#) [DealBook](#) [Media & Advertising](#) [Small Business](#) [Your Money](#) [Energy & Environment](#)

One of the Top 4 online bachelor's programs in the U.S.
—U.S. News & World Report **PACE UNIVERSITY**
Success stories start here

Telecom Italia Delays Results Because of Money-Laundering Scandal

By ELISABETTA POVOLEDO and DAVID JOLLY
Published: February 25, 2010

ROME — [Telecom Italia](#) has delayed the release of its 2009 results after the authorities seized 300 million euros from its Sparkle subsidiary in connection with a money-laundering scandal that has rocked the Italian business establishment.

[Enlarge This Image](#)



Milo Sotgiu/European Pressphoto Agency

Italian authorities are seeking Silvio Scaglia, a founder of Fastweb. The company has denied having any ties to the Mafia.

Add to Portfolio
[+ Telecom Italia SpA](#)
[+ Swisscom AG](#)

to&opzn&page=ww...

The company, based in Milan, said late Wednesday that it had “resolved not to proceed with the approval” of its 2009 financial statements, which had been scheduled for release Thursday, and would instead publish them March 25. Its shares fell 3.1 percent in Milan.

The Italian authorities this week issued arrest warrants for 56 people in connection with a 2 billion euro, or \$2.7 billion, tax fraud and money-laundering investigation linked to the 'Ndrangheta, or the Calabrian Mafia.

In addition to Telecom Italia's Sparkle unit, prosecutors are looking into the accounts of Fastweb, a broadband provider four-fifths owned by Swisscom, which bought its stake in 2007 after the incidents that set off the investigation.

[TWITTER](#)
[LINKEDIN](#)
[SIGN IN TO E-MAIL](#)
[PRINT](#)
[REPRINTS](#)
[SHARE](#)



More Articles in Business »
Get DealBook by E-Mail
 Sign up for the latest financial news delivered before the opening bell and after the market close.

[See Sample](#) | [Privacy Policy](#)

Panasonic
Ideas for Life
OUR TOUGHBOOK® LAPTOPS SAVE LIVES IN DISASTERS

APPLY NOW »

MOST POPULAR - BUSINESS
[E-MAILED](#) [BLOGGED](#) [VIEWED](#)

1. Degrees of Debt: A Generation Hobbled by the Soaring Cost of College
2. JPMorgan Sought Loophole on Risky Trading
3. As Dewey Collapses, Partners and Retirees Face Big Financial Losses
4. Wealth Matters: Investing in Restaurants Can Work, but It's Not as Easy as Pie
5. Common Sense: Gov. Marianne Ravé May Come at a

 **S21sec**

Fraude específico del sector telco

Fraud by sector

Financial**	£3.6 billion	Insurance fraud	£2.1 billion	
		Mortgage fraud	£1 billion	
		Plastic card fraud	£440 million	
		Online banking fraud	£60 million	
		Cheque fraud	£30 million	
		Motor finance fraud	£16 million	
		Telephone banking fraud	£12 million	
Financial***	£3.6 billion	Online banking fraud	£60 million	
		Cheque fraud	£30 million	
		Motor finance fraud	£16 million	
		Telephone banking fraud	£12 million	
Retail, wholesale and distribution	£2.7 billion	Corporate fraud against large businesses	£2.6 billion	
		Small to medium sized business fraud	£169 million	
Telecommunications**	£730 million	Telecommunications fraud	£730 million	
Third sector	Construction and engineering	£567 million	Corporate fraud against large businesses	£360 million
	Consumer goods	£294 million	Small to medium sized business fraud	£206 million
	Natural resources	£135 million	Corporate fraud against large businesses	£294 million
	Healthcare	£132 million	Small to medium sized business fraud***	-
	Other	£50 million	Corporate fraud against large businesses	£111 million
			Small to medium sized business fraud	£24 million
Charity	£1.3 billion	Charity fraud	£132 million	
Individuals	N / A	£4 billion	Small to medium sized business fraud	£0.31 million
			Corporate fraud against large businesses	-
			Small to medium sized business fraud	£50 million
Total AFI 2011 fraud loss		£38.4 billion	Mass marketing fraud	£3.5 billion
			Rental fraud	£314 million
			Online ticket fraud	£168 million
				£38.4 billion

* This figure only captures reported / detected fraud losses.

** It is not possible to separate out losses suffered by small, medium and large businesses for these industries.

*** None of the respondents to the survey run by the Federation of Small Businesses, classified themselves in this category, therefore we were unable to calculate an estimate of fraud against small to medium sized businesses for this industry.

Ataque SIM toolkit

 **Prezi** [Create](#) [Learn](#) [Explore](#) [Sign up](#) [Pricing](#) [Log in](#)

SIM Toolkit Attack

SIM Toolkit Attack [Bogdan Alecu](#)
06 February 2012

SMS fuzzing - SIM Toolkit Attack

Bogdan Alecu - <http://www.m-sec.net>



DEEPSEC Mobile

Push SIM from back to detach.

Get more security for your phone.

◀ ▶ More

Fraude televisión de pago

Mirror

NEWS



Real news, real entertainment ... in real time

How we make the Mirror better for YOU

[FRONT PAGE](#)[NEWS](#)[SPORT](#)[3AM](#)[LIFESTYLE](#)[MONEY](#)[PLAY](#)[OPINION](#)

[M](#) [News](#) [UK News](#)

By [Mirror.co.uk](#) | [Comments](#) | 16 Jul 2011 00:00

Set-top box fraud 'cost Virgin £144m a year'

A FRAUDSTER who sold 400,000 set-top boxes which could receive TV subscription channels for free cost Virgin Media £144million a year, a court heard yesterday.

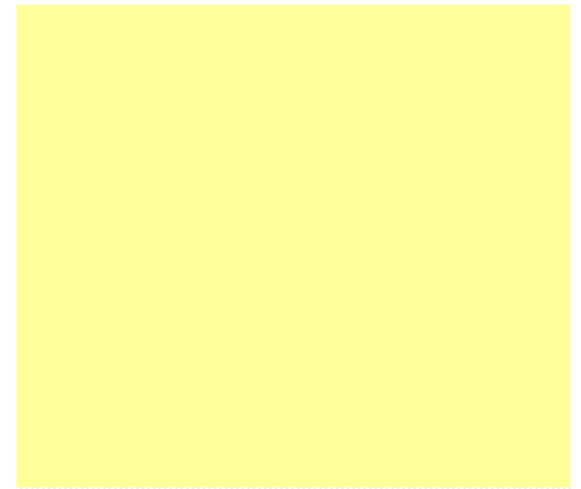
[Tweet](#) [0](#)

A FRAUDSTER who sold 400,000 set-top boxes which could receive TV subscription channels for free cost Virgin Media £144million a year, a court heard yesterday.

Munaf Zinga, 41, set up Rayyonics Ltd in 2005 to sell Eurovox devices for £100.

Mukundan Pillai, 42, was the technical expert and Salim Patel, 47, the delivery driver,

[rbc.bidder7.mookie1.com...](#) sold.



