



**Escuela Universitaria de
Informática**



**Escuela Universitaria de Ingeniería
Técnica de Telecomunicación**

Universidad Politécnica de Madrid

Temas Avanzados en Seguridad y Sociedad de la Información

**IX Ciclo de Conferencias
UPM - TASSI**

Curso 2012 - 2013

Del disco flexible a la nube: pasado, presente y futuro de la Informática Forense



Javier Pagès López
CEO de Informática Forense, S.L.
Colegiado Nº 198 del CPIICM
Colegio Profesional de Ingenieros en Informática
de la Comunidad de Madrid



Email: javier.pages@informatica-forense.es

Web: <http://www.informatica-forense.es>

Sobre el autor...



Javier Pagès López



- **CEO de Informática Forense, S.L.**
- **Licenciado en Informática (Univ. de Valladolid, 1991)**
- **Experto Universitario en Desarrollo de Sistemas para el Comercio Electrónico (Univ. Salamanca, 2010)**
- **Auditor jefe ISO/IEC 27001:2005 (BSI, 2010)**
- **Colegiado Nº 110 del CPIICYL**
- **Colegiado Nº 198 del CPIICM**

Áreas de Actuación Profesional



- **Informática Forense**
- **Dictámenes Periciales: Judiciales, Extrajudiciales y Arbitrales**
- **Seguridad Informática Gestionada**
- **Auditoría Informática: LOPD, LSSI, Seguridad, ISO-27001...**
- **Intervenciones contra piratería informática**
- **Actuaciones contra delitos informáticos**
- **Consultoría: B2B, e-commerce, Enterprise Integration, CRM, ERP...**
- **Análisis de Mercado, Estudios de Viabilidad**
- **SOC – Security Operation Center**
- **Laboratorio de Vulnerabilidades IC - SCADA**

Pertenezco a:

	<p>CPIICYL - Colegio Profesional de Ingenieros en Informática de Castilla y León</p> <ul style="list-style-type: none"> •Miembro del Cuerpo de Peritos •Colegiado nº 110
	<p>AI²- Federación de Asociaciones de Ingenieros en Informática</p> <ul style="list-style-type: none"> •Presidente Federal <p>www.ai2.es</p>
	<p>AI²- Madrid - Asociación de Ingenieros en Informática de Madrid</p> <ul style="list-style-type: none"> •Vocal de Relaciones Institucionales •Socio nº 15 <p>www.ai2madrid.org</p>
	<p>INFOPERITOS (Gabinete Técnico y Facultativo de AI²)</p> <ul style="list-style-type: none"> •Perito de Guardia <p>www.infoperitos.com</p>

Pertenezco a:

 <p>International Organization for Standardization</p>	<p>Lead Auditor ISO/IEC 27001:2005, por la British Standards Institution</p> <p>www.bsigroup.com</p> 
 <p>Information Systems Security Association The Global Voice of the Information Security Profession</p>	<p>Information Systems Security Association (ISSA)</p> <ul style="list-style-type: none"> •ISSA Member ID: 26.563 <p>www.issa.org</p>
 <p>Information Systems Security Association The Global Voice of the Information Security Profession</p>	<p>Asociación Española para la Seguridad de los Sistemas de Información (ISSA-España)</p> <ul style="list-style-type: none"> •Presidente-Fundador del Capítulo Español de ISSA •Actual Secretario del Capítulo <p>www.issa-spain.org</p>
	<p>Internet Society (ISOC)</p> <ul style="list-style-type: none"> •ISOC Member ID: 1.350.480 <p>www.isoc.org</p>
 <p>Commercenet MEMBERS</p>	<p>Commercenet Español</p> <p>www.commercenet.org</p>

Algunas referencias profesionales:



Definiciones: Informática Forense

informática.

(Del fr. *informatique*).

1. f. Conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de ordenadores.

informático, ca.

1. adj. Perteneciente o relativo a la informática.
2. adj. Que trabaja o investiga en informática.
Apl. a pers., u. t. c. s.

Real Academia Española © Todos los derechos reservados

forense¹.

(Del lat. *forensis*).

1. adj. Perteneciente o relativo al foro.
2. adj. ant. Público y manifiesto.
3. com. médico forense.

□ V.

medicatura forense

forense².

