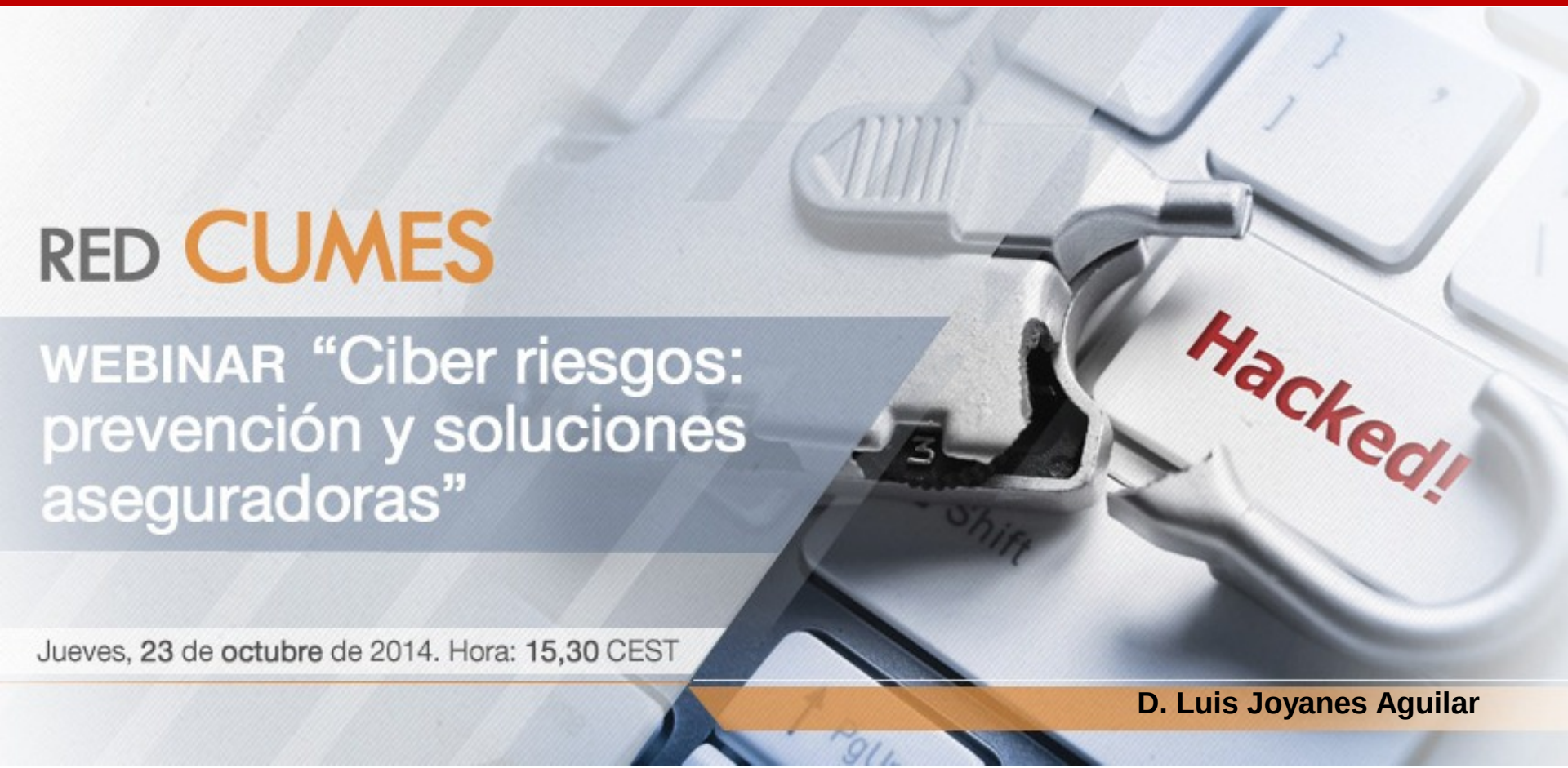
FUNDACIÓN MAPFRE

RED CUMES
La red para profesionales del seguro



D. Luis Joyanes Aguilar

ETIQUETAS DE CIBERSEGURIDAD

EL CIBERESPACIO

- El término fue acuñado por ***William Gibson,*** un escritor de ciencia ficción en el año 1982. Posteriormente en 1984 reiteró el término en su novela "***Neuromancer***"
- **Hoy día se ha convertido un el conjunto de dispositivos de computación, redes, cables de fibra óptica, enlaces inalámbricos y otras infraestructuras que llevan Internet a miles de millones de personas alrededor del mundo.**
- El ciberespacio ofrece grandes oportunidades y también tiene un ***lado oscuro*** que ha traído la necesidad de la **ciberseguridad** y todavía existe la **Web invisible o profunda** que presenta grandes e innumerables riesgos.

CIBERSEGURIDAD: Estado del arte y futuro

Prof. Luis Joyanes Aguilar

TELMEX INAGURA EL PRIMER CENTRO DE CIBERSEGURIDAD DE MÉXICO Y DE LATINOAMÉRICA (30 septiembre, 2014)

- Durante la inauguración del centro, el Lic. Héctor Slim Seade indicó*: "En TELMEX, analizamos el panorama actual al que nos enfrentamos con los **ciberataques y el cibercrimen** al que estamos expuestos, por ello enfrentamos estos retos creando un Centro de Ciberseguridad, con el objetivo de prevenir y atender a nuestros clientes ante un ataque".
- * **http://blog.telmex.com/2014/09/30/telmex-inaugura-el-primer-centro-de-ciberseguridad-de-mexico-y-latinoamerica/**

CENTRO DE CIBERSEGURIDAD DE TELMEX (30 septiembre, 2014)

- Actividades principales: **monitoreo 24X7** de los distintos componentes tecnológicos; emprendimiento de procesos de investigación y análisis de información para el envío de alertas ante posibles **ciberamenazas**
- El portafolio de este nuevo centro brindará a los clientes servicios como:
- **Diagnóstico y Protección contra Amenazas Avanzadas**
- **Servicios Forenses Avanzados**
- **Gestión Continua de Ciberriesgos basada en Inteligencia y Ciberinteligencia.**

ALIANZA Telefónica-Kaspersky

- **Telefónica y Kaspersky se alían para ofrecer ciberseguridad en Europa y Latinoamérica (junio 2014)**
- Cooperación estratégica en virtud del cual se mejorará el servicio de detección de amenazas de la operadora
- En concreto, en virtud de este acuerdo, Telefónica incorporará a su cartera de ciberseguridad los servicios de ciberinteligencia de Kaspersky Lab.

LA CIBERSEGURIDAD "HOY-MAÑANA"

- Un estudio de **Fortinet** señala que los principales retos a los que se enfrentan los **responsables de TI** españoles a la hora de mantener la **seguridad** de sus organizaciones son:

- Las tecnologías emergentes, como la **Internet de las Cosas (IoT)** y la **biometría**, seguidos del **BYOD (llevar su propio dispositivo a la empresa)** y de la creciente frecuencia y complejidad de las **amenazas** **APT (Advanced Persistent Thread), ataques DDOS y otras amenazas …**

LA CIBERSEGURIDAD "HOY-MAÑANA"

- La problemática en torno a la **privacidad de datos** es lo que ha llevado a que el 88% de los responsables de TI españoles estén planteando cambiar su estrategia de seguridad e invertir en seguridad, mientras que para otro 88% el principal impulsor del cambio es **big data** y la **analítica de datos**. En España, los sectores más predispuestos a invertir en seguridad son el sector de viajes y ocio y los servicios financieros, y las organizaciones de mayor tamaño son las que muestran también una mayor tendencia a la inversión. En este sentido, un 82% de los encuestados cree que contará con suficientes recursos en los próximos 12 meses.

LA CIBERSEGURIDAD "HOY-MAÑANA"

- Computerworld. Sociedad de la información | Noticias | 21 OCT 2014
- **Obama ordena que las tarjetas de crédito del gobierno posean un chip y código PIN**
- La medida llega tras las brechas de seguridad relacionadas con los pagos y sistemas bancarios que han afectado a más de 100 millones de americanos durante el último año. Esta medida podría empujar a los retailer y bancos a mejorar de esta forma sus propias tarjetas y sistemas.

LA CIBERSEGURIDAD "HOY-MAÑANA"

- **Cibercriminales rusos ganan hasta 680 millones de dólares con tarjetas robadas**
- Hasta 6,78 millones de tarjetas robadas puestas a la venta han sido descubiertas en el mercado llamado 'Swiped', uno de los seis sites más relevantes en los que se comercializa con tarjetas robadas, según la investigación reciente realizada por Group-IB. De estos, 5,5 millones han sido subidas sólo en el último año. El acceso ilegal a sistemas financieros alcanza los 426 millones de dólares.
- **Computerworld.es- Sociedad de la información | Noticias | 21 OCT 2014**

LA CIBERSEGURIDAD "HOY-MAÑANA"

- Riesgos tecnológicos en aumento que no parecen encontrar límites; así lo refleja por tercer año consecutivo el Informe de Riesgos Globales del World Economic Forum, que **sitúa el aumento de ciberataques, el robo de datos y la caída de redes e infraestructuras críticas entre las principales amenazas globales**.
- Gobiernos de todo el mundo han sido señalados en los últimos años como autores activos y pasivos en este tipo de amenazas. Nombres como Careto, **Stuxnet,** Flame o Duqu constituyen algunos de los recientes ciberataques más potentes llevados a cabo hasta el momento contra sistemas críticos de empresas, instituciones y naciones.

LA CIBERSEGURIDAD "HOY-MAÑANA"

- Está muy extendida la idea de que solo las empresas de *e-commerce* y las compañías que realizan transacciones en Internet tienen que preocuparse de los **ciberriesgos**, pero en realidad todas las empresas que utilizan Internet y sobre todo, el **sector minorista, hotelero, aéreo, financiero y de la comunicación**, entre otros, son los que más a menudo se enfrentan a riesgos de este tipo.