RECOMMENDED ON THE MIRROR [Why?](#)

Fraude PBX

TMCnet
BLOGGERS
Tom Keating
CTO


Home About Me Archives Contact TMCnet Blogs TMC Events Online Communities TMCnet Home

VoIP & Gadgets Blog
| VoIP & Gadgets blog - Latest news in VoIP & gadgets, wireless, mobile phones, reviews, & opinions

 [Subscribe](#)

SIPNOC US 2012 **The SIP Network Operators Conference**
Herndon, Virginia - June 25-27, 2012
Presented by **SIPFORUM**
[LEARN MORE](#)

[Search](#)

AstriCon VoIP Security - \$400,000 toll fraud - YIKES!
October 26, 2011
 [Digg](#)  [+1](#)  [Tweet](#)  [8](#)



During an AstriCon session on VoIP security the speaker discussed how easy it was to hack voicemail PINs, but not to listen to your voice messages but to initiate "call backs" using spoofed CallerIDs. Essentially, this leverages the "call back" feature that many voicemail systems have to call back the person that left the message.

He then asked the audience for any real world examples of how they were hacked. Several volunteered their stories. I captured one of them where their [Elastix](#) server was hacked - due to their parent company locking them out of the server and not updating /patching the server. This resulted in the hackers racking up toll fraud (Korean calls) of \$400,000! It's a fun watch. Enjoy! [HD available in full screen mode]

[Compartir](#) [More info](#)

 **Subscribe to Blog via RSS**

 [Submit](#)

Hot Tags [Categories](#) [Archives](#) [Blog Roll](#)

[android](#) [apple](#) [asterisk](#) [at&t](#) [blackberry](#) [cell](#)
[phone](#) [cisco](#) [dell](#) [digium](#) [e911](#) [fcc](#) [google](#) [google](#)
[talk](#) [gps](#) [im](#) [ip-pbx](#) [ipad](#) [iphone](#) [ipod](#) [itexpo](#) [ITEXPO](#)
[lync](#) [microsoft](#) [mobile](#) [phone](#) [open](#) [source](#) [outage](#)
[phone](#) [review](#) [sip](#) [skype](#) [sony](#) [unified](#)
[communications](#) [verizon](#) [video](#) [video](#)
[conferencing](#) [voip](#) [vonage](#) [wifi](#) [wireless](#) [xbox](#)
[360](#)

 [Now from](#) [VeriSign](#)

Fraude subscripción

EL PAÍS.COM Internacional Política España Deportes Economía Gente y TV Sociedad SModa

Viernes, 16/12/2011

EL PAÍS edición impresa

EL PAÍS CONTIGO
CADA MAÑANA
Recibe el periódico en su casa

AVANCE Consulta en PDF la portada de EL PAÍS, edición nacional, del viernes 16 de diciembre

SECCIONES DE LA EDICIÓN IMPRESA:
Primera Internacional España Economía Opinión Viñetas Sociedad Cultura Tendencias Gente Obituarios Deportes Pantalla Última

Estás en: [ELPAÍS.COM](#) > [Edición Impresa](#) > [España](#)

Una red de empleados de telefonías estafó a estas 27 millones

E. A. - Madrid - 07/08/2010

Vota ☆☆☆☆☆ | Resultado ★★★★★ 49 votos

Twitter 0

Recomendar

La Guardia Civil ha desarticulado una red acusada de estafar a compañías de telefonía móvil en un fraude que podría alcanzar los 27 millones de euros. Se ha detenido a 32 personas acusadas de delitos de estafa, usurpación de estado civil y encubrir delincuentes. La red estaba extendida por siete ciudades españolas y tenía en su poder más de 43.400 tarjetas y cerca de 1.500 teléfonos móviles, según la Guardia Civil. También se han incautado 180.000 euros en efectivo.

La noticia en otros webs

webs en español
en otros idiomas

La denominada Operación Movoda se inició el pasado febrero, cuando agentes del instituto armado detectaron una serie de estafas con tarjetas de telefonía móvil. Posteriormente se descubrió que en la trama participaban distribuidores oficiales de teléfonos móviles.

Estos trabajadores agotaban el saldo de tarjetas telefónicas llamándose a sí mismos a números de tarifa especial que previamente habían contratado. Después vendían las tarjetas ya sin saldo a varios locutorios y bazares. Los dueños de los locales distribuían las tarjetas a una red organizada que continuaba con una estrategia enrevesada y perfectamente coreografiada.

Cambio de operadora

A través de una web ubicada en Sudamérica, los dueños de los locales

Kiosko y más
Accede a EL PAÍS y todos sus suplementos en formato pdf enriquecido.
ACCEDER
KIOSKO y más

publicidad
Sé original y regala juguetes de siempre

www.oriento9.es
Ver más juguetes

E Última Hora
La presidenta y consejera delegada de The New York Times Company, Janet Robinson, anuncia su jubilación el próximo...

Malware y fraude servicios premium



LoginJoinSign In

UK EditionNewsReviewsBlogsOracle vs GoogleMobile ITWhite papersBroadbandWindows 8Cloud

CLOUD COMPUTING

The latest content and conversations.

Powered by  **BROCADE**

ZDNet UK / News and Analysis / Security / Security Threats

Chinese Android botnet 'netting millions', says Symantec

By Tom Espiner, ZDNet UK, 10 February, 2012 16:15 [Follow @tomespiner](#)

Daily Newsletters

Sign up to ZDNet UK's daily newsletter.

Topics

Android, Botnet, China

Sponsored Links

Antivirus for MacOS X
Defend Your MacOS
Against Malicious Attacks.

NEWS An Android botnet affecting hundreds of thousands of Chinese users is netting its masters millions of dollars annually, according to security company Symantec.

The network of compromised mobile phones generates revenue from premium-rate fraud, Symantec said in a blog post on Thursday. "Revenue generation through premium SMS, telephony, and video services is... limited to the networks of China's two largest mobile carriers," said Symantec researcher Cathal Mullaney in the blog post.

On any given day, 10,000 to 30,000 customers of China's two largest mobile operators, state-owned China Mobile and China Unicom, are being fleeced by the premium-rate malware. The botmaster has been raking in profits at this level since September 2011, according to Symantec.

This is the first time Symantec has established an appreciable amount of money being made through Android botnets, Tom Parsons, senior manager, quality assurance at Symantec, told ZDNet UK on Friday.

'Waste not, want not.'

The consumerisation of the data centre.

[Watch now](#)

colt
smarter / faster / further



Get ZDNet UK's daily newsletter

Enter your email address to sign up

[Sign up now](#)

ZDNet UK Ltd

Fraude M2M

BBC Mobile

News | Sport | Weather | Travel | TV | Radio | More ▾

Search BBC News

NEWS AFRICA

Home | UK | **Africa** | Asia-Pac | Europe | Latin America | Mid-East | South Asia | US & Canada | Business | Health | Sci/Environment | Tech | Entertainment | Video

7 January 2011 Last updated at 13:06 GMT



South Africa thieves hit traffic lights for Sim cards

Some 400 high-tech South African traffic lights are out of action after thieves in Johannesburg stole the mobile phone Sim cards they contain.

The thieves ran up bills amounting to thousands of dollars by using the stolen cards to make calls.

Johannesburg Road Agency (JRA) said it is investigating the possibility of an "inside job" after only the Sim card-fitted traffic lights were targeted.

The cards were fitted to notify JRA when the traffic lights were faulty.

JRA believes a syndicate "with links on the inside" is behind the thefts.



