S21sec

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

// INDICE

//01

Introducción

En una sociedad hiperconectada…

S21sec

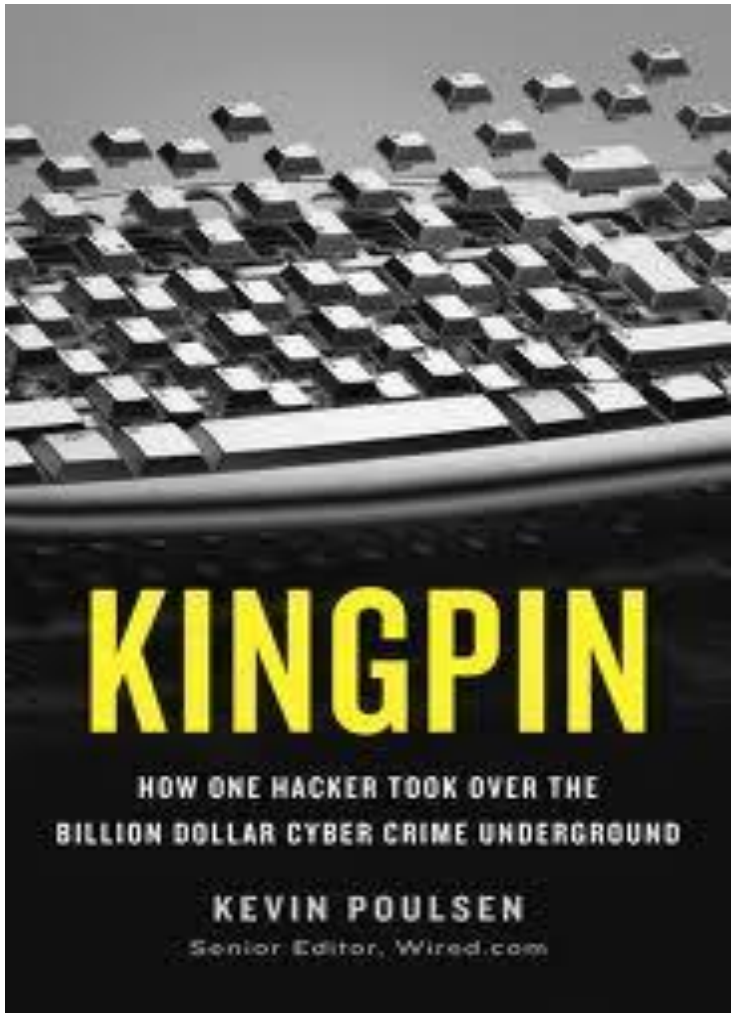
…donde la información es clave…

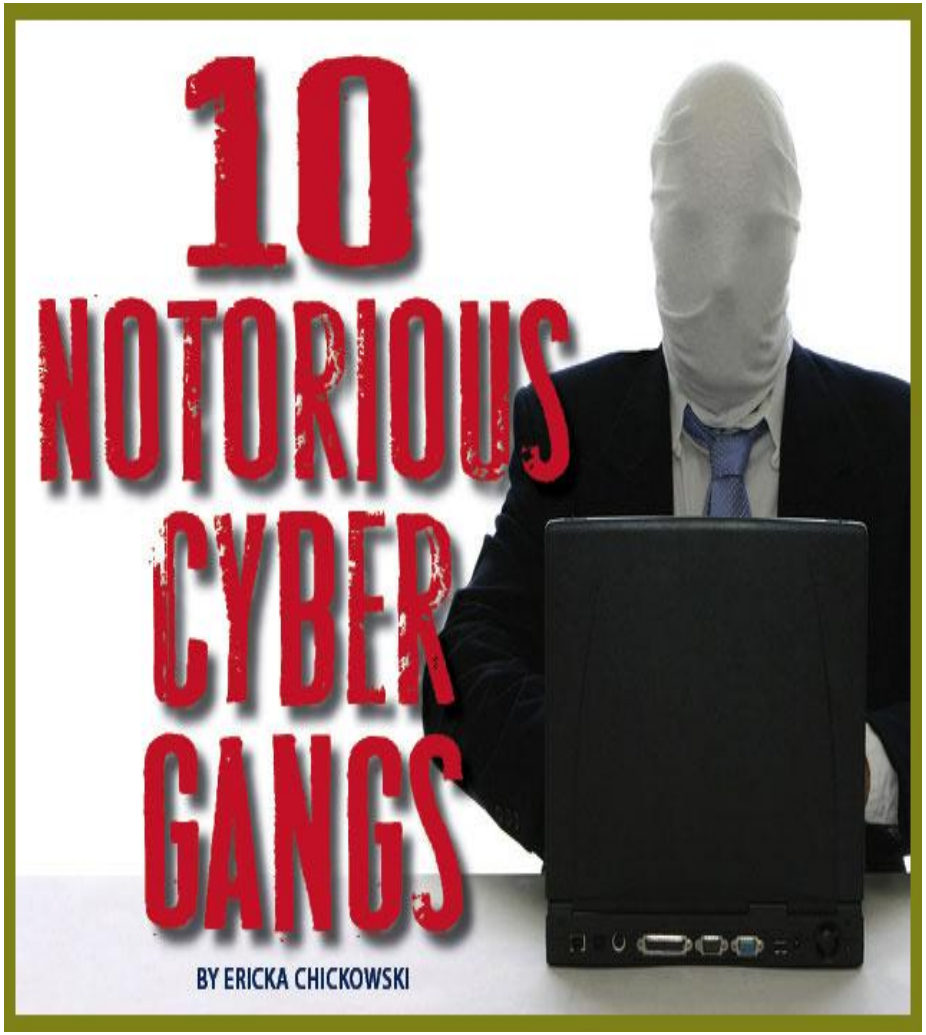
S21sec

…, de ahí, la llegada de la cibercriminalidad…

S21sec

…y la profesionalización del cibercrimen…





S21sec

…, donde las empresas TICs son esenciales…

S21sec

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

S21sec

… para generar y retener confianza

S21sec

//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 | buscar | RSS

ELPAIS.com > Tecnología

CiberPaís | 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 ★★★½☆ 40 votos | Twittear 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), envío 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.-

S21sec

Ataques a buzones de voz

S21sec

Robo de identidad…y de dinero

SC MAGAZINE AusCERT

SECURITY ON THE MOVE

AUSTRALIAN EDITION

SIGN IN JOIN

SC MAGAZINE SECURE BUSINESS INTELLIGENCE

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 30 Share 6 *3 Comments and 12 Reactions*

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.

Keywords

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

Related

Sign up to receive SC Magazine email newsletters

SIGN UP

FOLLOW US...

Most Read

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

S21sec

Fugas de información

S21sec

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

S21sec

Seguridad en la nube

rtve.es

Busca en rtve

Noticias | TV | Radio | Deportes

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

DIRECTO la vuelta

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 2

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. | Twittear 2 | +1 0 | Enviar

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

S21sec

Espionaje industrial…que salta fronteras

ZDNet

Search

Australian edition | NBN | Telstra | Government | Filter | Security | Android | Apple | Mobile Pho

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.

S21sec

Análisis forenses

S21sec

Al servicio de la ley

PORTALTIC.es | INTERNET

domingo, 13 de mayo 2012 editado por europa press

IBM PureSystems
Descúbralo ya en nuestro Webcast
Inscríbase aquí

Buscar...