(Del lat. *foras*, fuera).

1. adj. p. us. forastero.

Real Academia Española © Todos los derechos reservados

Fuente: <http://buscon.rae.es/draeI/>



Informática Forense: Definición y Objetivo

- La Informática Forense es una disciplina *criminalística* que tiene como objeto la **investigación** en sistemas **informáticos** de hechos **con relevancia jurídica** o para la simple investigación privada.
- Para conseguir sus objetivos, la Informática Forense desarrolla técnicas idóneas para ubicar, reproducir y analizar **evidencias digitales** con **fines legales**.



Informática Forense: Ámbito de actuación

Todo hecho en el que un sistema informático esté involucrado, tanto si es el **fin** o un **medio**, puede ser objeto de estudio y análisis, y por ello, puede llevarse a juicio como medio probatorio.



Informática Forense: Principios

- Adherirse a estándares legales
- Formación específica en técnicas forenses
- Investigación debe ser “*Forensically sound*”
- Obtener Permisos:
 - investigación/ recolección evidencias
 - monitorizar uso de ordenadores
- Control de Evidencias Digitales
 - **Cadena de Custodia**



Informática Forense: Normas Fundamentales

1. **Preservar** la evidencia original
 2. Establecer y mantener la **Cadena de Custodia**
 3. **Documentar** todo hecho
 4. **NO EXTRALIMITARSE**
 - ◆ Conocimientos personales
 - ◆ Leyes, Normas , Procedimientos
- **Riesgos:**
 - Corromper evidencias → **No admitirse en juicio**



Informática Forense: Objetivos del Proceso

- **Identificar** las posibles fuentes disponibles
- **Recoger** diferentes tipos de evidencias
- **Analizar** las evidencias encontradas
- **Confirmar** por pruebas cruzadas
 - Así se establecen las bases para **Probar** que se han cometido actos deshonestos o ilegales

Informática Forense:

Principio de Intercambio de Locard

Edmond Locard (Francia, 1877-1966). Pionero de la criminalística.

"Cada contacto deja un rastro"

- Siempre que dos objetos entran en contacto transfieren parte del material que incorporan al otro objeto
- En el momento en que un criminal cruza una escena del crimen, o entra en contacto con una víctima, la víctima se queda con algo del criminal, pero este a su vez se lleva algo a cambio.

Informática Forense:

Principio de Intercambio de Locard

- El *Principio de Locard* tiene plena validez en el ámbito informático y las evidencias electrónicas
- Hay que determinar el ¿Cómo? el ¿Dónde? podemos encontrar las evidencias
 - Determinar que quien escribió un “.doc”, o quién envió un email, es quien está acusado de ello.

Informática Forense: Breve Historia



Agosto 1986.- Caso Iran-Contras

- Tte. Coronel [Oliver North](#) escribió unos correos electrónicos que le involucraban en el caso
- Borro los correos de su ordenador
- No se percató que se hacían copias de respaldo de sus mensajes
- Los mensajes se recuperaron de los servidores de respaldo

→ **CULPABLE**

Informática Forense: Breve Historia



1991.- Caso Guttman

- La esposa de Guttman apareció muerta con una nota de suicidio sin firmar, escrita por ordenador con una impresora matricial
- El ordenador de Guttman **NO** contenía rastros del documento
- Guttman tenía una amante.
- Se registró la casa de la amante.
- Encontraron un disco flexible de 5 ¼ cortado en pedazos
- Se reconstruyó físicamente el disco y se recuperaron los datos con un programa llamado Anadisk

→ **CULPABLE**

Informática Forense:

Breve Historia

1995.- Caso MITNICK

- [Kevin Mitnick](#) fue detenido en 1995 después de tres años de persecuciones por parte del FBI
- Ya se le había procesado en 1981, 1983 y 1987 por [diversos delitos electrónicos](#)
- Se le acusó de haber entrado en algunos de los ordenadores más seguros de EE.UU.
- Se le pudo atrapar gracias a la participación de un experto académico en seguridad
- Se le condenó a no hacer llamadas telefónicas durante su encarcelamiento → **CULPABLE**
- Fue puesto en libertad en 2002
- La comunidad *hacker* le considera un **¿HÉROE?**