LA CIBERSEGURIDAD "HOY-MAÑANA"

- **Existe gran variedad de peligros en la red, entre los que destacan la violación de la privacidad, los riesgos multimedia Las redes sociales *y e/* contenido generado por el usuario (UCG) , la ciberextorsión y los fallos en la red. El más conocido y común de todos ellos es la violación de la información. Este tipo de riesgo provoca una extraordinaria cuantía de costes a los que tiene que hacer frente la compañía.**

LA CIBERSEGURIDAD "HOY-MAÑANA"

- **El cibercrimen se ha profesionalizado, y su lucha exige procedimientos nuevos**
- Día 09/10/2014 **director de Inteco**, Miguel Rego.
- **Hasta septiembre el Instituto Nacional de Tecnologías de la Comunicación ha gestionado alrededor de 11.000 incidentes relacionados seguridad en la red**
- **Computadores «zombie»** manejados por control remoto, amenazas altamente sofisticadas contra estados, tráfico de armas en la web más profunda: el *cibercrimen* se ha profesionalizado y exige herramientas más eficaces para combatirlo distintas a las tradicionales

LA CIBERSEGURIDAD "HOY-MAÑANA"

- **Los «ciberataques» a administraciones y empresas estratégicas españolas se dispararon un 82% en 2013**
- **http://www.abc.es/tecnologia/redes/20140310/abci-ataques-informaticos-201403101620.html**
- Según estos datos, recogidos por Europa Press, durante el año pasado el Centro Criptológico gestionó un total de 7.263 ciberincidentes, **lo que supuso un 82 por ciento más** que en el ejercicio anterior, al tiempo que notificó más de 11.370 vulnerabilidades de hardware y software y realizó 50 informes de amenazas, actualidad y código dañino.

EL FUTURO DE LA CIBERSEGURIDAD

- Remedies. **Prevention es better than cure. More vigilance and better defences can make cyberspace a lot safer. (*The Economist*, 12-18th July 2014)- El Ciberespacio nunca será totalmente seguro.**
- **MICROSOFT** (junio 2014). ***Cyberspace 2025 Today's Decisions, Tomorrow's Terrain***

EL FUTURO DE LA CIBERSEGURIDAD

- En marzo de 2014 un grupo de empresas incluyendo Cisco, AT&T, GE e IBM, crearon **Industrial Internet Consortium** para potenciar el Internet Industrial soportado en el **Internet de las cosas** (**www.iiconsortium.org**) y **enfrentarse a las políticas de ciberseguridad**. se han unido Microsoft, Deloitte, Toshiba, Samsung…

CIFRAS DE LA CIBERSEGURIDAD

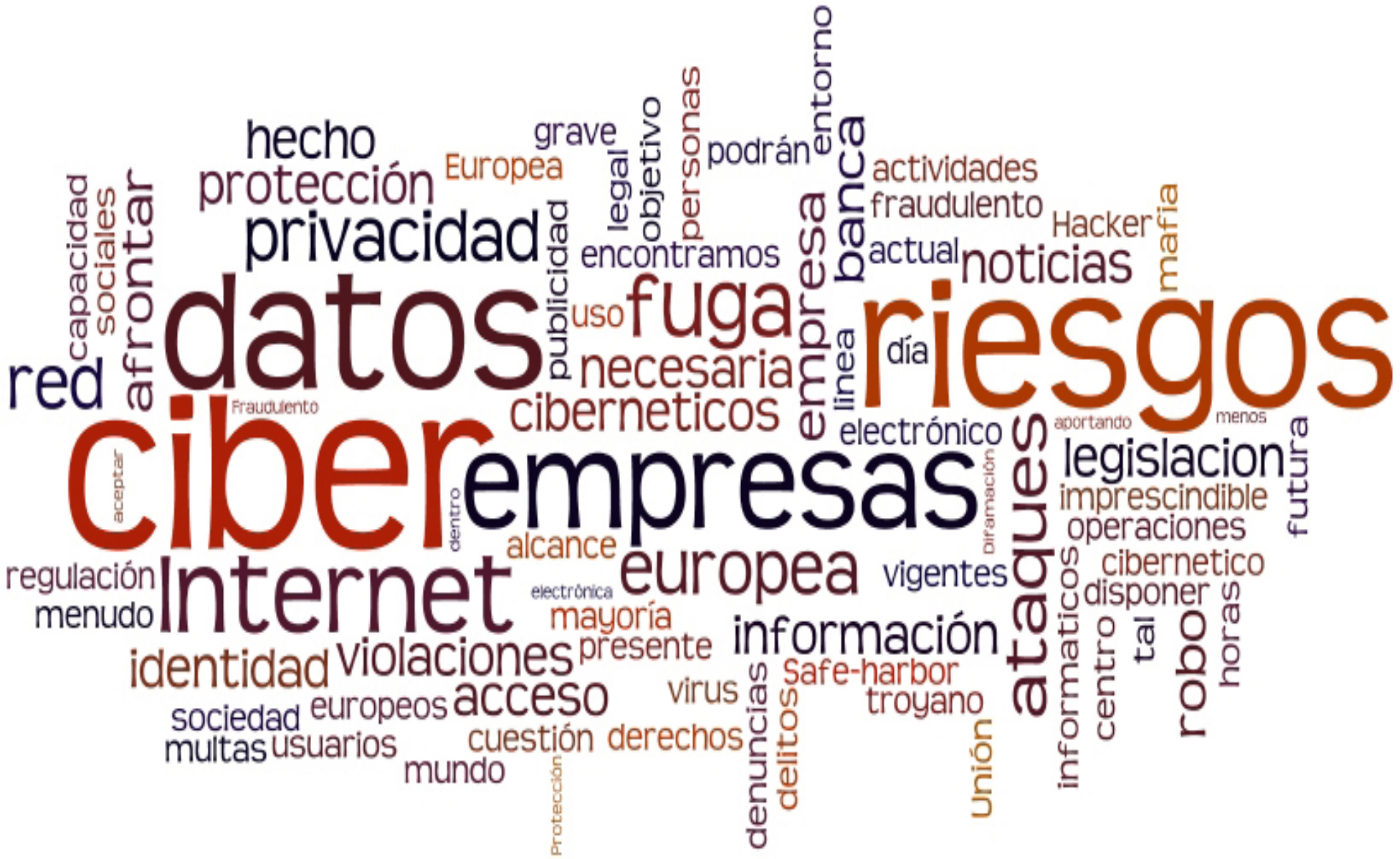
- En un mundo donde la tecnología está permeando todos los aspectos de los negocios y del funcionamiento de los gobiernos, la seguridad es cada vez más compleja y las medidas tradicionales ya no son adecuadas para hacer frente a las **nuevas amenazas** surgidas por **las nuevas tendencias tecnológicas**, como **el cambio a aplicaciones basadas en la web, la migración de la infraestructura en la nube, el BYOD, además del aumento de las ciberamenazas internas y externas.** Según datos de MarketsandMarkets, se espera que el mercado global de la ciberseguridad crezca de 95.600 millones de dólares en 2014 hasta **155.740 millones** de dólares en 2019, a una tasa compuesta anual del 10,3%.

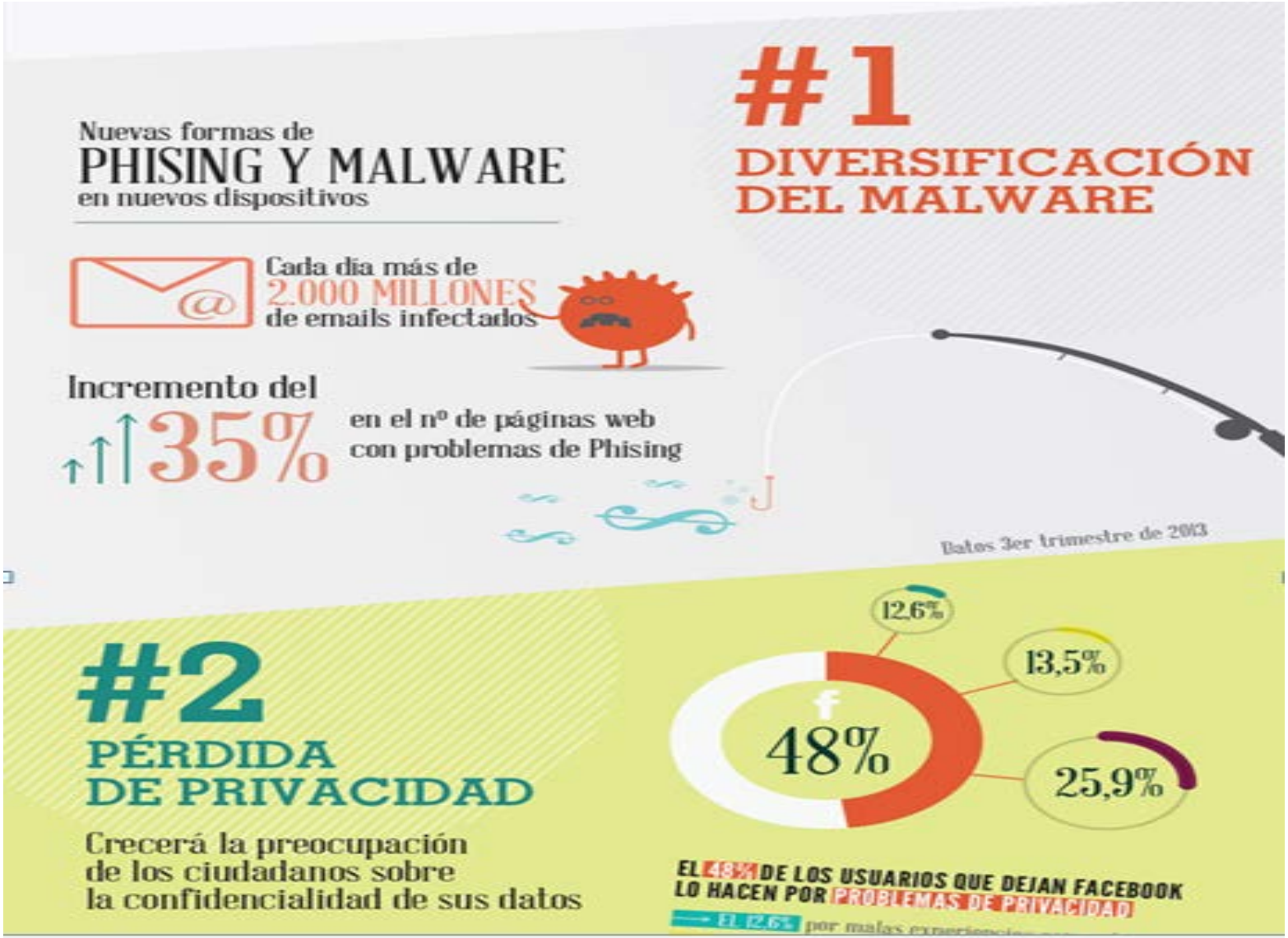
La web profunda (*Deep Web*)