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

9 6 menea tuenti Share +1 0

Anuncios Google

Comercio de divisas Fácil
Únase a Easy-Forex: comercio

The Pirate Bay

Foto: THE PIRATE BAY
Ampliar foto

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 Tribunal Superior de Justicia de Reino Unido para que los principales

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

ONO 6Mb + TLF + TV

Portaltic

S21sec

Medidas de seguridad en tela de juicio

WIRED SUBSCRIBE » SECTIONS » BLOGS » REVIEWS » VIDEO » HOW

Sign In | RSS Feed

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

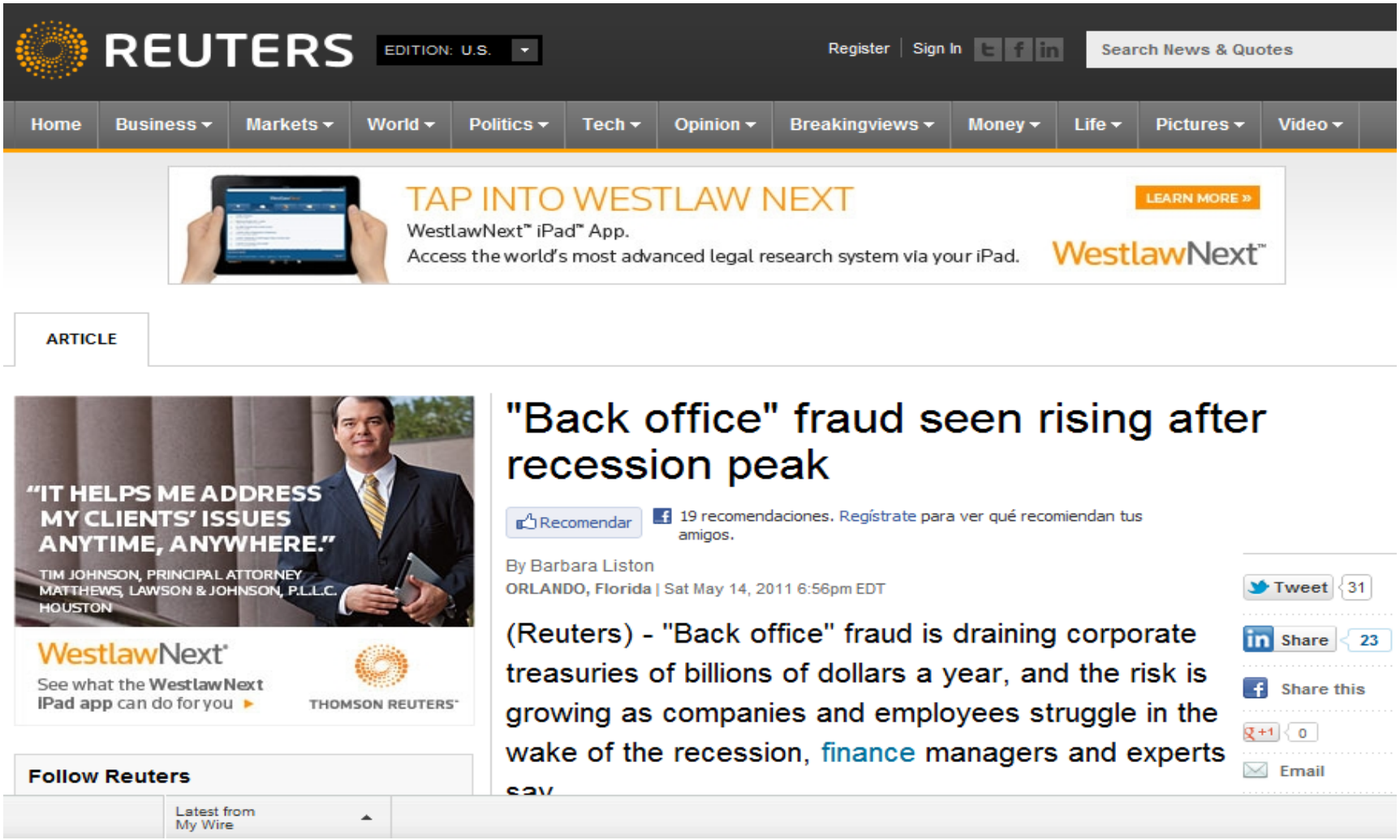
S21sec

//03

Algunos problemas de fraude

*

Fraude back-office, como en otro lugar



S21sec

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

Search All NYTimes.com

WORLD | U.S. | N.Y. / REGION | BUSINESS | TECHNOLOGY | SCIENCE | HEALTH | SPORTS | OPINION | ARTS | STYLE | TRAVEL | JOBS | REAL ESTATE | AUTOS

Search Business

Financial Tools — Select a Financial Tool

More in Business »
Global Business | Markets | Economy | DealBook | Media & Advertising | Small Business | Your Money | Energy & Environment

Telecom Italia Delays Results Because of Money-Laundering Scandal

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

TWITTER
LINKEDIN
SIGN IN TO E-MAIL
PRINT
REPRINTS
SHARE

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

Mlo Scialy/European Pressphoto Agency

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

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.

Add to Portfolio

Telecom Italia SpA
Swisscom AG

to&opzn&page=ww...

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.

Sign Up

See Sample | Privacy Policy

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: Gay Marriage Bans 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
	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
	Construction and engineering	£567 million	Corporate fraud against large businesses	£360 million
			Small to medium sized business fraud	£206 million
	Consumer goods	£294 million	Corporate fraud against large businesses	£294 million
			Small to medium sized business fraud***	-
	Natural resources	£135 million	Corporate fraud against large businesses	£111 million
			Small to medium sized business fraud	£24 million
	Healthcare	£132 million	Corporate fraud against large businesses	£132 million
			Small to medium sized business fraud	£0.31 million
	Other	£50 million	Corporate fraud against large businesses	-
			Small to medium sized business fraud	£50 million
Third sector £1.3 billion	Charity	£1.3 billion	Charity fraud	£1.3 billion
Individuals £4 billion	N / A	£4 billion	Mass marketing fraud	£3.5 billion
			Rental fraud	£314 million
			Online ticket fraud	£168 million
Total AFI 2011 fraud loss		£38.4 billion		£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.

S21sec

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

S21sec

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 | Search

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, old.

rbc.bidder7.mookie1.com...

RECOMMENDED ON THE MIRROR Why?

S21sec

Fraude PBX

S21sec

Fraude subscripción

EL PAÍS.COM Internacional | Política | España | Deportes | Economía | Gente y TV | Sociedad | SModa ← Ir a portada de ELPAÍS.com

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: ELPAIS.com> Edición Impresa> España

Una red de empleados de telefonías estafó a estas 27 millones

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

Vota ☆☆☆☆☆ | Resultado ★★★★½ 49 votos Twittear 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.oriente9.es
Ver más juguetes

Última Hora
La presidenta y consejera delegada de *The New York Times Company*, Janet

S21sec

Malware y fraude servicios premium

S21sec

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.

Traffic lights have become attractive targets for thieves in Johannesburg

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.