Informática Forense:

El criterio de *Daubert*

Daubert Criteria o ***Daubert Standard*** (1993) es el método que se sigue en los EEUU para admitir que una evidencia científica es no sólo **pertinente** (*relevant*) para el caso, sino que también es **fiable** (*reliable*)

- Se usa conjuntamente con la [Regla 702 de Evidencias Federales](#), Testimony by Experts:
 - “If scientific, technical, or other specialized knowledge will assist the trier of fact to understand the evidence or to determine a fact in issue, a witness qualified as an expert by knowledge, skill, experience, training, or education, may testify thereto in the form of an opinion or otherwise, if (1) the testimony is based upon sufficient facts or data, (2) the testimony is the product of reliable principles and methods, and (3) the witness has applied the principles and methods reliably to the facts of the case.”

Informática Forense: El criterio de *Daubert*

Se basa en cuatro factores utilizados para evaluar las evidencias científicas:

1. Pruebas realizadas
2. Revisiones cruzadas (*peer review*)
3. Tasa de error (*error rate*) de las pruebas
4. Aceptación por la comunidad científica

Informática Forense: El criterio de *Daubert*

- Ejemplo: HASH MD5 / SHA1
 - Pruebas realizadas → **FUNCIONA**
 - Revisiones cruzadas (*peer review*) → **COLISIONES**
 - Tasa de error (*error rate*) de las pruebas → **AD-HOC**
 - Aceptación por la comunidad científica → **OBSOLETOS**
→ **Reemplazar por SHA2, AES**



→ **cryptographic hash project**



Evidencias Digitales: ¿Qué son?

- Cualquier documento, fichero, registro, dato, etc. contenido en un soporte informático
- Susceptible de tratamiento digital
- Ejemplos:
 - Documentos de Ofimática (Word, Excell, ...)
 - Comunicaciones digitales: E-mails, SMSs, Fax, ...
 - Imágenes digitales (fotos, videos...)
 - Bases de Datos
 - Ficheros de Registro de Actividad → LOGS

Evidencias Digitales: Su Validez Jurídica

- Uno de los pilares más importantes de la informática forense
 - Valor que se le puede dar a las evidencias informáticas (*e-evidences*)
 - Para aportar en los procesos judiciales.
- Actualmente existen grandes debates entre juristas y expertos técnicos
 - a nivel nacional -> Foro de la Evidencias Electrónicas (www.evidenciaselectronicas.org)
 - a nivel internacional

Objetivo:

- Alcanzar un compromiso a nivel internacional
- Definir que hay que exigir a una evidencia informática para que se pueda aceptar como una prueba



Evidencias Digitales: Su Validez Jurídica

- Este extremo cada día cobra mayor importancia, dado que cada día hay más leyes y normativas que regulan las actividades relacionadas con la informática y el uso (o mal uso) que se haga de ella:
 - Leyes nacionales:
 - **Código Penal**
 - reforma DIC-2010 para penalizar el mal uso informático
 - responsabilidad de empresas
 - **LOPD, LSSI-CE**
 - **Ley de Firma Electrónica, DNI-e, eFactura...**
 - **Ley de Conservación de Datos**
 - **Ley Administración Electrónica**
 - Leyes europeas:
 - *“Data Retention Directive”* (Directiva 2006/24/EC)
 - *Documento Marco 2005/222/JAI* del Consejo de Europa, relativo a los ataques contra los sistemas informáticos
 - Leyes Inglesas:
 - *“Anti-Terrorism, Crime and Security Act 2001”*
 - *“Prevention of Terrorist Act 2005”*
 - Leyes norteamericanas:
 - **SOX** (*Sarbanex-Oxley Act 2002*)
 - **HIPAA** (*Health Insurance Portability and Accountability Act*)
 - ...