- 213 millones de referencias (Google, 15 de julio 2014)
- **Jill Ellsworth utilizó el término "la Web invisible" en 1994 para referirse a los sitios web que no están registrados por algún motor de búsqueda.*La Web invisible.*** Pese a que TOR se lanzó hace una década, en los últimos tiempos ha sido abordada con ingentes dosis de sensacionalismo por la prensa generalista. De todas los mitos que se han creado en torno a la web profunda destacan dos: que es **refugio de ladrones, criminales o pedófilos,** que es **muy peligroso** navegar por ella y que su contenido representa el **96 %** del volumen de datos que se mueven en la Red.

La web profunda (*Deep Web*)

- El sistema imperante en la *'deep web'* es **The Onion Router (TOR),** una red de comunicaciones que pone el énfasis en el **anonimato** de sus integrantes. Para conseguirlo, cifra los mensajes y los hace pasar por un número indeterminado de nodos de manera que sea, si no imposible, sí más difícil obtener la dirección IP del navegante. Precisamente su nombre ("***onion***" es cebolla en inglés) hace referencia a las distintas capas de anonimato que cubren los datos que se mueven por TOR. En cualquier caso TOR es **una parte de la 'deep web'.** **www.elconfidencial.com/ tecnologia/ 2013/04/09/ deep-web-un-paseo-por-los-bajos-fondos-de-internet-4641**





Tendencias de futuro en el mercado de la ciberseguridad

❑ MSSP (Servicios Gestionados de Seguridad)

- ❑ Las empresas están en una lucha constante para hacer frente a los nuevos retos de seguridad introducidos por la virtualización, el BYOD y las amenazas del cibercrimen organizado.
- ❑ Los servicios que ofrecen los proveedores MSSP incluyen el **bloqueo de virus, bloqueo de spam, detección de intrusos, firewalls, la gestión de redes privadas virtuales (VPN) y también la gestión de las modificaciones y actualizaciones de los sistemas**.

Tendencias de futuro en el mercado de la ciberseguridad

- **Security as a Service (seguridad en la nube)**
- Otra tendencia es la demanda creciente, sobre todo entre las pymes, de servicios de seguridad basados en la nube, para hacer frente a la falta de personal o de habilidades, reducir los costes, o para cumplir de forma rápida con las normas de seguridad. Estos incluyen, entre otros, **correo electrónico seguro, *gateways* web, administración de identidades y accesos (*Identity and Access Management* – IAM) y evaluación en remoto de la vulnerabilidad**, tendrán una demanda creciente.

Tendencias de futuro en el mercado de la ciberseguridad

❑ Seguridad en movilidad y BYOD

- El uso de dispositivos móviles para acceder a los datos corporativos es una tendencia creciente entre los empleados, tanto si se trata de dispositivo de propiedad de las mismas empresas, como de sus empleados (fenómeno este último conocido como *bring your own device*, o BYOD). En particular, el BYOD introduce retos importantes a la hora de hacer frente a ciberataques y a la intrusión en sus redes a través de estos dispositivos.

Tendencias de futuro en el mercado de la ciberseguridad

❑ Seguridad en *smart grid / smart city*

- ❑ Las *smart grid*, o redes eléctricas inteligentes, permiten una transmisión y distribución de energía eléctrica más eficiente. Sin embargo, crecen las amenazas a la privacidad y a los datos personales de los usuarios.
- ❑ La ciberseguridad aplicadas a *smart grid* consiste en la protección de estas redes inteligentes frente a las amenazas cibernéticas. Los hackers, p. e, , pueden tomar el control de las aplicaciones y de los servidores y acceder a información confidencial. Las *smart grid* requieren medidas de seguridad no sólo para manejar los sistemas y equipos, sino también para asegurar el intercambio de información entre sistemas. **La ciberseguridad juega un papel importante**

Tendencias de futuro en el mercado de la ciberseguridad

❑ Ciberguerra y ciberdefensa

- ❑ Los ciberataques entre los Estados no sólo están aumentando en frecuencia, sino se están volviendo cada vez más sofisticados.
- ❑ Esta creciente amenaza ha calado en la opinión pública y los gobiernos están aumentando sus presupuestos para el desarrollo de capacidades cibernéticas tanto ofensivas (**ciberataque**) como defensivas (**ciberdefensa**). Según Visiongain, el gasto mundial en ciberguerra llegará en 2014 a los 22.900 millones de dólares.

INTERNET DE LAS COSAS (IoT)

INTERNET DE LAS COSAS (OBJETOS)

MACHINE TO MACHINE (M2M)

- Intercambio de información en formato de datos entre dos puntos remotos, bien a través de red fija o móvil sin interacción humana con características específicas en cuanto a tráfico y tarjetas SIM e integradas en la fabricación de dispositivos
- Automatización de los procesos de comunicación entre máquinas, entre dispositivos móviles (celulares) y máquinas (Mobile to Machine) y entre hombres y máquinas (Man to Machine)
- En 2011 había más de 1.500 millones de dispositivos alrededor del mundo conectados entre sí; 15.000 millones en 2013. Previsiones de Cisco, 25.000 millones para 2015

INTERNET DE LAS COSAS (OBJETOS)

- Cada día aumenta el número de dispositivos de todo tipo que proporcionan acceso a Internet. Las "cosas" que permiten y van a permitir estos accesos irá aumentando con el tiempo. **Ahora ya tenemos videoconsolas, automóviles, trenes, aviones, sensores, aparatos de televisión, … y pronto el acceso se realizará desde los electrodomésticos**

World Wide Web, Internet móvil, *cloud computing*, INTERNET DE LAS COSAS

- Un mundo en el que miles de millones de objetos informarán de su posición, identidad e historia a través de conexiones inalámbricas … mediante tecnologías RFID, *bluetooth*, sensores inalámbricos, NFC, …
  - La realización del "Internet de las cosas" , probablemente requerirá cambios dramáticos en sistemas, arquitecturas y comunicaciones,… Invisible es la descripción de las nuevas tecnologías empotradas **"Computación ubicua"…** A medida que avance su penetración:
- Producirá un CAMBIO SOCIAL, posiblemente, de tanto impacto y tan poco previsible, como las actuales tecnologías Web

VENTAJAS Y RIESGOS DE IoT

❑VENTAJAS Y OPORTUNIDADES

- ❑ **CISCO, ERICSSON,…** prevén que para el año 2020 habrá cerca de 50 mil millones de dispositivos conectados a Internet, capaces de comunicarse entre sí, desde automóviles, aparatos de consumo en el hogar, teléfonos inteligentes, marcapasos, televisores, carros (coches), ropa inteligente, electrodomésticos, puertas - ventanas de hogares y edificios, PCs, tabletas… **Infinitas ventajas**