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

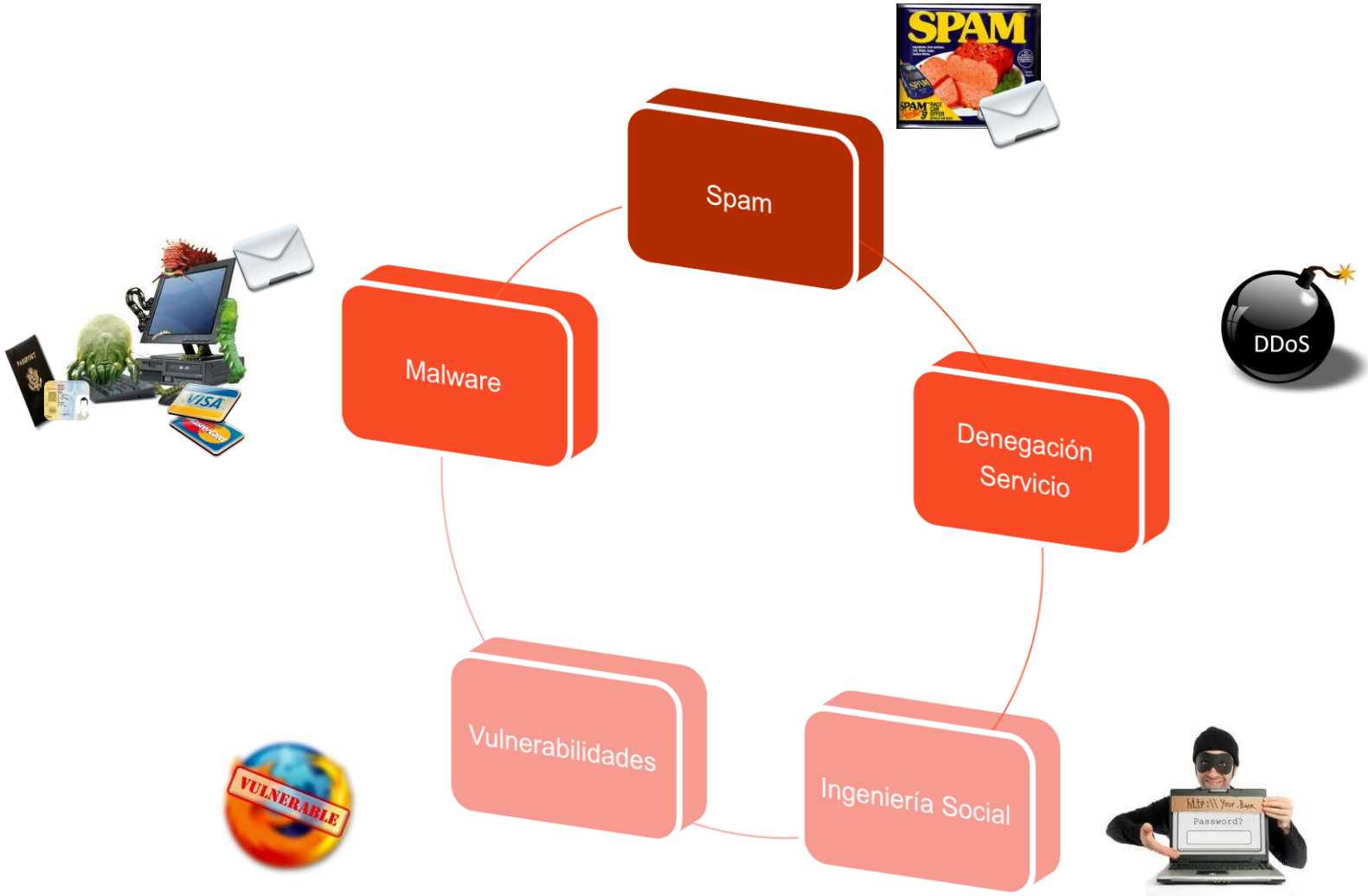
S21sec

//04

Evolución, a peor, del problema

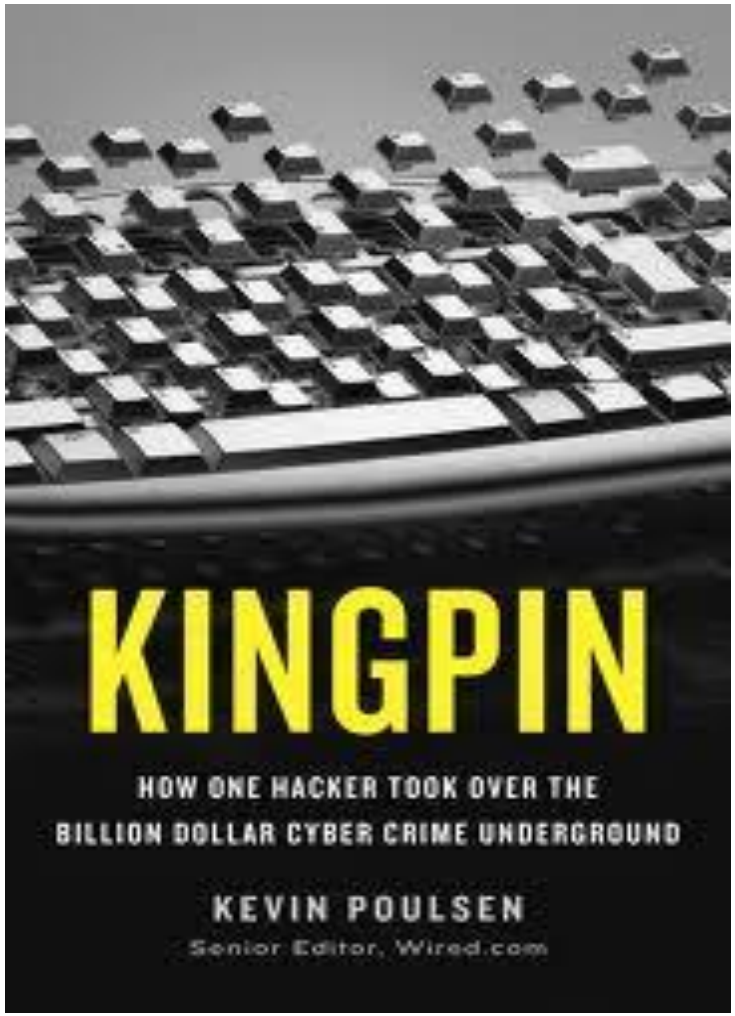
*

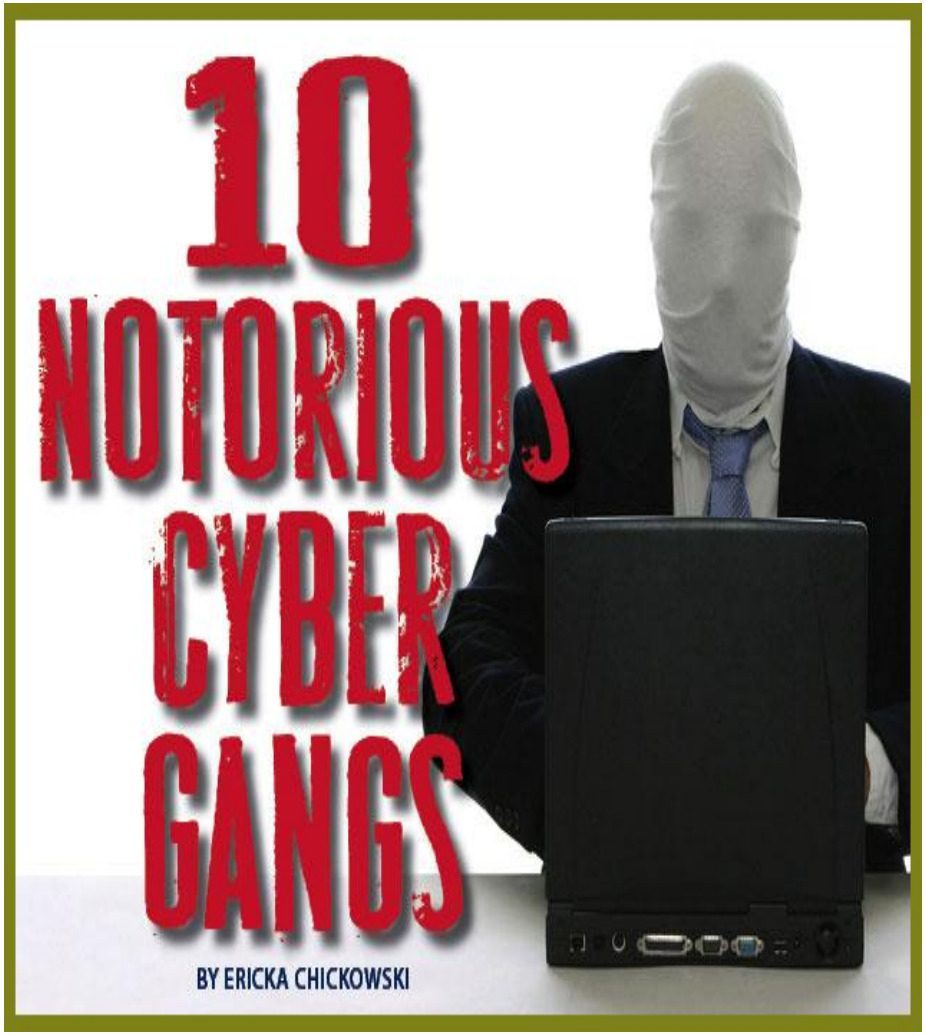
De las clásicas amenazas…



S21sec

… pasando por la profesionalización del cibercrimen…





S21sec

…se ha evolucionado a la gran amenaza…