Nueva Legislación Informática (2010)



- **Esquema Nacional de Seguridad** (Ene. 2010)
 - R.D. 3/2010, de 8 de enero
 - Todas las AA.PP. tienen que implantar medidas de seguridad en sus sistemas informáticos
 - Prepararse para combatir los CIBERATAQUES (Ej. Canada o Francia en 2011)
 - Reducir las fugas y robos de información (Ej, WikiLeaks)

Nueva Legislación Informática (2010)

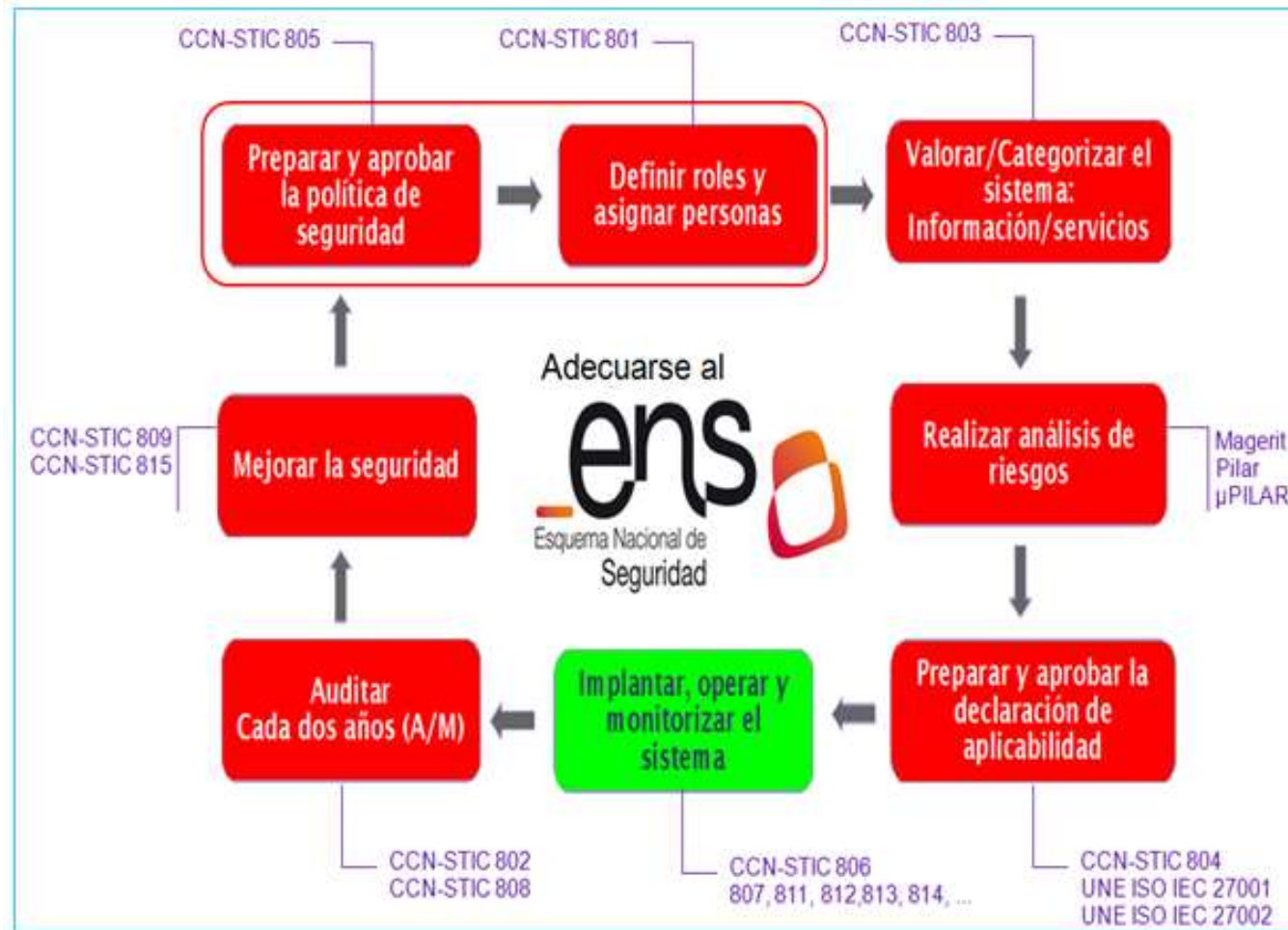
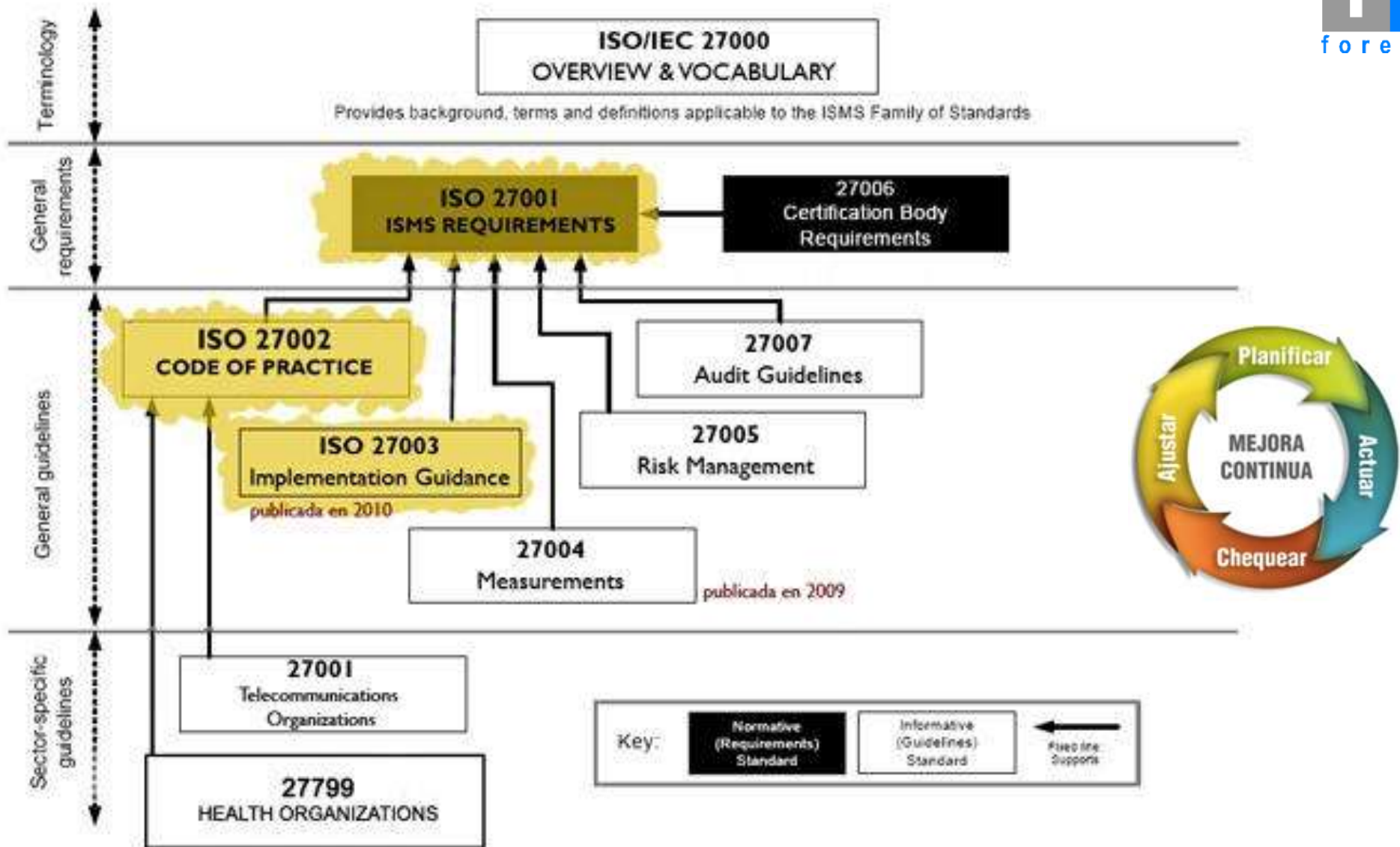