❑RIESGOS*…

Hackers "maliciosos", ciberespionaje …

* *Cibereespionajes, piratas y mafias*, El País, febrero 2013

http://elpais.com/elpais/2013/02/19/eps/1361281322_025092.html

NORMALIZACIÓN DE LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

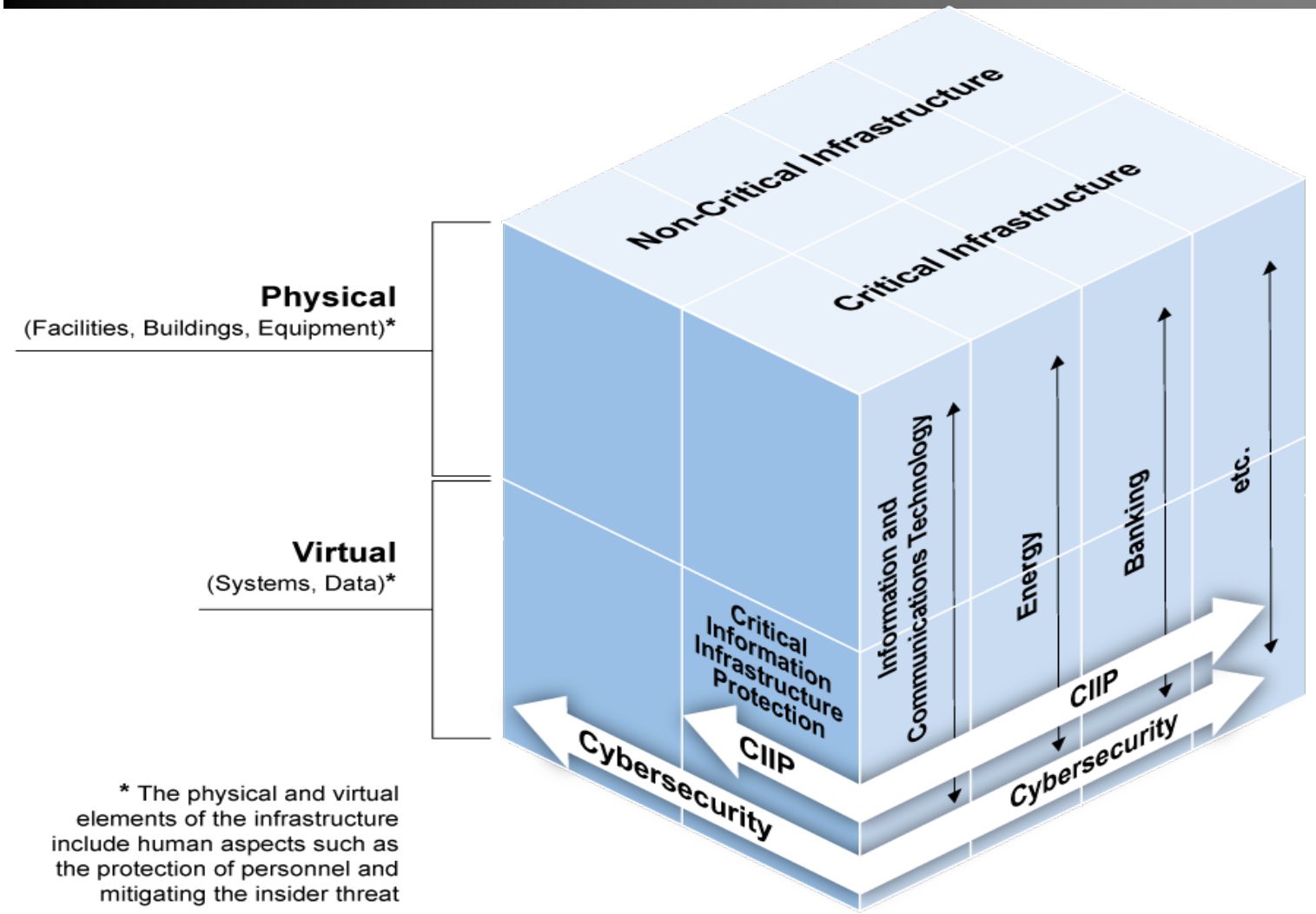
- **Normas ISO 27000:** Familia de estándares de ISO (*International Organization for Standardization*) e IEC (*International Electrotechnical Commission*) que proporciona un **marco para la gestión de la seguridad**
- **SO/IEC 27000: define el vocabulario estándar empleado en la familia 27000** ***(definición de términos y conceptos)***
- **ISO/IEC 27001: especifica los requisitos a cumplir para implantar un SGSI certificable conforme a las normas 27000**
- **Norma ISO/IEC 27032, nuevo estándar de ciberseguridad,** 17 oct 2012

Definición de CIBERSEGURIDAD, ITU

- ***Ciberseguridad*** se entiende, tal como se define en la Recomendación UIT-T X.1205:

- "**El conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno. Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los usuarios, los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedios, y la totalidad de la información transmitida y/o almacenada en el ciberentorno**."

Definición de CIBERSEGURIDAD, ITU



Normas de Ciberseguridad – IUT (UIT)

- Es importante entender la relación existente entre la ciberseguridad, la infraestructura esencial "crítica" (**CI, critical infrastructures**), la infraestructura de información esencial (**CII, critical information infrastructure**), la protección de la infraestructura de información esencial (**CIIP, critical information infrastructure protection**) y la infraestructura no esencial. Esta relación queda ilustrada en la Figura 1.

Normas de Ciberseguridad – IUT (UIT)

- El significado del término "**esencial" (crítica)** puede variar según sea el país considerado, pero normalmente incluye elementos de la tecnología de la información y la comunicación, incluyendo las telecomunicaciones, (**TIC**) y **los sectores de la energía, banca, transporte, salud pública, agricultura y alimentación, suministro de agua, industria química, industria naviera y servicios públicos esenciales.**
- Los países deben planificar y elaborar políticas que protejan lo consideren sus infraestructuras esenciales (en otras palabras, protección de la infraestructura esencial, incluida la protección física y virtual), para garantizar un nivel razonable de resistencia y seguridad de tales infraestructuras y así contribuir al logro de los objetivos y la estabilidad económica nacionales.

Normas de Ciberseguridad – IUT (UIT)

- Los ciberincidentes pueden incidir en infraestructuras de información esenciales y no esenciales y adoptar muchas formas de actividad maliciosa, por ejemplo, la utilización de redes robot para llevar a cabo ataques de denegación de servicio y difundir correo electrónico basura y soporte lógico perjudicial (virus, gusanos, etc.) que reduzcan la capacidad de funcionamiento de las redes. Además, los ciberincidentes pueden incluir actividades ilícitas tales como el **hurto de identidades** y credenciales financieras (***phishing: envios de correos-e… páginas web falsas***) y la clonación de servidores de nombres de dominio (***pharming: suplantar nombres de dominio-→ página web falsa***) así como el robo de identidad..

Normas de Ciberseguridad – IUT (UIT)

- Una de las funciones de un enfoque nacional respecto a la ciberseguridad es promover conciencia entre el público acerca de **la existencia del ciberriesgo**, así como crear estructuras para abordar la ciberseguridad y establecer las relaciones necesarias para afrontar los eventos que puedan producirse. Evaluar el riego, adoptar medidas de mitigación, y gestionar las consecuencias, son también elementos de un programa nacional de ciberseguridad.

- ***Un buen programa de ciberseguridad nacional*** contribuirá a proteger el funcionamiento normal de la economía de un país, a promover la continuidad de la planificación en todos los sectores, proteger la información almacenada en los sistemas de información, preservar la confianza pública, mantener la seguridad nacional y garantizar la salud y la seguridad públicas.

Ciberataques, ciberamenazas: Ciber-riesgos

Ciberamenazas destacadas 2014*

- * INTECO (Instituto de tecnologías de la comunicación, ESPAÑA). Listado elaborado con el objetivo de servir de base de información, noticias, sucesos, o cualquier evento importante en materia de ciberseguridad. (Octubre 2014)
- **Vulnerabilidad Heartbleed**: anunciado como "El mayor fallo de seguridad en Internet" se trató de una importante vulnerabilidad en las librerías OpenSSL. La gravedad de la vulnerabilidad está en la posibilidad de obtener información sensible de los sistemas afectados, permitiendo "romper" ese cifrado en las comunicaciones.

Ciberamenazas destacadas 2014*

- **2. *Celebgate,* robo masivo de imágenes de celebridades**: se trata del robo de fotografías de famosas desnudas y publicados en diversos foros de Internet, las cuales supuestamente fueron obtenidas a través del servicio de almacenamiento en la nube de Apple encargado de almacenar las copias de seguridad.
- **3. Robo de Información en el Banco Central Europeo**: según anuncio el BCE en una nota de prensa su página web *fue hackeada*, y se robó información de unos 20.000 usuarios.

Ciberamenazas destacadas 2014*

- **4. Amenaza avanzada o APT para sistemas de control industrial "dragonfly"**: Symantec: campaña de malware enfocado a Sistemas de Control Industrial utilizados en el sector energético en Europa, aunque también se ha detectado en el sector farmacéutico. Esta amenaza utilizaba un sistema de acceso remoto RAT para infectar y controlar remotamente los equipos afectados.
- **Machete, una ATP de habla hispana**: a través de la empresa de seguridad Kaspersky se conoce la existencia de esta amenaza, activa desde 2010. Se dirigía especialmente a servicios de inteligencia, militares y organizaciones gubernamentales de países latinoamericanos.

Ciberamenazas destacadas 2014*

- **6. Robo de información personal en Orange Francia**: un incidente de seguridad ha permitido el robo de datos personales de 1,3 millones de clientes del total de clientes en Francia. Entre los datos sustraídos se encontrarían nombre, apellidos, direcciones de correo electrónico, números de teléfonos móviles y fijos y fechas de nacimiento. No se robaron datos financieros o información de pago o tarjetas de crédito.

Ciberamenazas destacadas 2014*

- **7. Fin de Windows XP y Office 2003**: en abril finalizó el soporte para Windows XP SP3 y Office 2003, Desde entonces, Microsoft ha dejado de proporcionar para Windows XP actualizaciones de seguridad o parches para errores. Se estima que, a finales de marzo, Windows XP aún se utilizaba en el 30% de los ordenadores de escritorio.
- **8. Hackers rusos roban 1200 millones de credenciales**: se hace pública una fuga de información masiva de la que se responsabiliza a una organización criminal rusa llamada CyberVor. Hold Security estima que el robo contiene un total de 1.200 millones de credenciales son únicas

Ciberamenazas destacadas 2014*

- **9. FBI investiga múltiples ciberataques contra varios bancos americanos**: los hackers tuvieron acceso a docenas de servidores de JPMorgan en un periodo de dos meses. El ataque afectó a los datos de 76 millones de hogares y a 7 millones de pequeñas empresas.
- **10. Robo masivo de datos de tarjetas de crédito en Home Depot**: aproximadamente 56 millones de números de tarjetas de débito y de crédito de clientes de Home Depot, una de las principales empresas minoristas de bricolaje a nivel mundial. El robo se llevó a cabo entre abril y septiembre del 2014.

Ciberriesgos versus Ciberataques

Riesgos en el sitio Web

- **Ataques de "denegación de servicio (DoS, DDoS)** que tienen como objeto saturar el servidor en el que la web está alojada y dejarla inoperativa e inaccesible.
- **Intrusiones no permitidas en la administración de la web, para cambiar o eliminar alguna de la información que se muestra** (por ejemplo, cambiar fotos o textos por otros insultantes o sarcásticos)
- **Accesos no autorizados al servidor en el que se aloja la web,** para copiar o robar información nuestra o de nuestros clientes.

Riesgos en el sitio Web

- **Incumplimientos de términos de contrato por el proveedor de hosting** (caídas de la web, tiempo de descarga, etc.)
- **Inserción de virus en archivos descargables desde nuestra web**.
- **Webs falsas o que imitan la nuestra con nombres de dominios similares para confundir a nuestros clientes (pharming)**

Riesgos en comercio electrónico

- **Virus:** El e-mail es una de las dianas favoritas de muchos tipos de virus, que envían una copia de sí mismos a nuestra agenda de contactos sin que nosotros lo sepamos. Estos contactos reciben un correo desde nuestra dirección que les insta a entrar en una web determinada o a descargar un archivo.