Traffic lights have become attractive targets for thieves in Johannesburg

AFP

Related stories

Criminal baboons terrorise South Africa

Top Stories



Greeks strike over new austerity

Global shares drop on Fed warning

New images of falling satellite

France imposes first niqab fines

Pope making historic German visit

Features & Analysis



State of fear?

Israeli author says Palestine is seen as an existential threat



War on two fronts

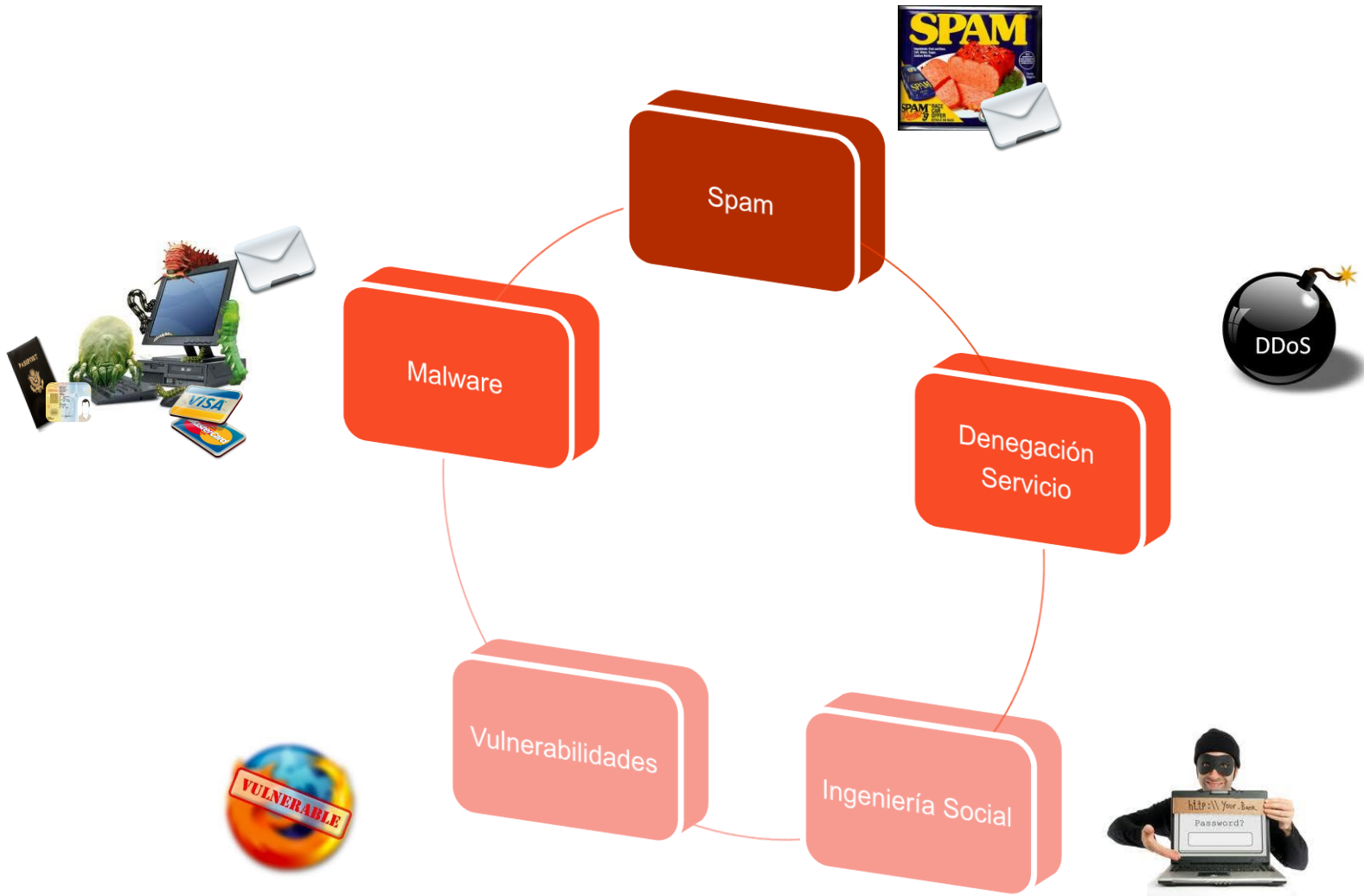
The female veterans tormented by combat and sexual trauma

//04

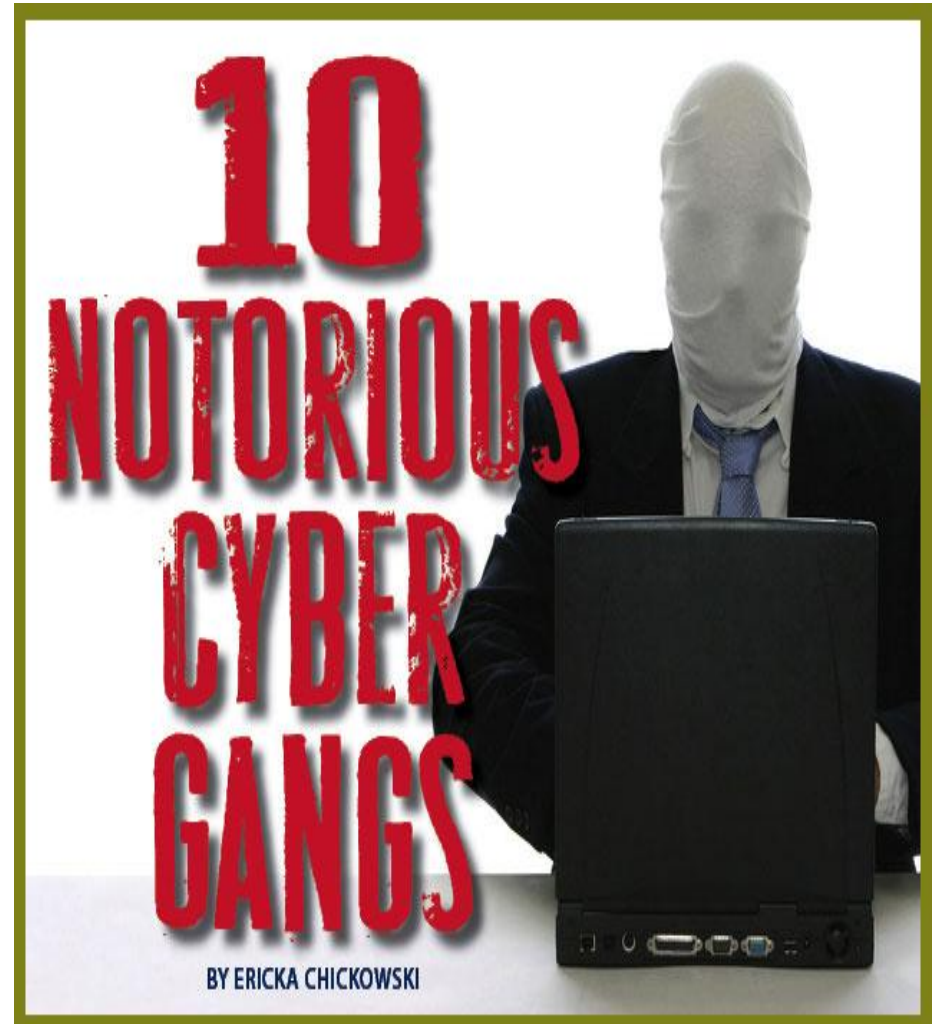
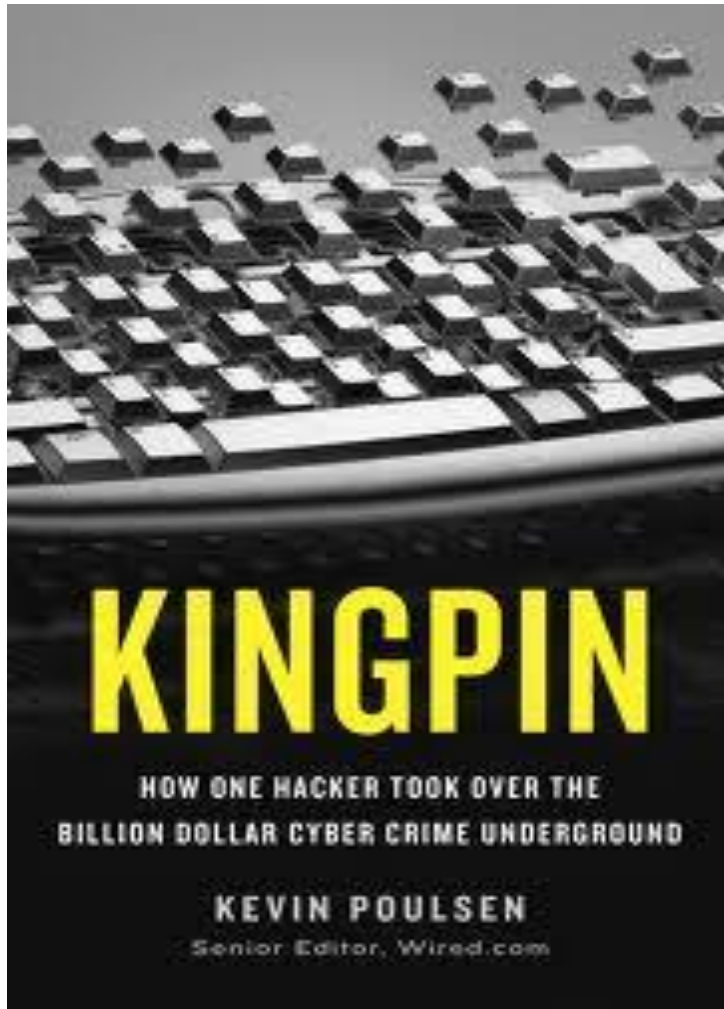
**Evolución, a
peor, del
problema**