Figura: Adecuación al Esquema Nacional de Seguridad.



Relaciones entre la familia de normas 27000- SGSI

Nueva Legislación Informática (2010)

- **Reforma Código Penal** (Dic. 2010)
 - Más delitos informáticos (ej, DoS, intrusiones...)
 - Responsabilidad PENAL de las EMPRESAS
 - Por delitos cometidos por sus empleados desde la empresa
 - Por no implantar medidas de seguridad en sus sistemas informáticos
 - Por incumplir la Ley (ej, LOPD)

Evidencias Digitales:

Preservar información de uso

- Muchas de estas leyes obligan a las empresas a conservar una serie de datos relacionados con el uso que se hace de la información contenida en los sistemas informáticos.
- Información que se almacena actualmente en:
 - *logs de actividad* de los sistemas informáticos
 - *logs de actividad* de aplicaciones informáticas
 - que se ejecutan en:
 - cada servidor
 - en cada ordenador personal.



Evidencias Digitales: Validez de los Logs

Pregunta:

“¿Que valor probatorio tiene un log de ordenador?”

Respuestas:

- *“Ningún valor. Se puede alterar muy fácilmente”*
- *“Valor Total. Aquí lo tengo impreso, y dice lo que está escrito”.*



Evidencias Digitales: Validez de los Logs

Mi opinión:

- un log, o un correo electrónico o cualquier otra evidencia informática:
 - Tiene el valor que le quieran dar las partes
 - Si ninguna lo pone en duda, su valor será total
 - Pero si alguno duda de su autenticidad habrá que esforzarse (y mucho) para darle valor probatorio
- Esta ambigüedad en el valor de las pruebas informáticas
 - es muy interesante y da mucho juego desde el punto de vista pericial
 - provoca una gran incertidumbre a nivel jurídico.
- Estamos en el *Génesis de la Informática Forense*, en sus inicios.



Evidencias Digitales: Validez de los Logs

Soluciones actuales:

- Proyecto “*Integridad y Seguridad de la Historia Clínica*” (2008)
 - Plan Avanza I+D 2008 (TSI-020302-2008-67)
 - KINAMIC + Informática Forense + Hospital de Fuenlabrada
 - Serialización del log con kNotary
 - Asegurar el 100% de las Historias Clínicas del 1er Hospital “sin papeles” de Europa





Evidencias Digitales: Validez de los Logs

Soluciones actuales:

Servicio de Depósito y Custodia de Soportes Informáticos (2010)

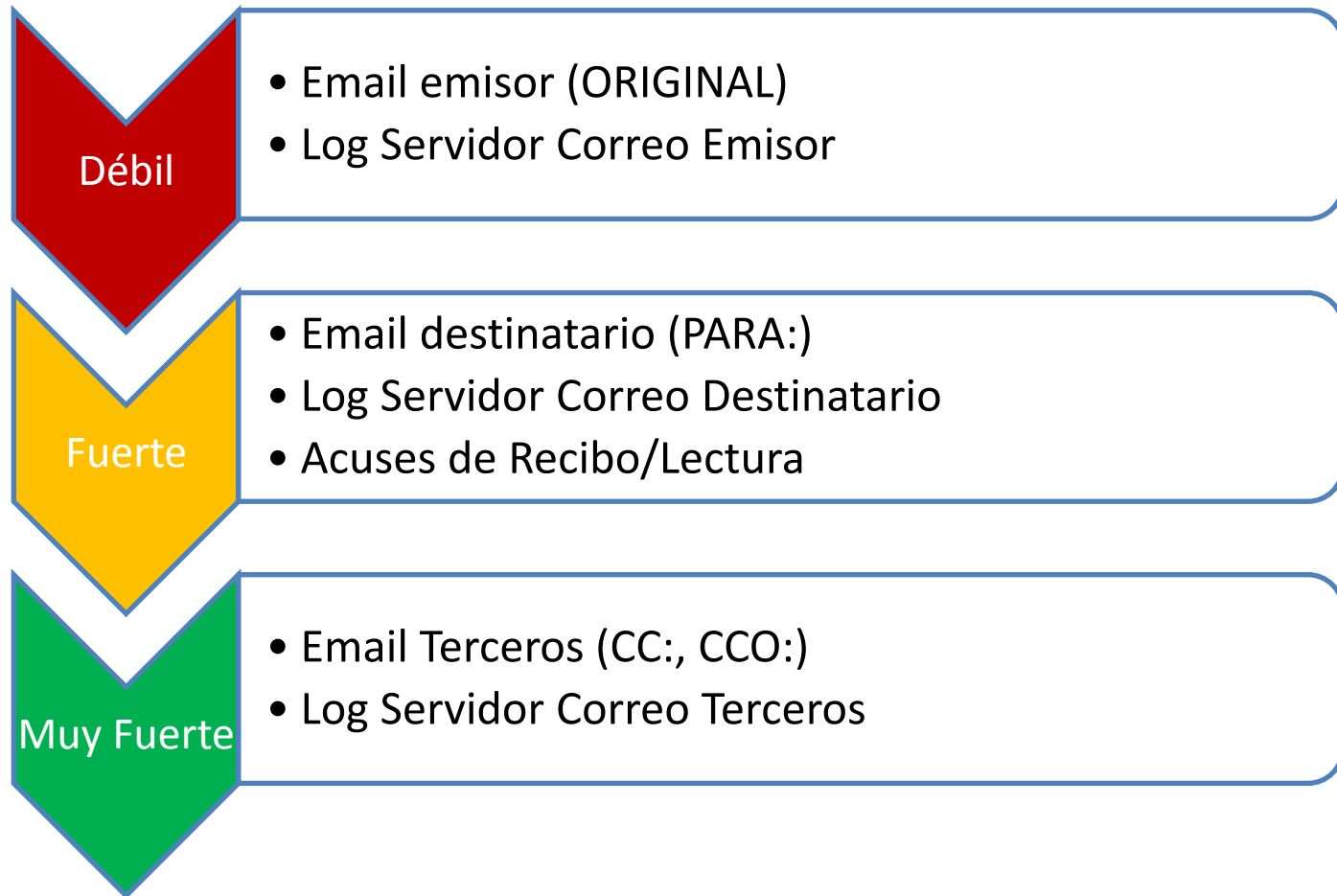
- Almacenamiento Seguro de Discos Duros, Cintas de Backup, Memorias USB, CD/DVD...
- Tercera Parte Privada
- Mantenimiento Cadena de Custodia
- Garantiza la no alteración desde el Depósito hasta la Retirada
- Servicio Certificado bajo las normas ISO-27001 e ISO-20000