- ***Phising:*** El robo de las contraseñas de acceso a nuestro correo puede tener la intención de suplantar nuestra identidad para llevar a nuestros clientes a una web que es aparentemente igual que la nuestra (incluso con una URL parecida, cambiando una sola letra) para que éstos dejen datos sensibles (numeración de cuentas bancarias o tarjetas, PIN de las mismas, etc…)

Riesgos en comercio electrónico

- **Spam:** Si se consiguen las claves de acceso, nuestro correo electrónico puede ser utilizado para el envío de "correos basura" a toda nuestra agenda de contactos
- **Incumplimiento de la Ley de Servicios de la Sociedad de la Información (LSSI)** que regula las condiciones de la venta de artículos por medios electrónicos.
- **Accesos no autorizados** (desde fuera del sistema o por empleados de la empresa) a los datos de clientes para su uso fraudulento, especialmente datos bancarios.
- **Pérdidas económicas por tarjetas o datos de terceros usados fraudulentamente para realizar compras en nuestro sistema**

Uso de aplicaciones de gestión y bases de datos en la nube:

- **Pérdida de información por negligencia o accidente del** proveedor del software y el alojamiento de los datos.
- **Accesos no autorizados a los sistemas del proveedor y robo o borrado de datos.**
- **Pérdidas económicas** por caída de sistemas o no disponibilidad de datos.
- **Robo de datos**, bien por los propios empleados o por accesos no autorizados.
- **Invasión de virus y pérdida o deterioro de datos.**
- **Espionaje industrial**

Riesgos en redes sociales

- **Reclamaciones judiciales** por difamación o daños al honor de terceros.
- **Coste de reclamaciones judiciales por daños a nuestro honor o difamación por parte de terceros.**
- **Publicidad engañosa**.
- **Pérdidas económicas derivadas de crisis de reputación *online*.**
- **Vulneración de derechos de propiedad in**telectual en la publicación de imágenes, vídeos o textos en las redes sociales, blog o web.

Protección de datos de carácter personal:

- **Negligencia en la custodia de datos o incumplimiento de medidas de protección contempladas en la LOPD**.
- Negligencia en la destrucción de datos o no destrucción de los mismos en el plazo legal establecido en cada caso.
- Responsabilidades económicas y/o penales derivadas de la difusión, intencionada o accidental, de datos de terceros de los que nosotros somos encargados de tratamiento o titulares de ficheros.

INFORME DE ENISA

INFORME DE ENISA SOBRE CIBERASEGURADAS

- **Enisa confía en el mercado de ciberaseguradores para concienciar a las empresas**
- Enisa ha publicado un informe en el que confirma que la Unión Europea confía en el fortalecimiento del mercado de ciberaseguradoras para concienciar a las empresas. En su informe, Enisa destaca la gran diferencia entre el mercado de EEUU y el europeo.
- Así lo pone de manifiesto un estudio publicado por la Agencia Europea para la Seguridad de las Redes y la Información (Enisa) y que critica la distancia que separa a este sector en Europa con respecto a Estados Unidos.

INFORME DE ENISA SOBRE CIBERASEGURADAS

- En relación con todo ello, la Unión Europea también está impulsando la colaboración entre los distintos países para garantizar la seguridad en el mundo TI. Así, la comisaria para la Agenda Digital de la UE, Noelie Kroes, apuesta por ***una estrategia de seguridad cibernética común*** para toda Europa y que permita afrontar con garantías los nuevos desafíos en esta materia.

  Aunque el fenómeno **BYOD** (*bring your own device*), o que los empleados de una compañía utilicen sus propios dispositivos para su uso empresarial, **conlleva muchos beneficios para las empresas, sobre todo en materia de productividad, también implica nuevos retos en materia de seguridad**

INFORME DE ENISA SOBRE CIBERASEGURADORAS

- No hay que perder de vista al ***cloud computing***, al posibilitar que los empleados se puedan conectar a los sistemas empresariales desde cualquier sitio con conexión a Internet. Entonces, ¿cuáles son los retos que se plantean? "Al utilizar dispositivos propios para acceder a redes corporativas, se usa un software que puede no ser el recomendado por la empresa. El comportamiento de estos usuarios puede escaparse del control del departamento de IT".
- "Las empresas de éxito están utilizando cada vez más la tecnología para incrementar las ventas, maximizar la eficiencia y reducir los gastos, pero algunas tecnologías emergentes como el **cloud computing** y las **redes sociales** elevan el riesgo de robos, fraudes y sabotajes cibernéticos"

NECESIDAD DE UN SEGURO DE CIBERRIESGOS

- Breves reflexiones sobre el seguro de ciberriesgos desde una perspectiva académico-tecnológica
- ¿Qué contempla un seguro de ciberriesgos?
- En general, los seguros de ciberriesgos, además de la responsabilidad civil ante terceros por el uso fraudulento de datos o los daños causados por virus enviados desde nuestro sistema, tienen una amplia cobertura de daños propios

NECESIDAD DE UN SEGURO DE CIBERRIESTOS

- Aunque depende de la compañía con la que se decida contratar, estas coberturas suelen estar disponibles:
- **Gastos de descontaminación, eliminación de virus del sistema y/o recuperación de datos perdidos por ataques de virus.**
- **Gastos de defensa legal**.
- **Informática forense:** Peritajes informáticos para procesos judiciales, recuperación de datos borrados intencionadamente.

NECESIDAD DE UN SEGURO DE CIBERRIESTOS

- **Gastos por sanciones en materia de protección de datos.**

- **Gastos por reclamaciones de terceros ante pérdidas de datos, usos fraudulentos o incapacidad de acceder a sus propios datos por inaccesibilidad del sistema.**

- **Incremento en costes de explotación y pérdidas de beneficios derivados de un incidente cibernético o una crisis de reputación *online***

Mercado de ciberseguros*

- "*El brazo de seguros de Marsh & McLennan Companies estima que el mercado de ciberseguros de Estados Unidos estaba valorado en 1.000 millones de dólares el año pasado en primas brutas y podría alcanzar hasta 2.000 millones de dólares este año. El mercado europeo es en la actualidad una fracción de esa cifra, de alrededor de 150 millones de dólares, pero está creciendo entre el 50 y el 100 por cien anualmente, según Marsh*."
- *Las aseguradoras tratan de actualizarse en el pujante mercado del ciberriesgo - ***elEconomista.es (14 julio 2014)***
  http://www.eleconomista.es/telecomunicaciones-tecnologia/noticias/5938615/07/14/Las-aseguradoras-tratan-de-actualizarse-en-el-pujante-mercado-del-ciberriesgo.html

DEMANDA DE PROFESIONALES DE CIBERSEGURIDAD

- En los próximos años contando el actual (2014-2020) la necesidad de expertos en ciberseguridad para las empresas. Universidad, Fuerzas Armadas, Cuerpos de Seguridad, Ministerios, Centros de Investigación, etc. crecerá de modo "exponencial".
- Se requiere a medio y largo plazo la concienciación en la educación (media y universitaria), las organizaciones y empresas, Defensa, Interior, etc... y la incorporación de asignaturas relacionadas con la ciberseguridad en los diferentes niveles.

DEMANDA DE PROFESIONALES DE CIBERSEGURIDAD

- Impartición de Master/Maestria en Ciberseguridad organizados por universidades, escuelas de negocio y empresas
- **Deloitte, S21Sec, Indra, INTECO**
- **U-Tad; U. Carlos III de Madrid, U. Autónoma de Madrid, etc.**
- **Máster en Ciberseguridad "*online*"** por la nueva escuela de negocios española **IETEN (www.ieten.es)** ***pensado y diseñado para España y Latinoamerica*** en ambientes de organizaciones y empresas, así como profesionales

CIBERRIESGOS

Estrategias nacionales de Ciberseguridad

Prof. Luis Joyanes Aguilar

ESTRATEGIAS NACIONALES DE CIBERSEGURIDAD

Países con estrategia nacional de ciberseguridad (verde) y en vías de desarrollo (amarillo). Fuente: Enisa 2014

ESTRATEGIAS NACIONALES DE CIBERSEGURIDAD

- Estados Unidos, la Unión Europea y España (además de numerosos otros países) han lanzado y publicado estrategias de Ciberseguridad.
- Estrategia de Ciberseguridad de la Unión Europea (2013)
- Estrategia de Ciberseguridad de la Unión Europea (2013)
- Así mismo han creado Organismos específicos para el aseguramiento de la Ciberseguridad a nivel nacional:

ESTRATEGIA NACIONAL DE CIBERSEGURIDAD DE ESPAÑA

- **La Estrategia de Ciberseguridad Nacional es el marco de referencia de un modelo integrado basado en la implicación, coordinación y armonización de todos los actores y recursos del Estado, en la colaboración público-privada, y en la participación de la ciudadanía**. Asimismo, dado el carácter transnacional de la ciberseguridad, la cooperación con la Unión Europea y con otros organismos de ámbito internacional o regional con competencias en la materia, forma parte esencial de este modelo.

MCCD (Mando Conjunto de Ciberdefensa)

Emblema del Mando Conjunto de Ciberdefensa (MCCD).