S21sec

…con distintos objetivos,…

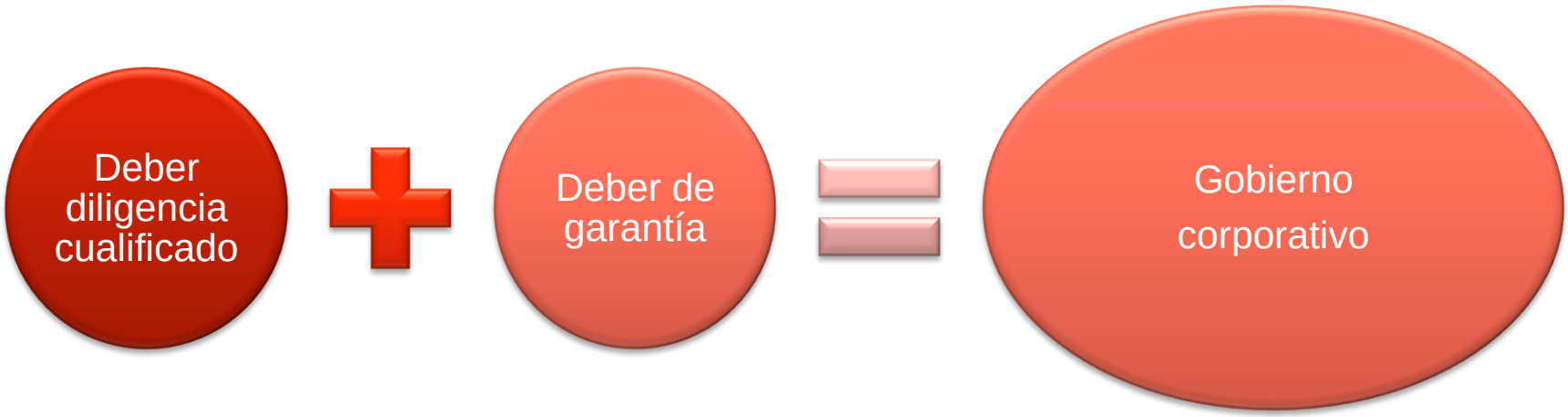
S21sec

//05

Obligaciones de los operadores

*

Gobierno Corporativo…

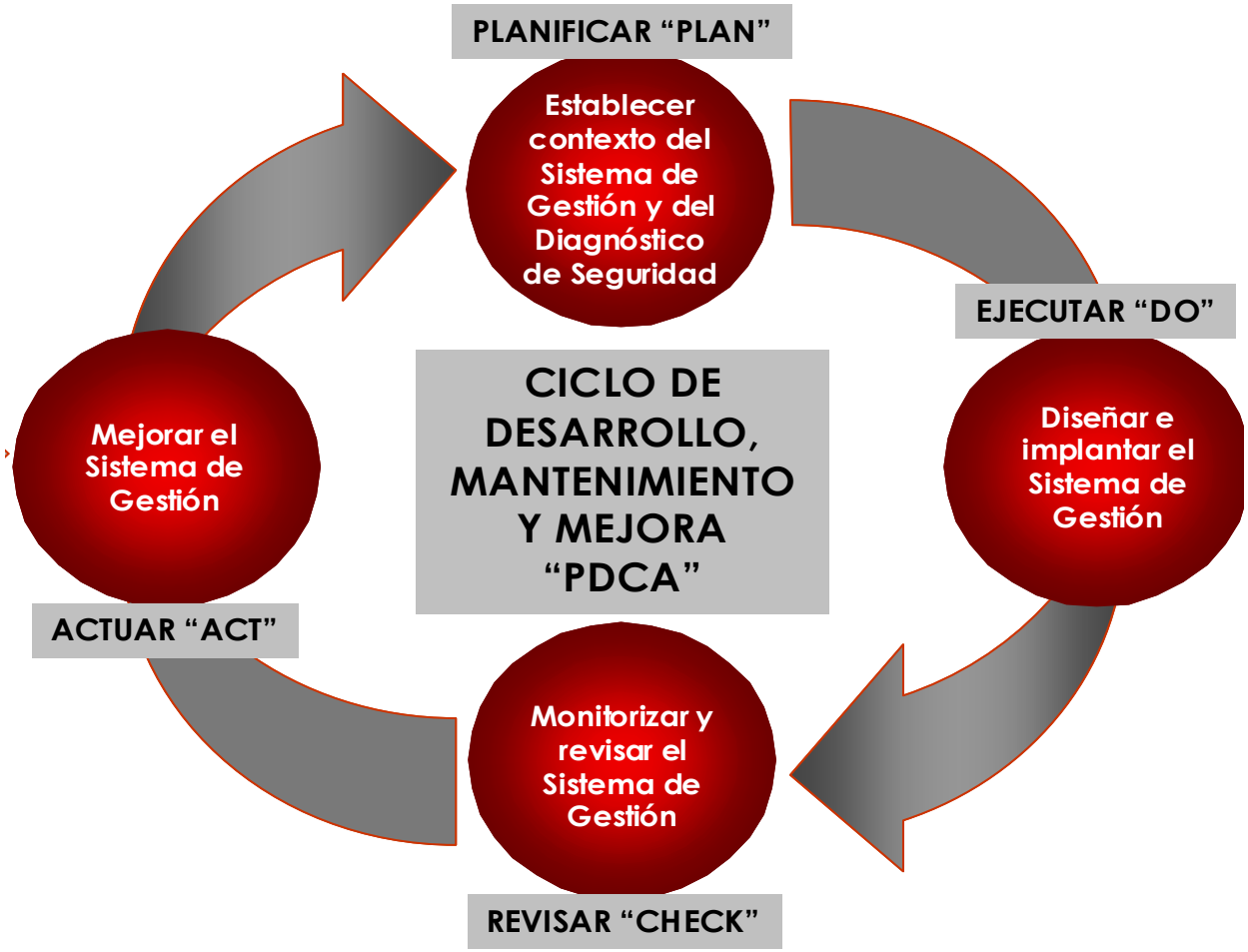


S21sec

…gestionando el riesgo…

S21sec

…, en un proceso de mejora continua…

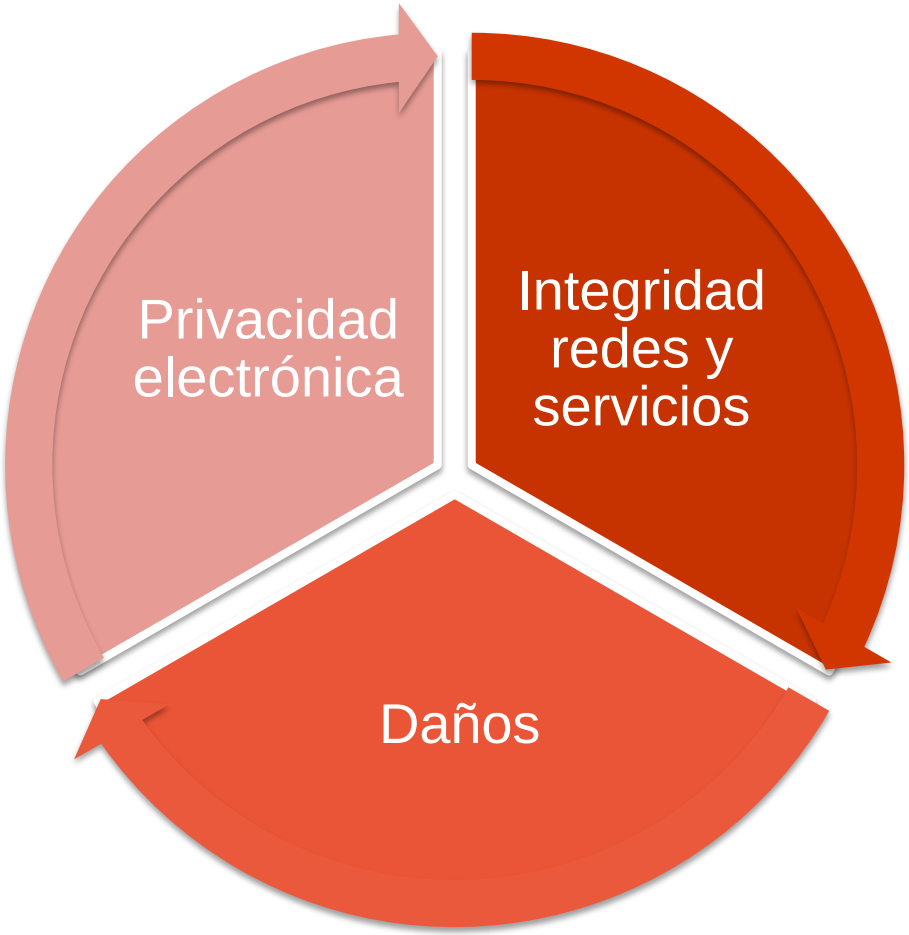


S21sec

Diversas obligaciones de seguridad…