*

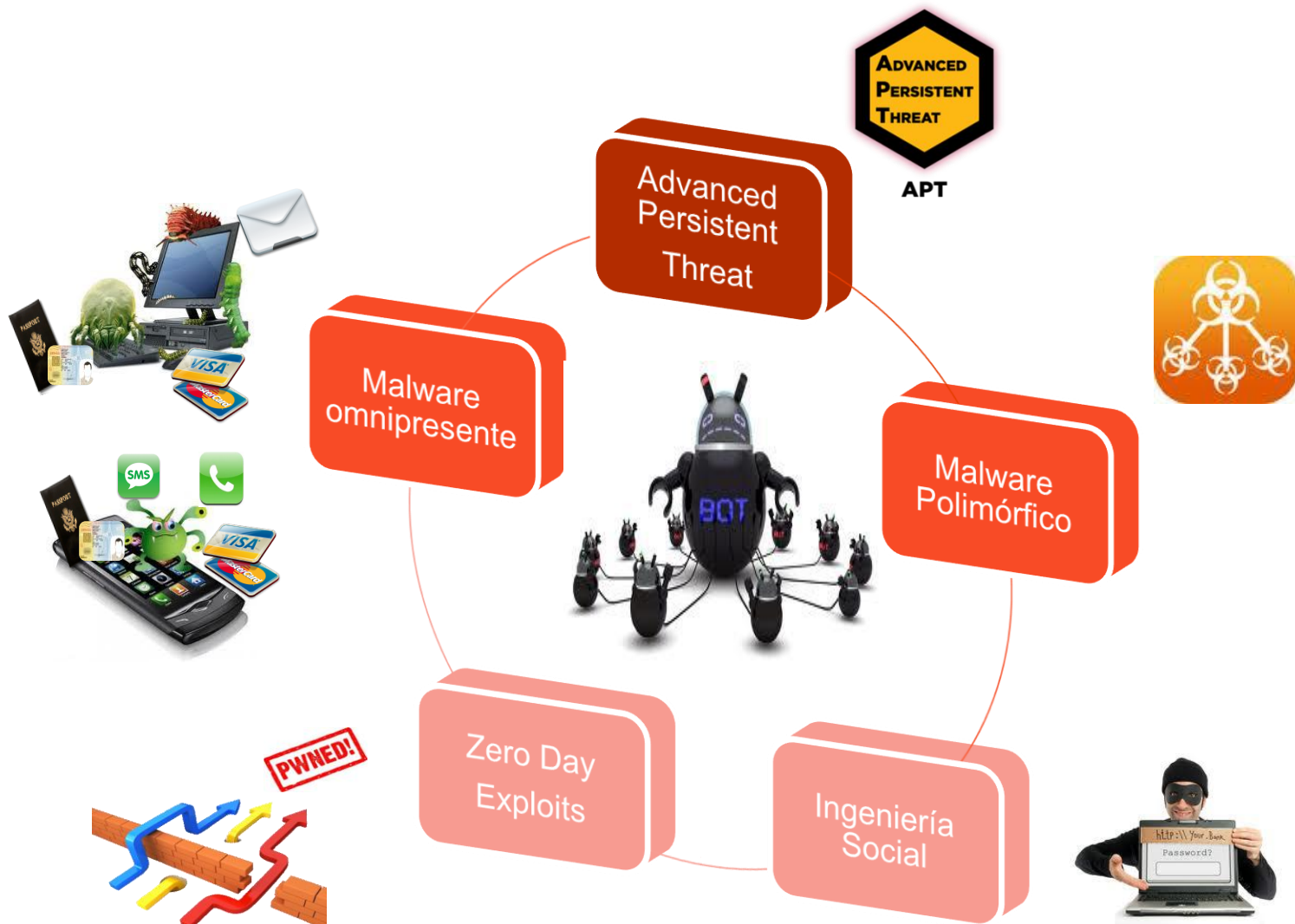
De las clásicas amenazas...



... pasando por la profesionalización del cibercrimen...



...se ha evolucionado a la gran amenaza...



...con distintos objetivos,...