ORGANISMOS E INSTITUCIONES ESPAÑOLAS CON COMPETENCIAS EN CIBERSEGURIDAD

- **Centro Nacional de Inteligencia (CNI)** que tiene a su cargo la gestión de la seguridad del ciberespacio en las tres administraciones del Estado.
- El **CCN-CERT** es el Centro de alerta nacional que coopera con todas las administraciones públicas para responder a los incidentes de seguridad en el ciberespacio y vela también por la seguridad de la información nacional clasificada

ORGANISMOS E INSTITUCIONES ESPAÑOLAS CON COMPETENCIAS EN CIBERSEGURIDAD

- El Centro Nacional para la Protección de las Infraestructuras Críticas (**CNPIC**) que depende del Ministerio del Interior.
- El Instituto Nacional de Tecnologías de la Comunicación (**INTECO**) encargado de velar por la ciberseguridad de las PYMES y los ciudadanos en el ámbito doméstico.
- El Grupo de Delitos Telemáticos de la Guardia Civil y la Unidad de Investigación de la Delincuencia en Tecnologías de la Información de la Policía Nacional, responsables de combatir la ciberdelincuencia.
- **La Agencia Española de Protección de Datos**

Organismos de Seguridad en Empresas

- Las principales empresas españolas del sector de la seguridad informática crearon, el año 2009, **el Consejo Nacional Consultor sobre Ciber-Seguridad (CNCCS**) con el objetivo de fomentar la defensa del ciberespacio y colaborar con las entidades públicas y privadas. Este organismo respaldado por la iniciativa privada, facilita normativas, asesoramiento,... a las empresas y en particular a sus departamentos de Seguridad Informática.
- Entre los organismos internacionales europeos es de destacar la agencia europea **ENISA (European Network Information Security Agency)** cuya última iniciativa **Cyber Europe 2013 .**
-

LA CIBERSEGURIDAD "HOY-MAÑANA"

- **La ciberseguridad «debe entrar de inmediato en la agenda de todos: gobiernos, empresas y ciudadanos y hacerlo además con voluntad de permanencia».**

- Director del CNI de España en la presentación de los informes del Centro Criptológico Nacional.
- **NECESIDAD DE UN DEPARTAMENTO Y UN PLAN DE CIBERRIESGOS EN LA EMPRESA**

MUCHAS GRACIAS … ¿Preguntas?

Portal tecnológico y de conocimiento

www.mhe.es/joyanes

Portal GISSIC "El Ágora de Latinoamérica":

gissic.wordpress.com

Twitter:@luisjoyanes

Facebook: www.facebook.com/joyanesluis

www.slideshare.net/joyanes

www.slideshare.net/luismackoy

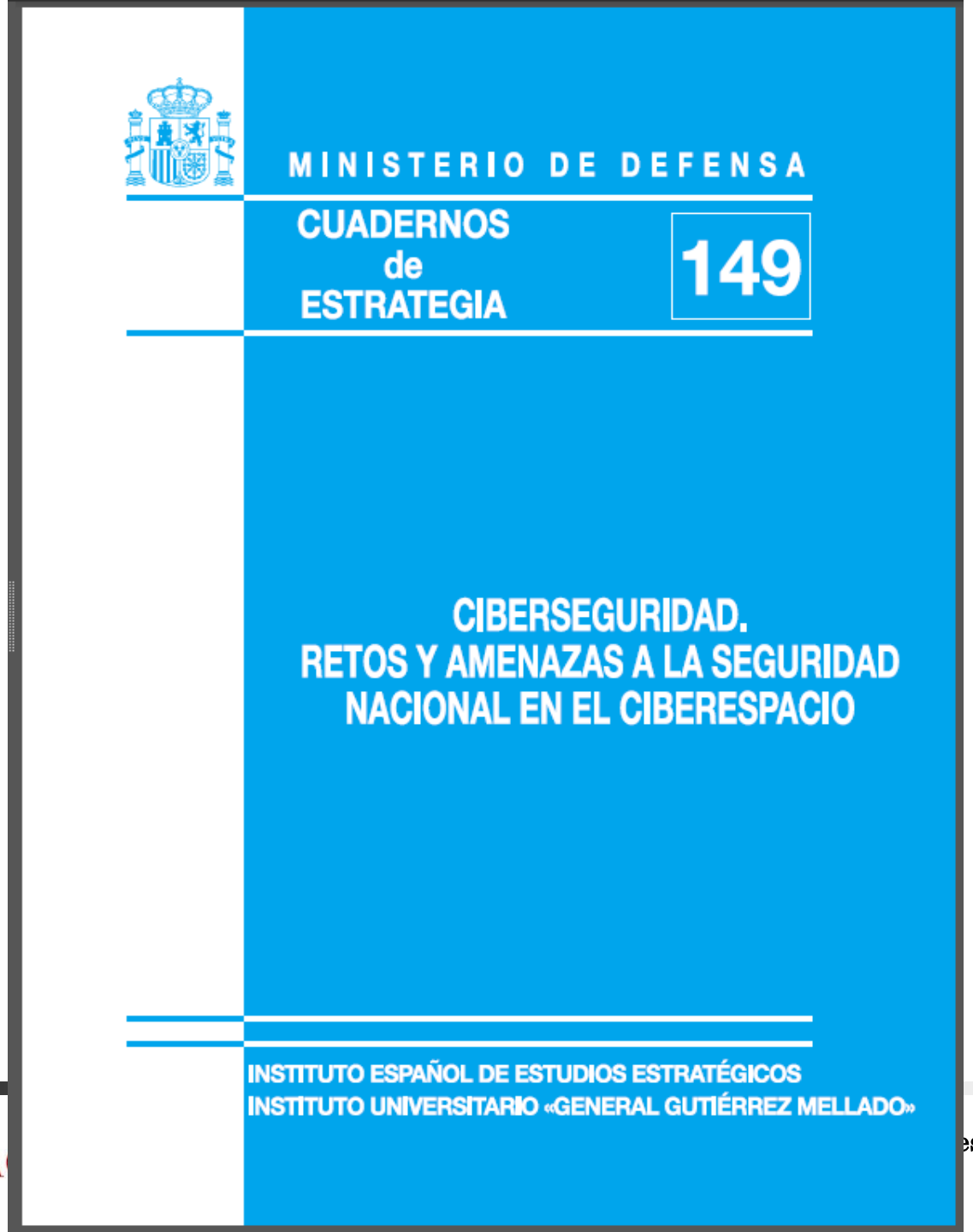
CORREO-e: joyanes@gmail.com

BIBLIOGRAFÍA

Prof. Luis Joyanes Aguilar

CIBERSECURITY FOR DUMMIES (free)

- PALO ALTO NETWORKS
- http://connect.paloaltonetworks.com/cybersecurity-dummies-es?utm_source=google-retargeting&utm_medium=retarget-banners&utm_term=&utm_campaign=FY14-es-displayrt-FWBG&utm_content=45529844191&custom2=5a377e036f7829bd.anonymous.google



JOYANES, Luis (Coordinador). *Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio.* Madrid: IEEE.es, 2011

Referencias CIBERSEGURIDAD

- *JOYANES, Luis. (ed. y coor.). Ciberseguridad. Retos y desafíos para la defensa nacional en el ciberespacio.* **Madrid: IEEE (Instituto Español de Estudios Estratégicos). 2011. Editor y Coordinador**

  www.ieee.org

  Cuadernos de estrategia, nº 149

http://www.ieee.es/documentos/areas-tematicas/retos-y-amenazas/2011/detalle/CE149.html