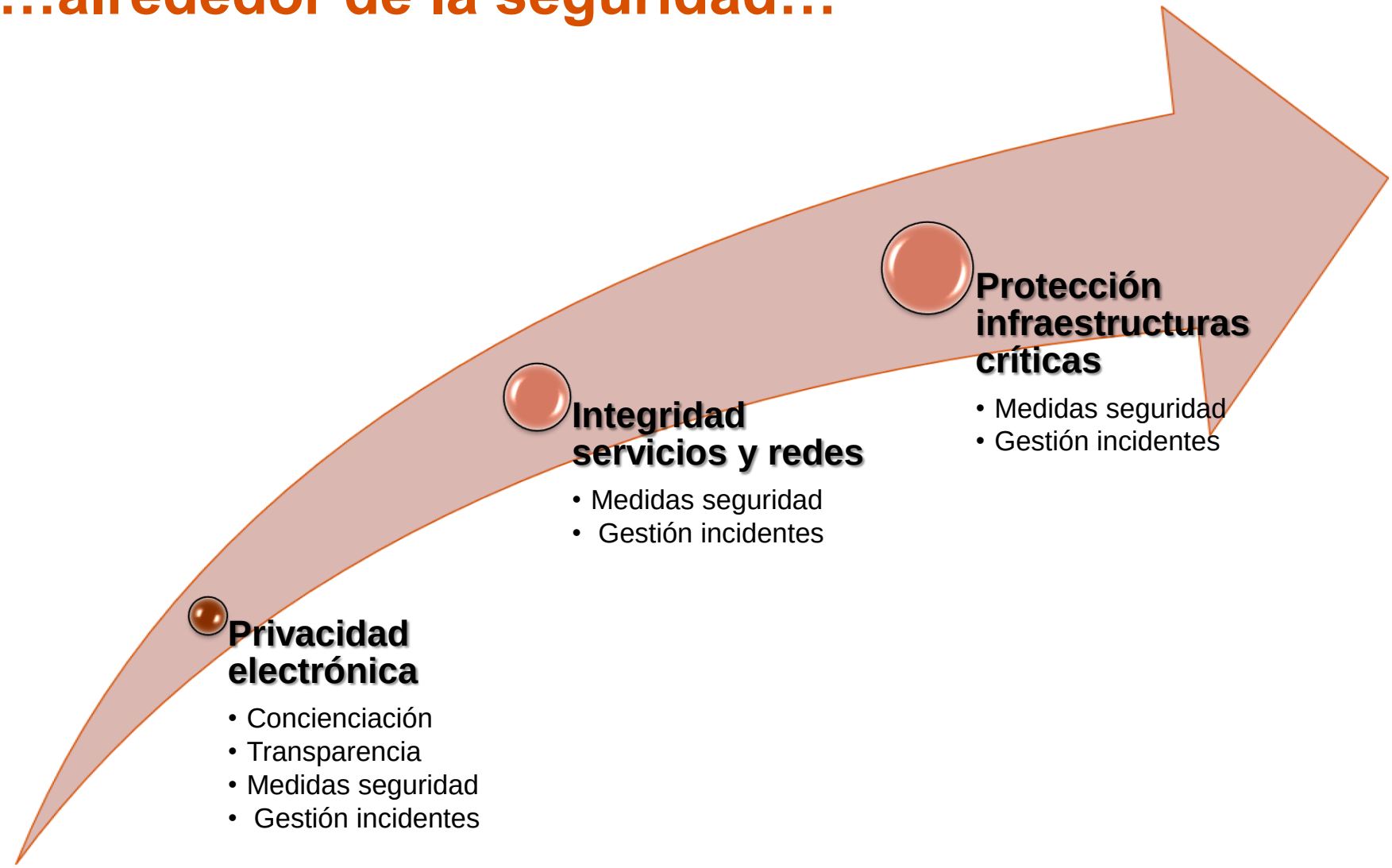
S21sec

…con objetivos distintos, pero interrelacionados…



S21sec

…alrededor de la seguridad…



S21sec

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

Personas Físicas

Personas Jurídicas

Infraestructuras Críticas

SOCIEDAD

S21sec

//06

Gestión de seguridad y lucha contra el fraude

*

Eeeeeh,… ¿eso cómo se hace?