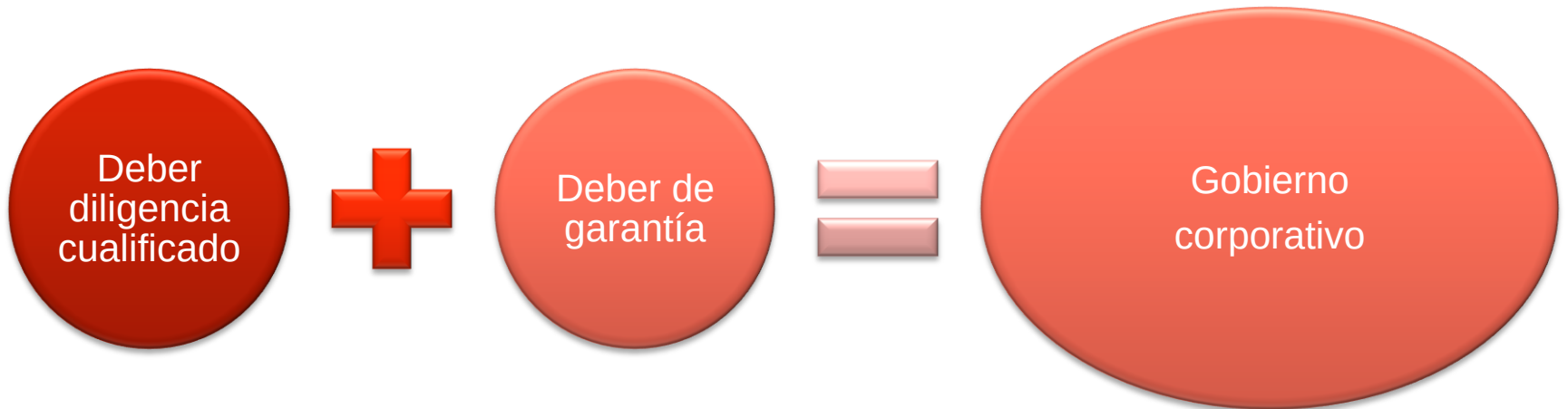


//05

Obligaciones de los operadores

*

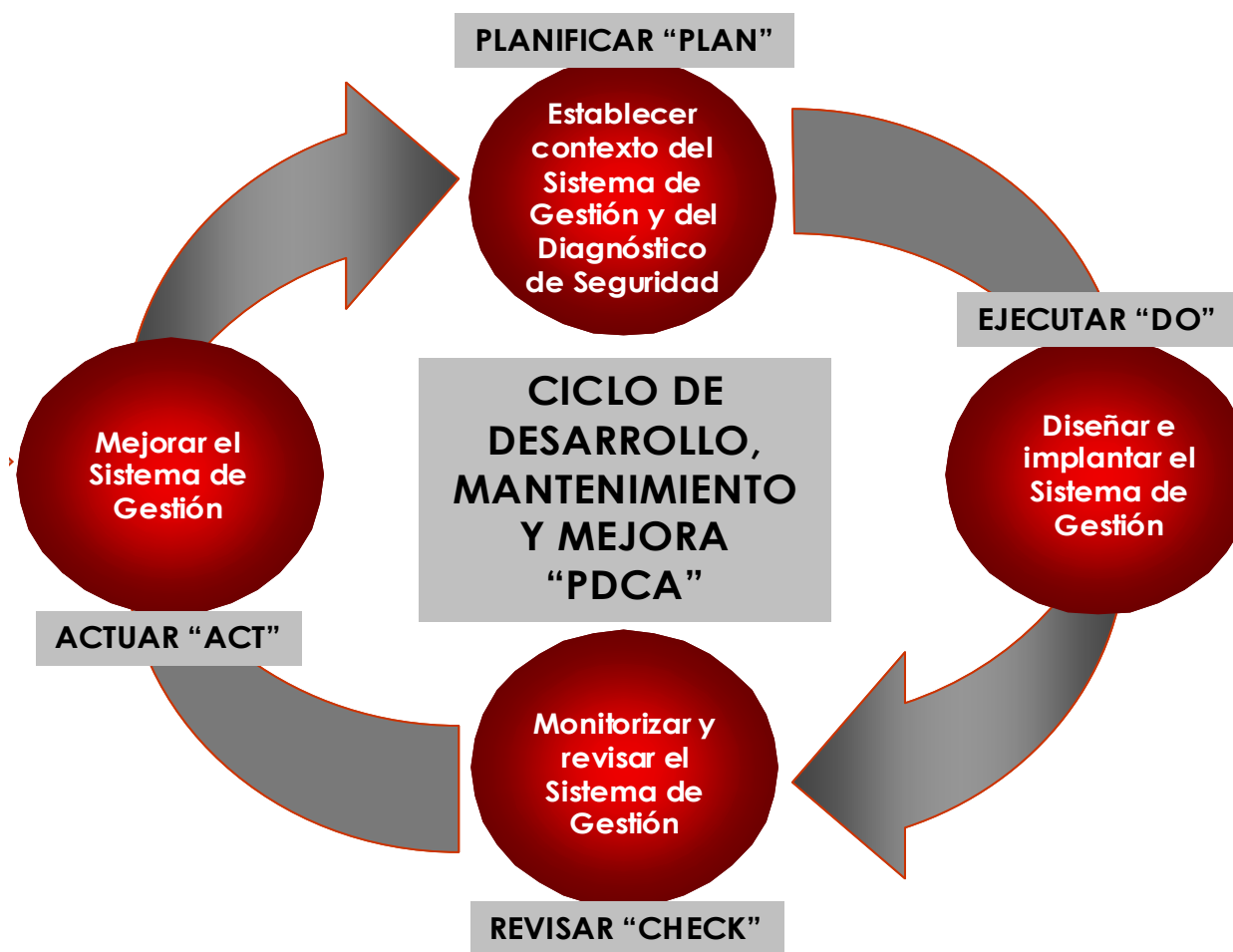
Gobierno Corporativo...



...gestionando el riesgo...



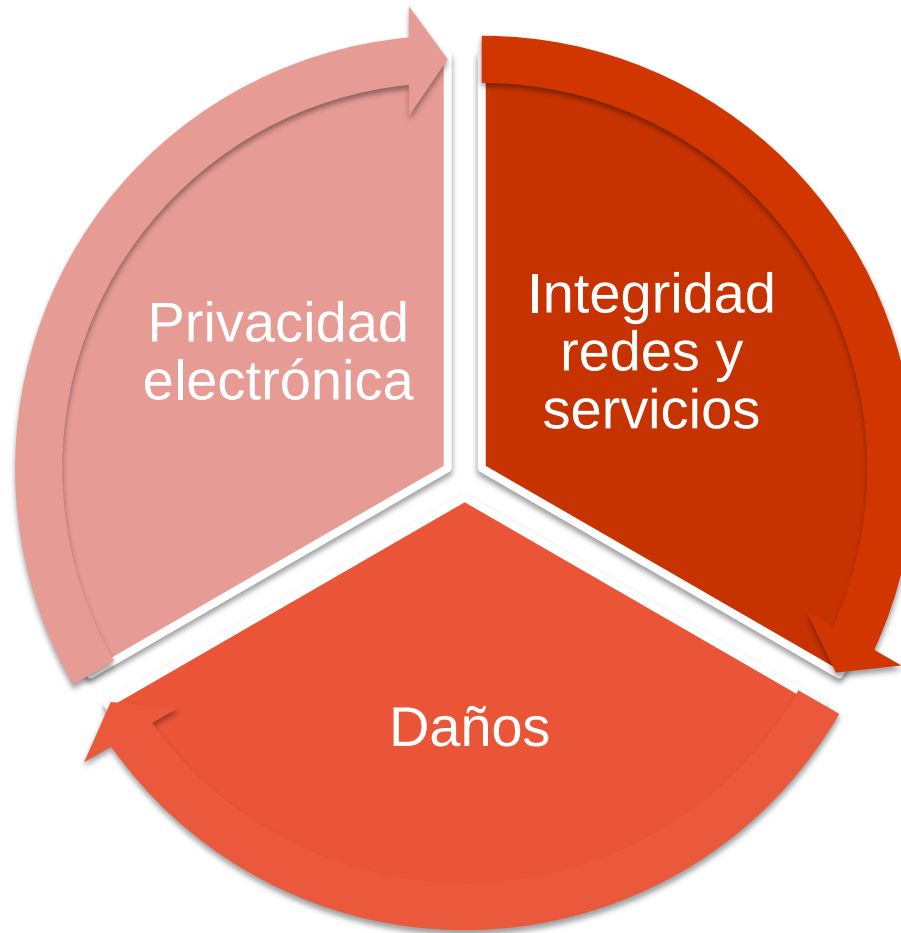
..., en un proceso de mejora continua...