ESTADO DEL ARTE DE *CLOUD COMPUTING*

COMPUTACIÓN EN LA NUBE

La nueva era de la computación

Prof. Luis Joyanes Aguilar

Colección NTICS: Negocios, Tecnología, Innovación, Conocimiento y Sociedad

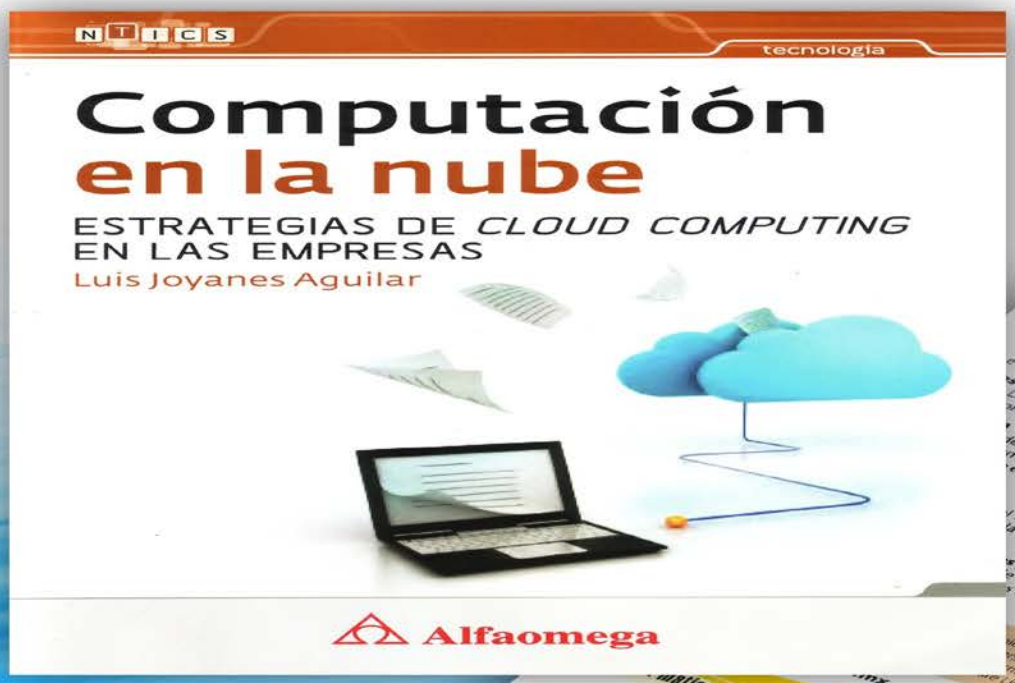
NUEVO LIBRO DE

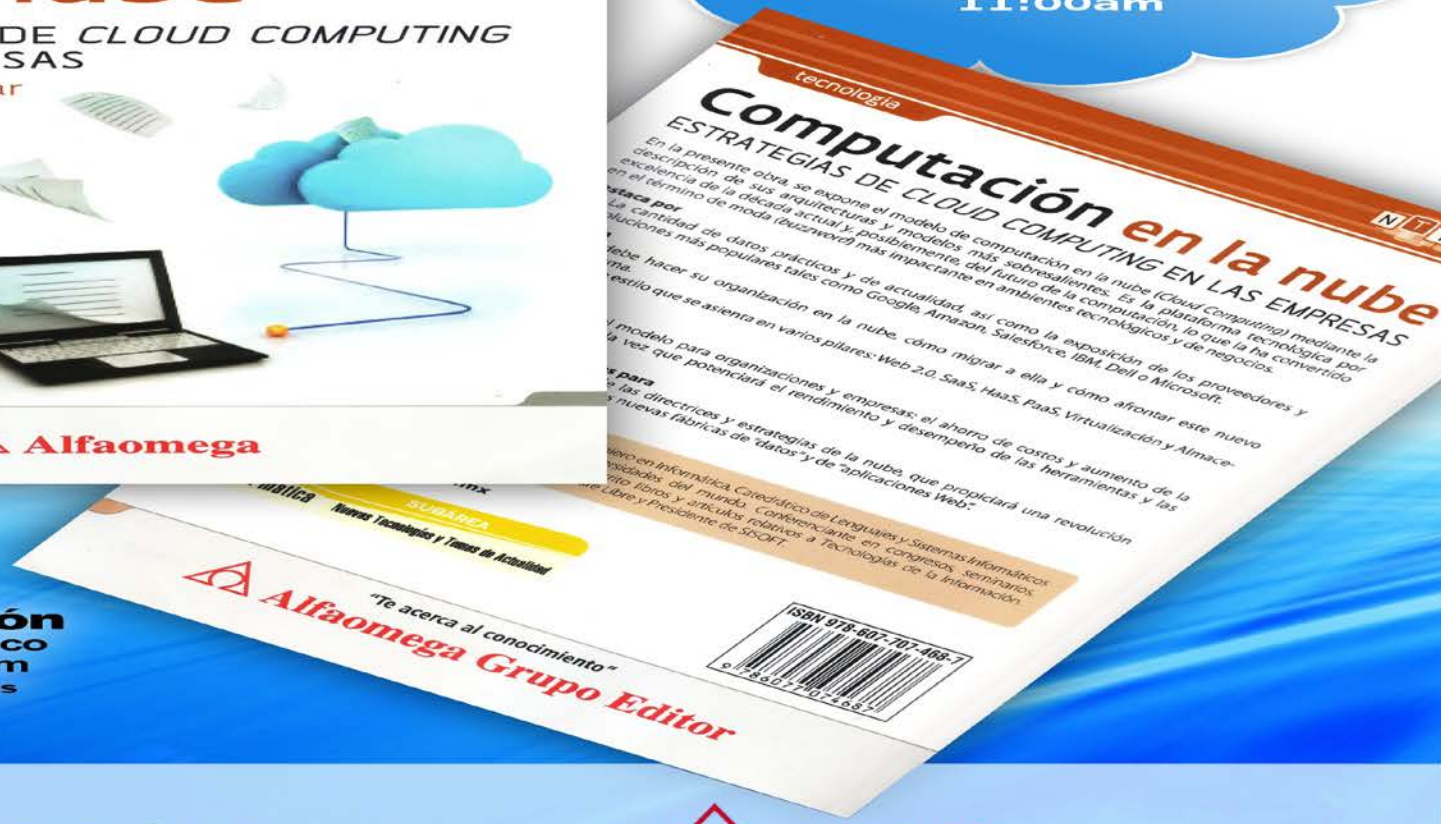
Luis Joyanes Aguilar

Presentación Exclusiva

ITESM CUERNAVACA

Día: 9 de noviembre 2012
11:00am





Más información
www.alfaomega.com.co
gissic.wordpress.com
Facebook.com/JoyanesLuis

INVITAN:

TECNOLÓGICO DE MONTERREY®

Alfaomega

LUIS JOYANES AGUILAR

Big Data

ANÁLISIS DE GRANDES VOLÚMENES DE DATOS EN ORGANIZACIONES

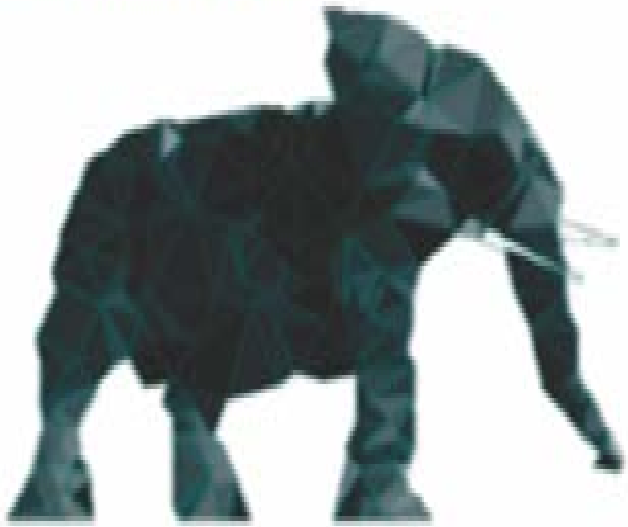
Luis Joyanes Aguilar

Alfaomega

Big Data

ANÁLISIS DE GRANDES VOLÚMENES DE DATOS EN ORGANIZACIONES

Luis Joyanes Aguilar



Alfaomega

Sistemas de Información

LUIS JOYANES AGUILAR

Contenidos Interactivos Web

libroWeb

Alfaomega

BIBLIOGRAFÍA BÁSICA

- JOYANES, Luis (2014). Computación en la nube. Estrategias de cloud computing en las empresas. Barcelona: Marcombo; México DF: Alfaometa
- JOYANES, Luis (2014). *Inteligencia de negocios. Un enfoque móvil, en la nube y de big data.* Barcelona: Marcombo; México DF: Alfaomega
- TURBAN, Efraim, SHARDA, Ramesh, DELEN, Dursun (2012).*Decision Support and Business Intelligence Systems.* Ninth edition. New Jersey: Pearson/Prentice-Hall
- JOYANES, Luis (2013). *Big Data. El análisis de los grandes volúmenes de datos*. Barcelona: Marcombo; México DF: Alfaomega.

ORGANISMOS E INSTITUCIONES ESPAÑOLAS CON COMPETENCIAS EN CIBERSEGURIDAD

- El Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica fue regulado en el Real Decreto 2/2010, de 8 de enero, pero cubre únicamente las administraciones públicas. Existen otras leyes nacionales, europeas e internacionales que abordan la seguridad, tales como: **Ley Orgánica de Protección de Datos (LOPD), la Ley General de las Telecomunicaciones (LOT) y la Ley de la Sociedad de la Información y Comercio Electrónico (LSI-CE).**
- * FOJÓN ENRIQUE Y SANZ ÁNGEL. "*Ciberseguridad en España: una propuesta para su gestión*", Análisis del Real Instituto Elcano, ARI nº 101/2010
-

INFORME DE ENISA SOBRE CIBERASEGURADORAS

- *Incentives and barriers of the cyber insurance market in Europe*
- **June 2012**

BIBLIOGRAFÍA

- **KOSUTIC**, Dejar. *Ciberseguridad en 9 pasos. El manual sobre seguridad de la información para el gerente,* 2012. EPPS Services, Zagreb.

  www.iso27001standard.com

  www.cci-es.org

- **ENISA.** The European Network and Information Security Agency. *Incentives and barriers of the cyber insurance market in Europe*. junio 2012. ¿Qué es cyber-insurance? ¿Porqué cyber-insurance?

- **CENTRO DE CIBERSEGURIDAD INDUSTRIAL**. *Mapa de ruta: Ciberseguridad Industrial en España 2013-2018*

BIBLIOGRAFÍA

- **NIST**. Framework for Improving Critical Infrastructure Cibersecurity. Febrero 2014.
- **CARO** Bejarano, Mª José. Estrategia de Ciberseguridad Nacional. Documento de Análisis. Instituto Español de Estudios Estratégicos. www.ieee.es.
- **ITU (UIT).** *Garantía de seguridad en las redes de información y comunicación: prácticas óptimas para el desarrollo de una cultura de ciberseguridad*
- **KRUTZ**, Ronald y **DEAN**, Rusell. *Cloud Security. A Comprehensive Guide to Secure Cloud Computing*. Wiley, 2010

BIBLIOGRAFÍA

- **CARR,** Jeffrey. *Cyber Warfare*. Sebastopol, USA: O´Reilly, 2010.
- **CLARKE,** Richard y KNAKE, Robert K. *Cyber War: The Next Threat to National Security and What to Do About It.* New York*:* Harper Collins, 2010.
- **CLARKE**, Richard A. Guerra en la Red. Los nuevos campos de batalla. Barcelona: Planeta, 2011.
- **FOJÓN** ENRIQUE Y **SANZ** ÁNGEL. "*Ciberseguridad en España: una propuesta para su gestión*", Análisis del Real Instituto Elcano, ARI Nº 101/2010

BIBLIOGRAFÍA

- LIBICKI, Martin C. *Cyberdeterrence and Cyberwar.* Santa Mónica: RAND Corporation, 2009.
- LYNS III, William J, *Foreign Affairs*, vol. 89, nº 5, septiembre/octubre de 2010, pp. 97
- **PANDA. Glosario de Seguridad de la Información:** http://www.pandasecurity.com/spain/homeusers/security-info/glossary/
- **VERISIGN (Infografía de ciberseguridad)** http://www.verisigninc.com/es_ES/why-verisign/innovation-initiatives/cyber-security/index.xhtml
- **HISPAVISTA Antivirus** http://hoax.antivirus.hispavista.com/glosario

REFERENCIAS

- **INTECO.** www.inteco.es
- **AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS.** www.aepd.es
- **ENISA** (Agencia Europea de Seguridad)
- **ITU** (Unión Internacional de Telecomunicaciones). https://www.itu.int/

  https://www.itu.int/es/Pages/default.aspx
- **CISCO 2014** Anual Security Report

  https://www.cisco.com/web/offers/lp/2014-annual-security-report/index.html?.keycode=000350063

INFORME DE ENISA SOBRE CIBERASEGURADORAS

- *Incentives and barriers of the cyber insurance market in Europe*
- **June 2012**

HP ha publicado el Informe de Ciber Riesgos 2013 (Marzo de 2014)

- HP ha publicado el Informe de Ciber Riesgos 2013, que **identifica las principales vulnerabilidades de la seguridad empresarial y proporciona un análisis del creciente panorama de amenazas**
- El informe de este año detalla los factores que más contribuyeron al incremento de los ataques en 2013, tales como **el aumento de la confianza hacia los dispositivos móviles, la proliferación de software inseguro o el uso creciente de Java**. Además, esboza una serie de recomendaciones para las organizaciones con el objetivo de minimizar los riesgos de seguridad y el impacto global de los ataques.