Ejemplo: Validez de eMail

- Problemas Actuales:
 - Ausencia de evidencias
 - ¿Alguien tiene una copia del correo?
 - ¿políticas de retención/custodia de email?
 - Repudio de emisión / recepción:
 - ¿Se ha enviado un email?
 - ¿Se ha recibido un email?
 - Autenticidad de evidencia
 - ¿Se ha alterado un email recibido?
 - (casi) Nadie usa **FIRMA ELECTRÓNICA**

Ejemplo: Validez de eMail



Evidencias Digitales: Validez de eMail

ArchivaMail



Google Postini Services

Soluciones actuales:

ArchivaMail®: Servicio de Archivo y Custodia Segura de Correo Electrónico (2012)

- Tercera Parte de Confianza
- Almacenamiento Seguro por 10 años de todos los correos enviados y recibidos por las partes de una conversación
- Políticas de Correo electrónico corporativo
- Recepción Garantizada
- Cumplimiento Legal, apto para eDiscovery
- Cifrado

(www.archivamail.com)

¿El futuro?

- La nube.... ¿Quién controla los datos?
- Ciberseguridad \leftrightarrow Ciberdelitos
- IC - Infraestructuras Críticas

¿Qué son las IC?

La **LPIC** (Ley 8/2011 de Protección de Infraestructuras Críticas) establece una definición oficial de lo que en España debe ser considerado como Infraestructura Crítica:

- “Las infraestructuras estratégicas (es decir, aquellas que proporcionan servicios esenciales) cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales”.
- En el caso de sufrir un ataque, causarían gran impacto en la seguridad, tanto física como económica, de los ciudadanos o en el buen funcionamiento del Gobierno de la Nación.
- Este impacto se mide según unos criterios horizontales que determinan la criticidad de una infraestructura. Se han establecido tres:
 - el número potencial de víctimas
 - el impacto económico
 - y el impacto público

Tipos de Ciberamenazas

1. **Ciberespionaje** (Robo propiedad industrial/intelectual)

- Objetivo: Administraciones públicas / Empresas estratégicas
- China, Rusia, Irán, otros...
- Servicios de Inteligencia / Fuerzas Armadas / Otras empresas

2. **Ciberdelito** (Crimen por Internet)

- Objetivo: Robo información de tarjetas de crédito / Fraude Telemático / Blanqueo de dinero...
- HACKERS y crimen organizado