Diversas obligaciones de seguridad...



...con objetivos distintos, pero interrelacionados...



...alrededor de la seguridad...



...para proteger a la sociedad, además de a sí mismos



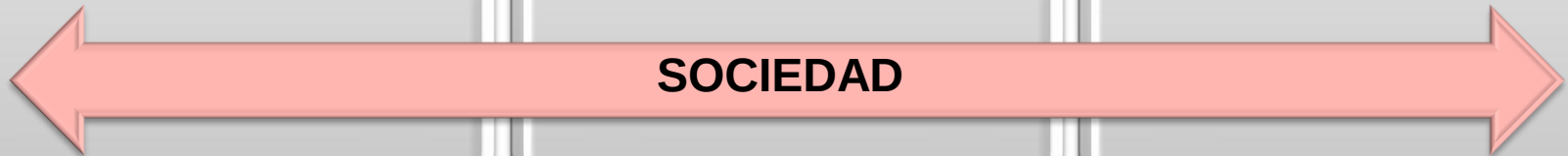
**Personas
Físicas**



**Personas
Jurídicas**



**Infraestructuras
Críticas**



SOCIEDAD

//06

**Gestión de
seguridad y
lucha contra el
fraude**



Eeeeh,... ¿eso cómo se hace?



Pues con un enfoque integral...

Seguridad Física



Área Común



Seguridad Lógica



...con base en estándares internacionales...



International
Organization for
Standardization

International Standards for Business, Government and Society

Search >>

Home

Products

Standards development

News and media

About ISO

For ISO Members · FAQs · Fr | Ru

 ISO Store

Products > ISO Standards > By TC > JTC 1 Information technology > SC 27

ISO Store

ISO Standards

By ICS

>> By TC

How to use the ISO Catalogue

Standards in action

Management and leadership standards

The ISO portfolio

FAQs

Country codes (ISO 3166/MA)

Directory of aerospace standards

Publications and e-products

ISO Concept Database (ISO/CDB)

Copyright

ISO/IEC 27002:2005

Information technology -- Security techniques -- Code of practice for information security management

Media and price

Language	Format	Add to basket
English	 PDF (1 128 kB)	CHF 210,00 
English	 Paper	CHF 210,00 
English	 ePub (161 kB)	CHF 210,00 
English	 iPad (210 kB)	CHF 210,00 
English	 mobipocket (358 kB)	CHF 210,00 
French	 PDF (761 kB)	CHF 210,00 
French	 Paper	CHF 210,00 
French	 ePub (152 kB)	CHF 210,00 
French	 iPad (184 kB)	CHF 210,00 
French	 mobipocket (340 kB)	CHF 210,00 

General information

Number of Pages: 115

These standards could also interest you

- [ISO/IEC 29192-2:2012](#)
Information technology -- Security techniques -- Lightweight cryptography -- Part 2: Block ciphers
- [ISO/IEC TR 29149:2012](#)
Information technology -- Security techniques -- Best practices for the provision and use of time-stamping services
- [ISO/IEC 27010:2012](#)
Information technology -- Security techniques -- Information security management for inter-sector and inter-organizational communications

...y sectoriales de seguridad...

**International
Telecommunication
Union**



Français Español



Home : [ITU-T](#) : [Publications](#) : [Recommendations](#) : [X Series](#) : [X.1051](#) : X.1051 (02/08)

[Recently posted](#) - [Search Recommendations](#) - [Shopping cart](#)

[ITU Sectors](#) | [Newsroom](#) | [Events](#) | [Publications](#) | [Statistics](#) | [About ITU](#)

X.1051 : Information technology – Security techniques – Information security management guidelines for telecommunications organizations based on ISO/IEC 27002

Recommendation X.1051 (02/08)

Approved in 2008-02

Status : In force

[Table of Contents](#)

[Summary](#)

Access : Freely available items

Available languages and formats :

 **Click on the selected format and language to get the document**

Format	Size	Posted	Article Number
English  .PDF (acrobat)	333641 bytes	2009-04-06	E 33422

Access : [TIES users](#) / [Subscription Service \(ITU Recommendations Online\)](#)

[Electronic Bookshop](#) - E-Price : 30 CHF (Swiss Francs)

Available languages and formats :

...de seguridad y fraude...

Technical Projects

- [VoLTE](#)
- [PathFinder](#)
- [Fraud & Security](#)**
 - [IMEI Database](#)
 - [Security Algorithms](#)
 - [Security Accreditation Scheme](#)
 - [Security Advice for Mobile Phone Users](#)
- [GSMA Spam Reporting Services](#)
- [HD Voice](#)
- [Smarter Applications](#)



Quick Links:

- [Membership](#)
- [Press Releases](#)
- [Worldwide Offices](#)
- [GSMA Latin America](#)
- [GSMA Europe](#)

Fraud & Security

IMEI Database

Centrally located database of valid and stolen handset IMEIs to which operators may connect to upload and download data to control mobile device access on their networks.

Security Algorithms

Provide authentication, cipher key generation, integrity and radio link privacy to users on mobile networks.

Security Accreditation Scheme

Voluntary scheme where smart card suppliers subject their production sites and processes to a comprehensive security audit providing confidence to network operators that adequate security is in place.

Security Advice for Mobile Phone Users

These pages aim to provide mobile phone users with simple, easy to follow advice to help mobile users minimise the risk of experiencing potential problems firsthand.



Who do you want to meet in the SOLD-OUT Expo?



tmforum

Collaboration

Standards

Conferences

Training

Research & Publications

News



About Us | Membership | Help

Sign In | Register

Home » Collaboration » Document Library » Document Catalog » Guidebooks

Document Catalog Guidebooks

Document Catalog

About

Guidebooks

Definitions

Business Agreements

Technical Specifications

Information Agreements

Interface Implementation Series

Technical Reports

Templates and Forms

Contracts

Charter Documents

Feature Documents



Business Metrics and Key Indicators

Documents for Review/Evaluation

GB947, Fraud Operations Management Guide, Release 1.0

The Fraud Operations Management Guide is designed to outline and explain Level 3 and Level 4 business processes associated with an operator's fraud management program. It contains detailed explanations of all processes, and diagrammatic illustrations showing connectivity and association to other processes within several layers of the business, including:

- Internal fraud team operations (intra-team ops)
- External department interactions (inter-team ops)
- External agency interactions (e.g., Law Enforcement entities)

This guide has been created based on best practice information as provided by both operator expertise and other industry expertise. It is expected to be a "living document", however, to account for changes in business practices, products, and technologies over time.