INFORME DE CIBERSEGURIDAD, 4 MAYO DE 2014, *El País,* Madrid

- **El Centro Europeo contra los Ciberdelitos, (EC3),** dependiente de **Europol, y la Comisión Europea (CE)** consideran que la nube informática es uno de los principales retos a los que habrá que hacer frente contra los delitos en internet.
- "**Los servicios en nube tiene muchos beneficios para consumidores y empresas, pero también permiten a muchos criminales almacenar material en internet en lugar de en sus propios ordenadores, lo que hace cada vez más difícil su localización**", Comisaria europea de Interior, Cecilia Malmström (febrero 2014).

APLICACIONES DE IMPACTO DEL IoT*

- **SHODAN, buscador en la Internet de las cosas* (http://www.shodanhq.com/)**
- **A Google for Hackers. Shodan es una nueva herramienta utilizada por "los chicos buenos y malos" para encontrar todos los dispositivos conectados "ahora" a la Internet: luces de tráficos, plantas de energía e incluso el monitor de su bebé"**
- ***** *Forbes*, sección *Technology*. **23 de septiembre, 2013 (nº de esa semana en España)**

BUSCADOR SHODAN DE LA IoT

CONFERENCIA EN SLIDESHARE.NET

- http://www.slideshare.net/joyanes/conferencia-bigdata-uem

GLOSARIO DE TÉRMINOS DE CIBERSEGURIDAD

- **PANDA Security**. Glosario de términos de seguridad.

http://www.pandasecurity.com/spain/homeusers/security-info/glossary/

Guía de ciberseguridad para los países en desarrollo. ITU 2007.

www.itu.int/ITU-D/cyb/publications/2007/cgdc-2007-s.pdf

INTECO. Tipos de herramientas avanzadas para garantizar la ciberseguridad en la empresa.

http://www.inteco.es/blogs/post/Seguridad/BlogSeguridad/Articulo_y_comentarios/herramientas_avanzadas_ciberseguridad_empresa?origen=dHOME

GLOSARIO DE CIBERSEGURIDAD

- **Malware.** Programa informático malicioso que tiene como objetivo infiltrarse y destruir otro sistema sin el permiso del propietario. La mayoría toma la forma de virus, gusanos, troyanos (apariencia inofensiva) y otros mecanismos como el "*spyware*" (programas espía) o el "*scareware*" (mensajes de alerta que pretenden infundir miedo en el usuario)

GLOSARIO DE CIBERSEGURIDAD

- **Centro Cristológico Nacional (CCN).** Organismo publico español adscrito al Centro Nacional de Inteligencia (CNI) encargado de velar por la seguridad de los sistemas informáticos del Estado mediante el análisis de códigos.

GLOSARIO DE CIBERSEGURIDAD

- **Spamhaus.** Organización fundada en 1998 y radicada en Londres y Ginebra cuyo objetivo es detectar y perseguir los ataques realizados mediante ´spam´ (correo electrónico que puede contener virus informáticos)
- **Caso *Heartbleed.*** Fallo masivo de seguridad surgido en diciembre de 2011 y descubierto el pasado abril que permitia el acceso a las claves personales de cualquier usuario en paginas como Facebook, Yahoo, google, la plataforma de pago PayPal, etc....

GLOSARIO DE CIBERSEGURIDAD

- **Data Loss Prevention (DLP).** Sistema ideado para prevenir el robo de datos informáticos y la entrada de cualquier “malware”
- ***Hacker.*** Usuario que entra de forma no autorizada en un computador o un sistema conectado de computadores, generalmente con fines delictivos. Algunos especialistas matizan que existen “hackers” benignos que utilizan sus técnicas de forma constructivas. A estos se les conoce como “hacker” de sombrero blanco.

GLOSARIO DE CIBERSEGURIDAD

- **Open SSL**. Sistema abierto de software en el que los usuarios comparten códigos informáticos. **Fue el sistema que sufrió el error que dio lugar al caso ‘ Heartbleed’**
- **Ley CISPA.** La Cyber Intelligence Sharing and Protection Act (CISPA) es un proyecto legislativo de EE UU, pendiente de su aprobación en el Senado que permite que el Gobierno comparta información con un determinado grupo de empresas (Microsoft, Intel, Boeing, Symantec y otras(con el objetivo de combatir la ciberdelincuencia. Sometida a muchas criticas, por la posibilidad que ven los detractores de espiar indiscriminadamente.

Definición de términos (PANDA)

- **DoS / Denegación de servicios:** Es un ataque, causado en ocasiones por los virus, que evita al usuario la utilización de ciertos servicios (del sistema operativo, de servidores Web, etc).
- **DdoS / Denegación de servicios distribuida:** Es un ataque de Denegación de servicios (DoS) realizado al mismo tiempo desde varios ordenadores, contra un servidor. Ataques destinados a impedir que un usuario acceda a su sistema. El 27 de marzo de 2013 se produjo un ataque masivo de este tipo que afectó a toda Europa. Junto conl os APT son uno de los ciberataques más comunes.

GLOSARIO DE CIBERSEGURIDAD

- **Pharming.** Es la explotación de una vulnerabilidad en el software de los servidores DNS (*Domain Name System*) o en el de los equipos de los propios usuarios, que permite a un atacante redirigir un nombre de dominio (*domain name*) a otra máquina distinta. De esta forma, un usuario que introduzca un determinado nombre de dominio que haya sido redirigido, accederá en su explorador de internet a la página web que el atacante haya especificado para ese nombre de dominio.

GLOSARIO DE CIBERSEGURIDAD

- ***Phishing:*** El phishing consiste en el envío masivo de mensajes que, aparentando provenir de fuentes fiables, intentan conseguir que el usuario proporcione datos confidenciales. El caso más típico de *phishing* es el envío de correos electrónicos que se hacen pasar por procedentes de una entidad bancaria online, para conseguir que el usuario introduzca sus contraseñas en una página web falseada.

ORGANISMOS DE CIBERSEGURIDAD EN ESPAÑA

- Consejo de Ciberseguridad Nacional
- Centro Nacional para la protección de infraestructuras críticas (CNPIC)
- INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN (INTECO)
- Departamento de Seguridad Nacional (DNS)
- El Mando Conjunto de Ciberdefensa (MCC)

Ciberataques, ciberamenazas: Ciber-riesgos

Ciberamenazas destacadas 2014*

- * INTECO (Instituto de tecnologías de la comunicación, ESPAÑA). Listado elaborado con el objetivo de servir de base de información, noticias, sucesos, o cualquier evento importante en materia de ciberseguridad. (Octubre 2014)
- **Vulnerabilidad Heartbleed**: anunciado como "El mayor fallo de seguridad en Internet" se trató de una importante vulnerabilidad en las librerías OpenSSL. La gravedad de la vulnerabilidad está en la posibilidad de obtener información sensible de los sistemas afectados, permitiendo "romper" ese cifrado en las comunicaciones.

Ciberamenazas destacadas 2014*

- **2. Celebgate, robo masivo de imágenes de celebridades**: se trata del robo de fotografías de famosas desnudas y publicados en diversos foros de Internet, las cuales supuestamente fueron obtenidas a través del servicio de almacenamiento en la nube de Apple encargado de almacenar las copias de seguridad.
- **3. Robo de Información en el Banco Central Europeo**: según anuncio el BCE en una nota de prensa su página web *fue hackeada*, y se robó información de unos 20.000 usuarios.

Ciberamenazas destacadas 2014*

- **4. Amenaza avanzada o APT para sistemas de control industrial "*dragonfly*"**: Symantec: campaña de malware enfocado a Sistemas de Control Industrial utilizados en el sector energético en Europa, aunque también se ha detectado en el sector farmacéutico. Esta amenaza utilizaba un sistema de acceso remoto RAT para infectar y controlar remotamente los equipos afectados.
- **Machete, una ATP de habla hispana**: a través de la empresa de seguridad Kaspersky se conoce la existencia de esta amenaza, activa desde 2010. Se dirigía especialmente a servicios de inteligencia, militares y organizaciones gubernamentales de países latinoamericanos.

Ciberamenazas destacadas 2014*

- **6. Robo de información personal en Orange Francia**: un incidente de seguridad ha permitido el robo de datos personales de 1,3 millones de clientes del total de clientes en Francia. Entre los datos sustraídos se encontrarían nombre, apellidos, direcciones de correo electrónico, números de teléfonos móviles y fijos y fechas de nacimiento. No se robaron datos financieros o información de pago o tarjetas de crédito.

Ciberamenazas destacadas 2014*

- **Fin de Windowa XP y Office 2003**: en abril finalizó el soporte para Windows XP SP3 y Office 2003, Desde entonces, Microsoft ha dejado de proporcionar para Windows XP actualizaciones de seguridad o parches para errores. Se estima que, a finales de marzo, Windows XP aún se utilizaba en el 30% de los ordenadores de escritorio.
- **Hackers rusos roban 1200 millones de credenciales**: se hace pública una fuga de información masiva de la que se responsabiliza a una organización criminal rusa llamada CyberVor. Hold Security estima que el robo contiene un total de 1.200 millones de credenciales son únicas

Ciberamenazas destacadas 2014*

- **9. FBI investiga múltiples ciberataques contra varios bancos americanos**: los hackers tuvieron acceso a docenas de servidores de JPMorgan en un periodo de dos meses. El ataque afectó a los datos de 76 millones de hogares y a 7 millones de pequeñas empresas.
- **10. Robo masivo de datos de tarjetas de crédito en Home Depot**: aproximadamente 56 millones de números de tarjetas de débito y de crédito de clientes de Home Depot, una de las principales empresas minoristas de bricolaje a nivel mundial. El robo se llevó a cabo entre abril y septiembre del 2014.