S21sec

Pues con un enfoque integral…

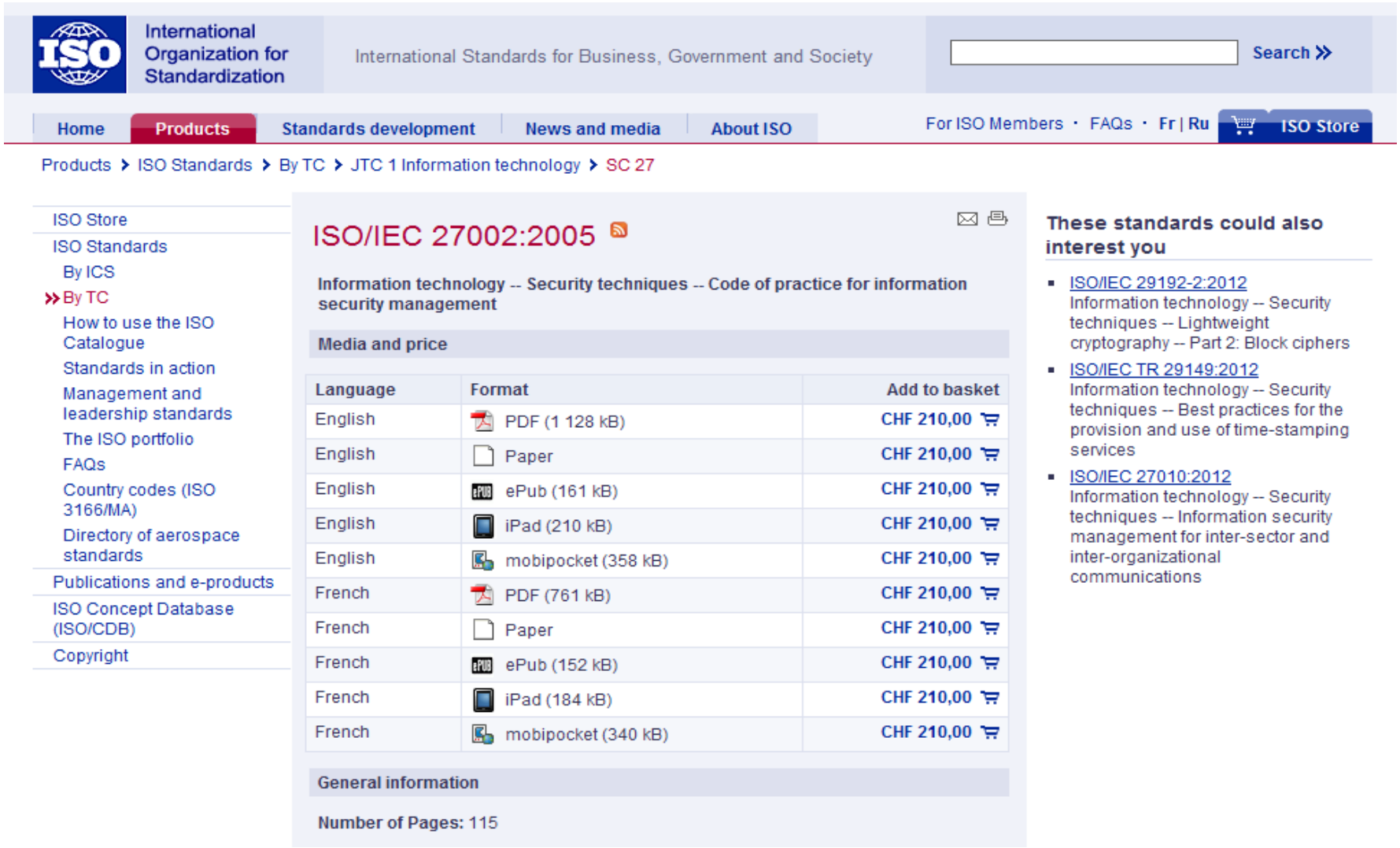
Seguridad Física

Área Común

Seguridad Lógica

S21sec

…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

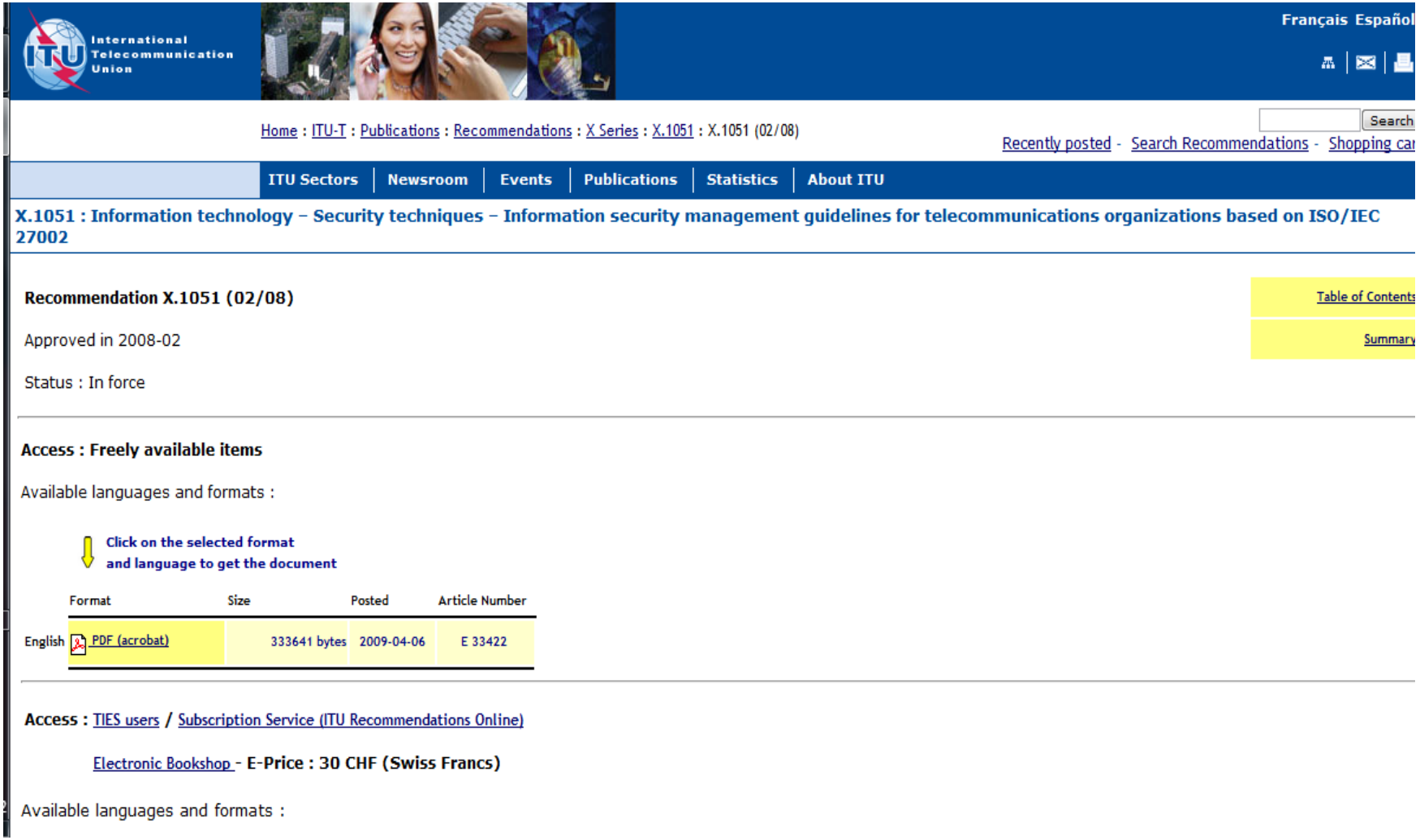
Number of Pages: 115

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

S21sec

…y sectoriales de seguridad…



International Telecommunication Union

Français Español

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

Search

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)

Table of Contents

Summary

Approved in 2008-02

Status : In force

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

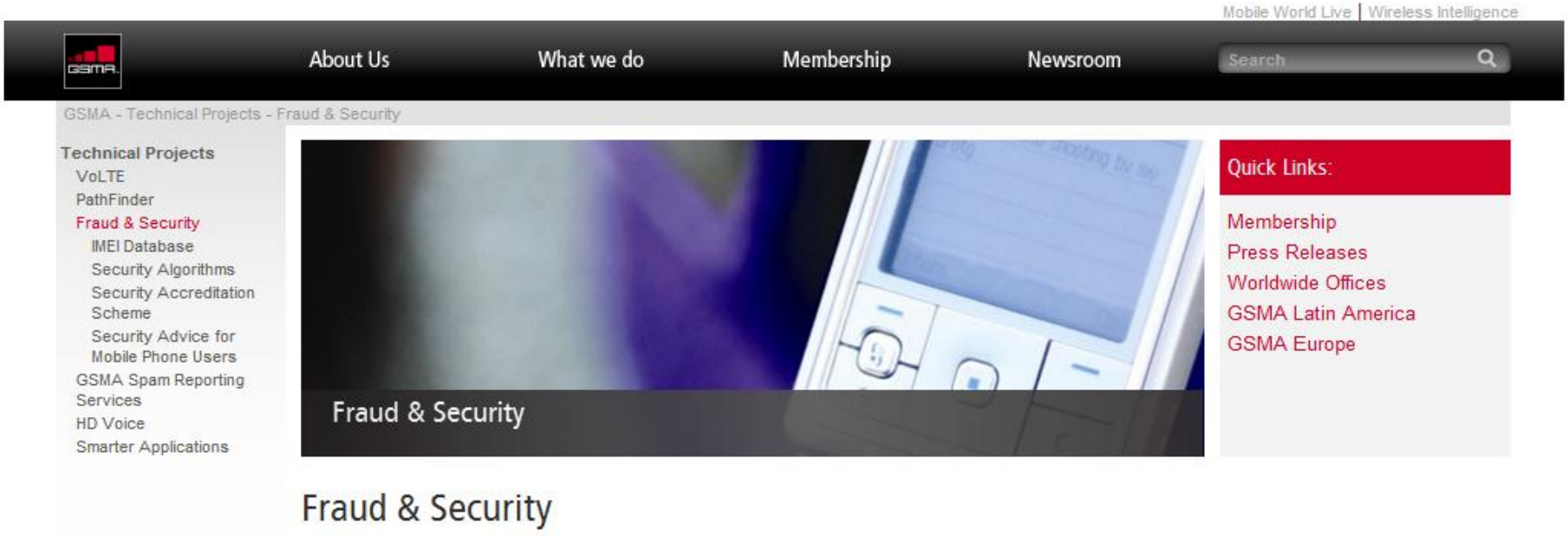
Access : TIES users / Subscription Service (ITU Recommendations Online)