For further information on the Revenue Management Initiative [click here](#)

To return comments on this document click here

[Declaration of Patent Interest Form](#)

If you would like help on this material or to join current discussions please visit the [Fraud Management](#) Community Area

[Return to the Revenue Management Home page](#)

...donde importa la monitorización externa, pero sobre todo también la interna...

¿Por qué registrarse? | [Regístrate](#) | [Iniciar sesión](#)

EL PAÍS.com | Gente y TV Martes, 26/7/2011, 11:0

[Inicio](#) [Internacional](#) [Política](#) [España](#) [Deportes](#) [Economía](#) [Tecnología](#) [Cultura](#) [Gente y TV](#) [Sociedad](#) [Opinión](#) [Blogs](#) [In English](#)

ELPAÍS.com > Gente y TV

CiberP@ís [volver a tecnología](#)

CIBERSEGURIDAD

"Las doctrinas de vigilancia informática han quedado obsoletas"

Uri Rivner, representante de la empresa líder en el sector de la seguridad, aconseja usar solo tecnologías de virtualización para entrar en las redes

MERCÉ MOLIST - Barcelona - 27/06/2011

Vota ☆☆☆☆☆ | Resultado ★★★★★ 42 votos | [Twitter](#) 139 | [Recomendar](#) 76

La compañía israelí RSA, referente mundial en seguridad informática, se convertía recientemente en actor de lo que parece una novela *ciberpunk*: tropas virtuales de élite entraron en su red corporativa y robaron códigos que usaron para espiar a sus clientes, fabricantes de armamento del Ejército de Estados Unidos. Uri Rivner, representante de RSA, se defiende poniendo en duda las doctrinas de seguridad cibernética de los últimos 15 años.

La noticia en otros webs

- webs en español
- en otros idiomas

"Es la nueva guerra fría, con naciones que se espían las unas a las otras"

"Al concentrar la inversión en las defensas perimetrales, hemos dejado el interior menos protegido, algo que se está demostrando obsoleto. Hay que defender también el interior, asumir que tienes alguien dentro que va a hacer actividades maliciosas, **monitorizar** qué hacen los empleados para detectar movimientos extraños".

Así fue como descubrieron el ataque:

"Notamos una actividad irregular en la red interna. Parecía más un

publicidad

Génesis

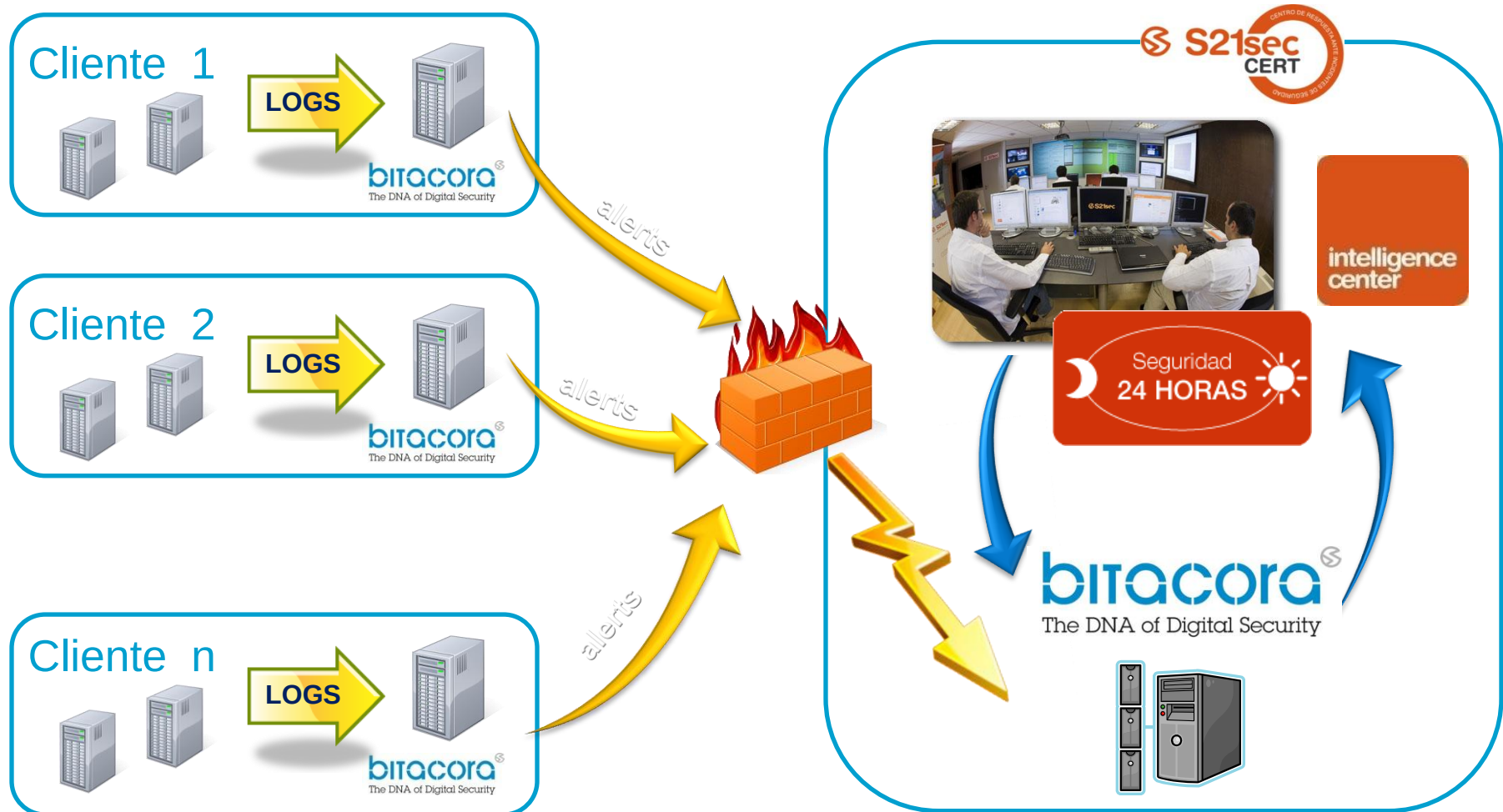
NADIE TE CUIDA COMO YO

Última Hora

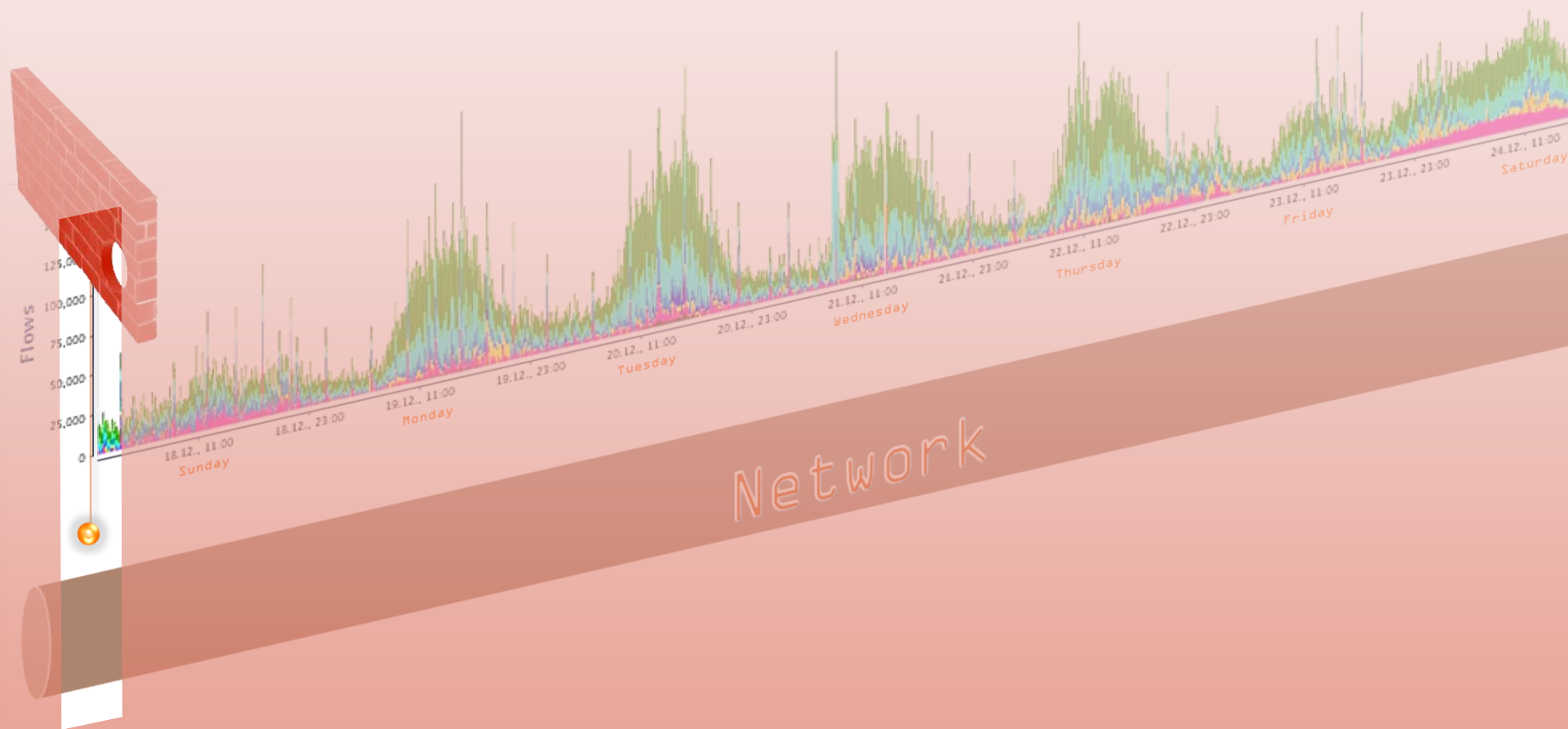
fw @miquelaberola: Más para Camps. El candidato, tras decirle a Camps que siempre será "Molt Honorable", se reclama pragmático y austero en la palabra. Apuesta por resolver y no crear problemas: "Estos son mis principios. Los principios de Francisco Camps y del PP"



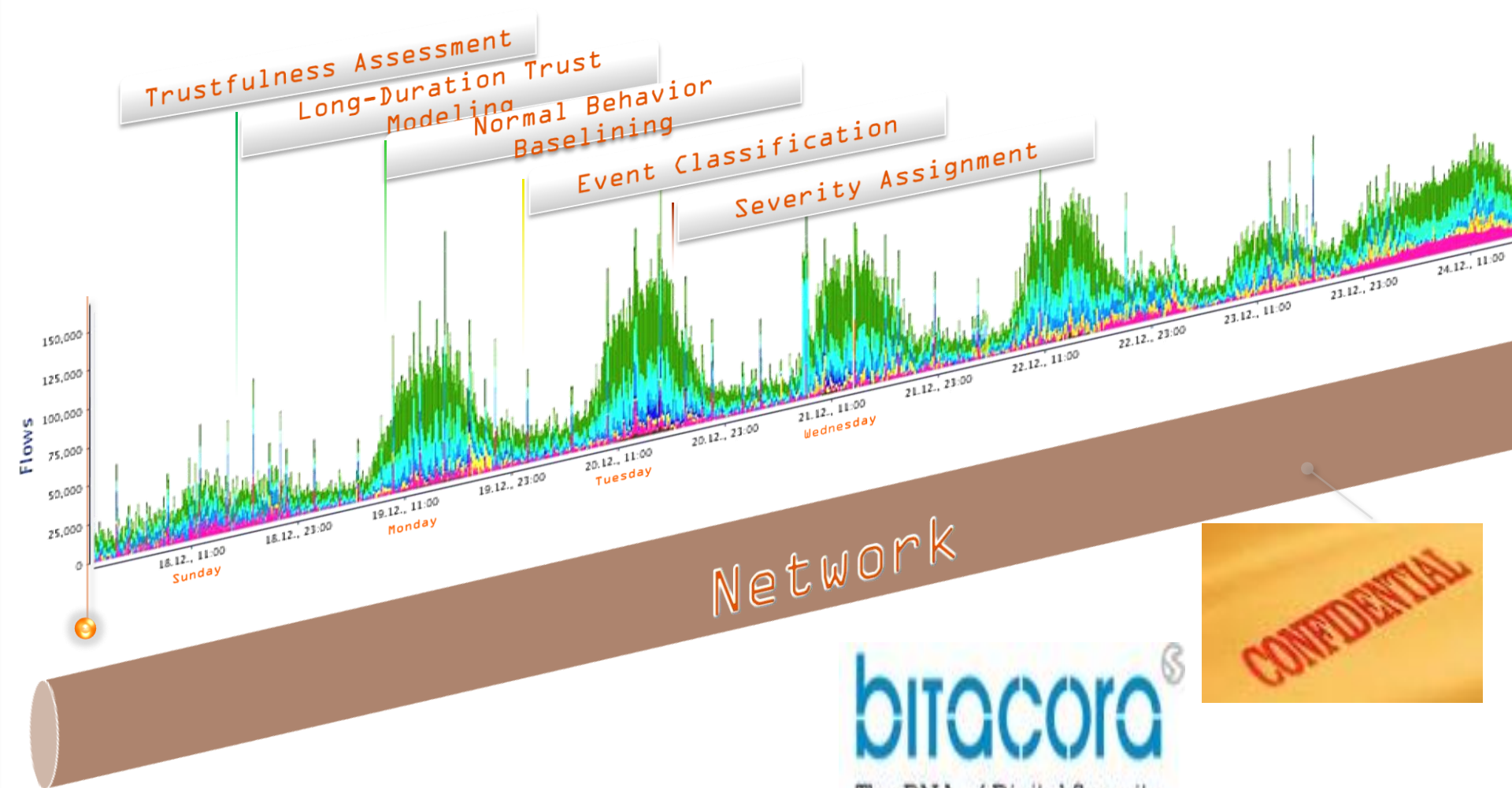
...uno de los principales servicios de S21sec...



...y como la seguridad basada en firmas no es suficiente...



...está en evolución y mejora frente a nuevas amenazas...



bitacora[®]
The DNA of Digital Security

CONFIDENTIAL

S21sec

...,de modo que apoye la gestión de incidentes...



...y permita evitar o reducir sanciones



GRACIAS

SPAIN • MEXICO • BRASIL • UK • USA

www.s21sec.com