Electronic Bookshop - **E-Price : 30 CHF (Swiss Francs)**

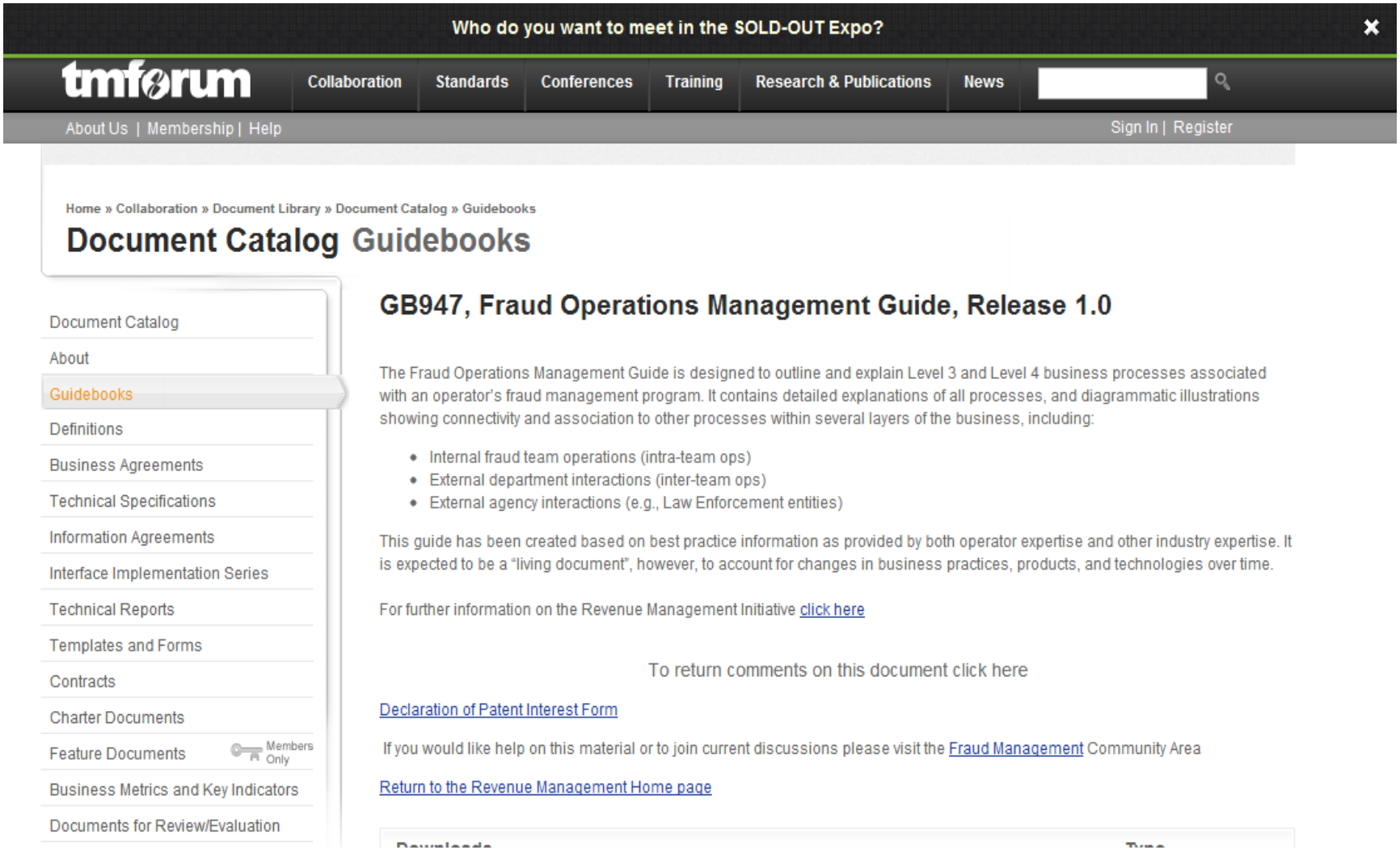
Available languages and formats :

S21sec

…de seguridad y fraude…



S21sec


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
Members Only
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

S21sec

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

¿Por qué registrarse? | Regístrate | Iniciar sesión

EL PAÍS.com | Gente y TV

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

ELPAIS.com > Gente y TV

CiberPaís 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

MERCÈ MOLIST - Barcelona - 27/06/2011

Vota | Resultado 42 votos | Twittear 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 Riv-ner, 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

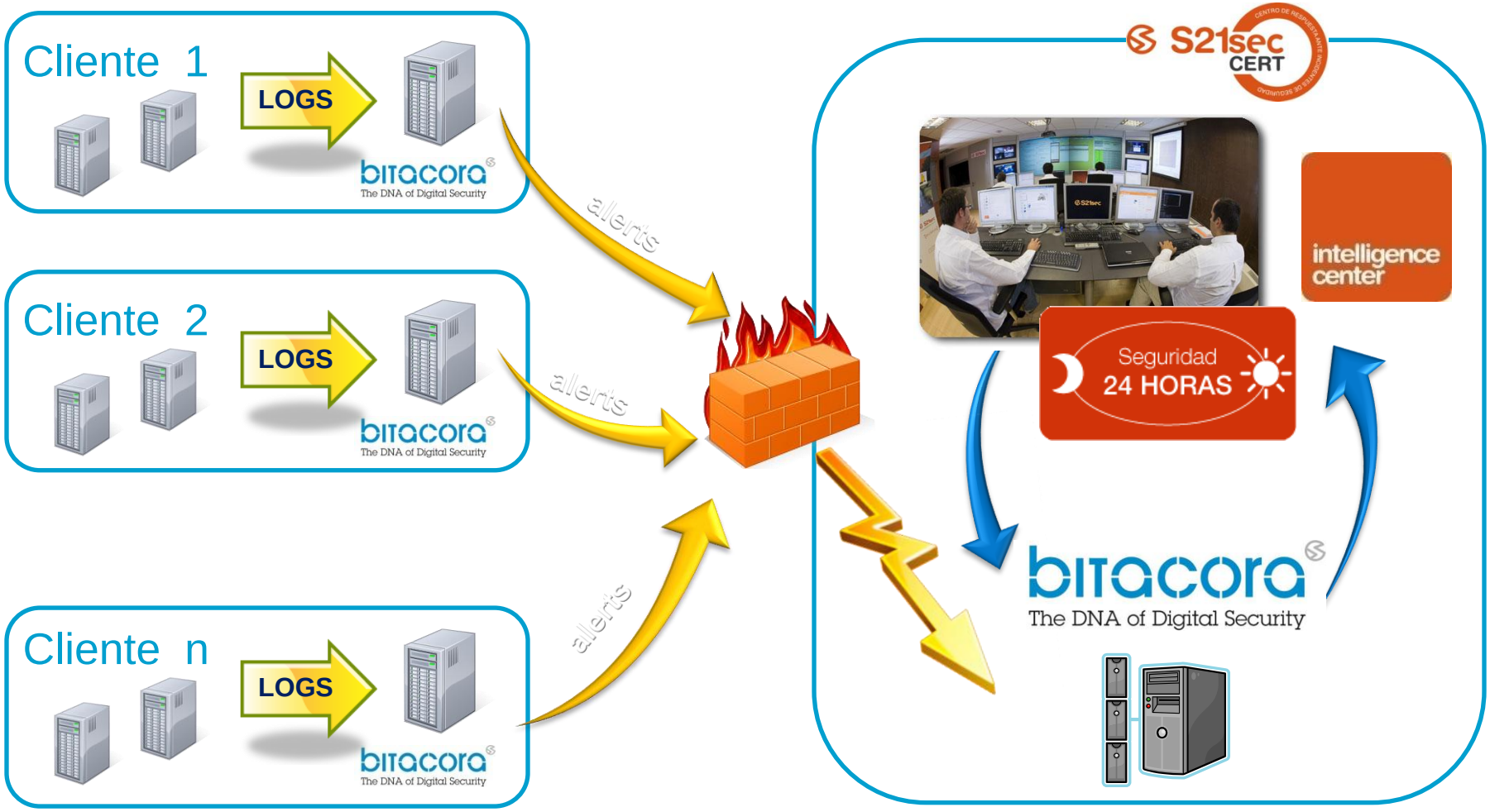
Génesis
NADIE TE CUIDA COMO YO

Última Hora

fwd @miquelalberola: **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"

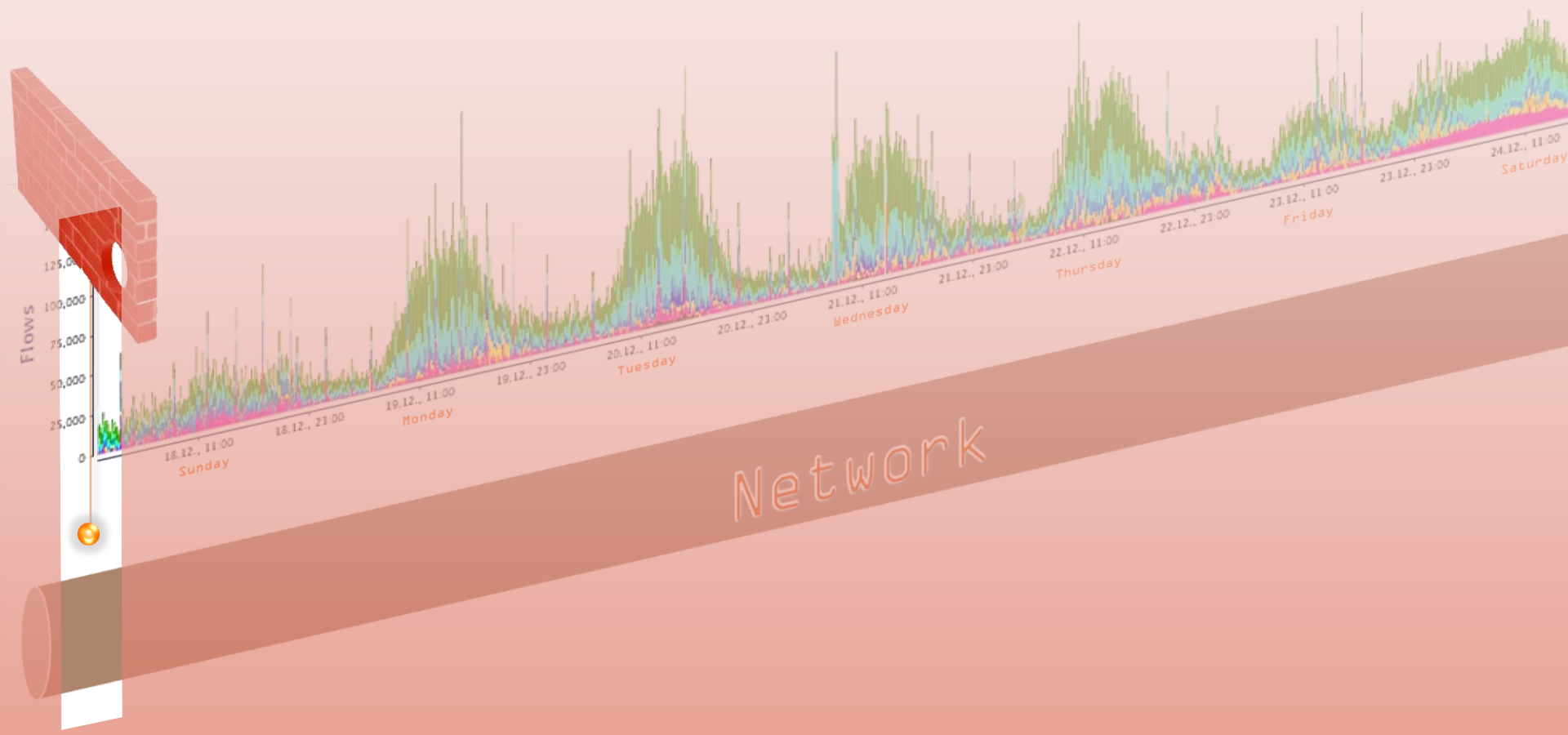
S21sec

…uno delos principales servicios de S21sec…



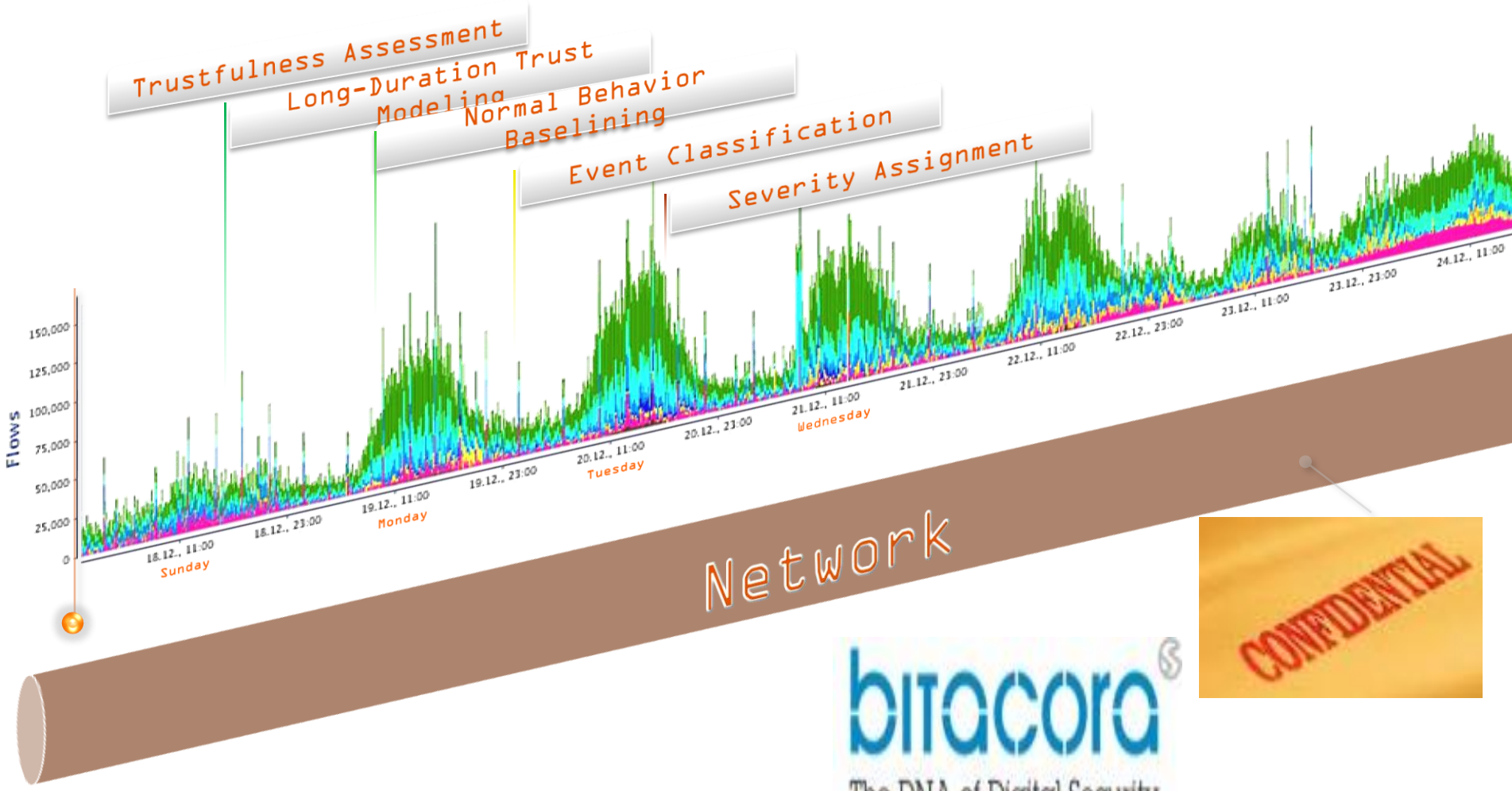
S21sec

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



S21sec

…está en evolución y mejora frente a nuevas amenazas…



bitacora®
The DNA of Digital Security

S21sec

…,de modo que apoye la gestión de incidentes…

S21sec

…y permita evitar o reducir sanciones

S21sec

GRACIAS

SPAIN • MEXICO • BRASIL • UK • USA

www.s21sec.com

S21sec

Comprometidos con la seguridad