Tipos de Ciberamenazas

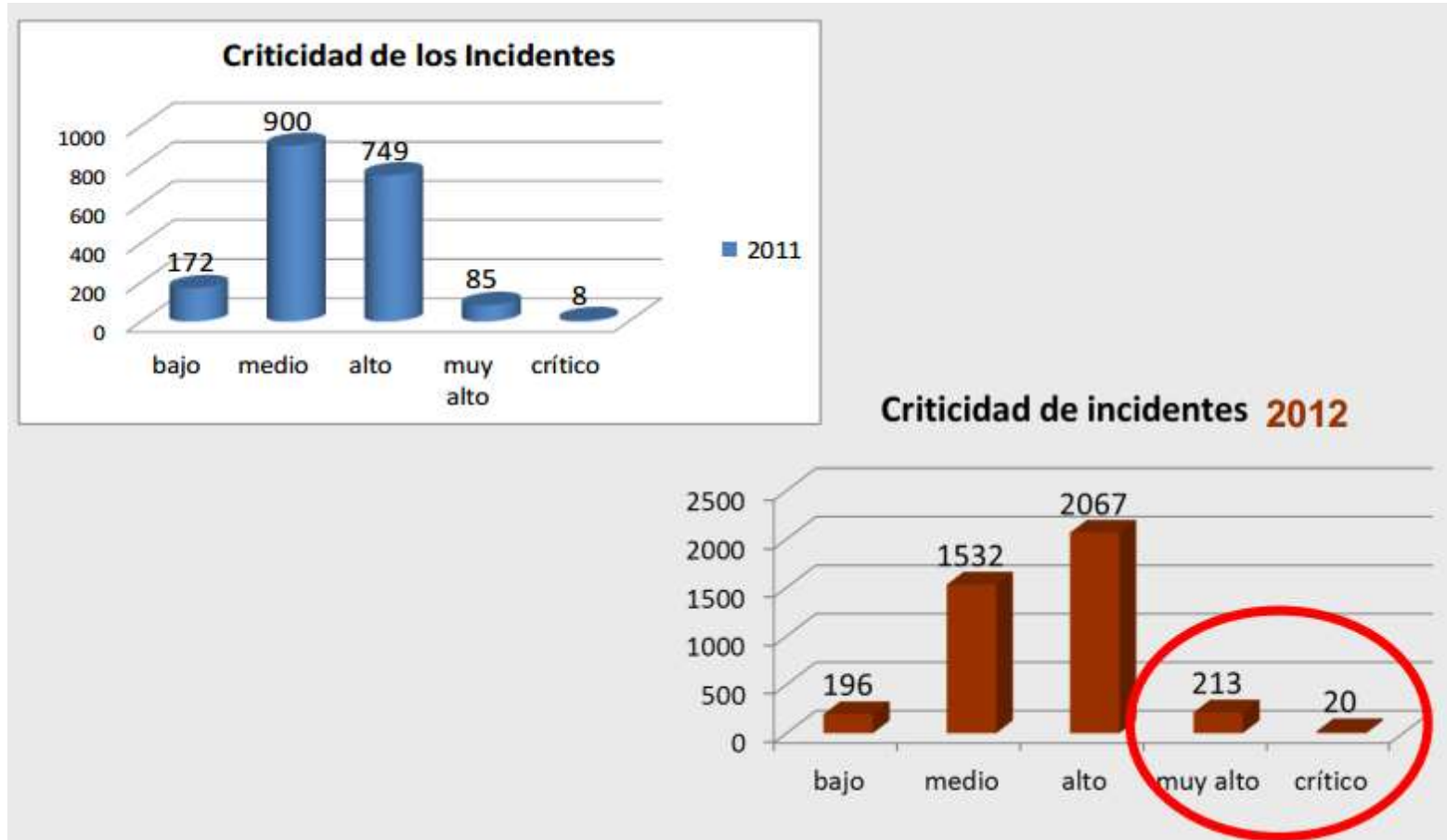
3. **Ciberactivismo** (Uso político de Internet)

- Objetivo: Ataques a servicios webs / Robo y publicación de datos e información sensible o de carácter personal.
- ANONYMOUS y otros grupos

4. **Ciberterrorismo** (Uso de Internet por terroristas)

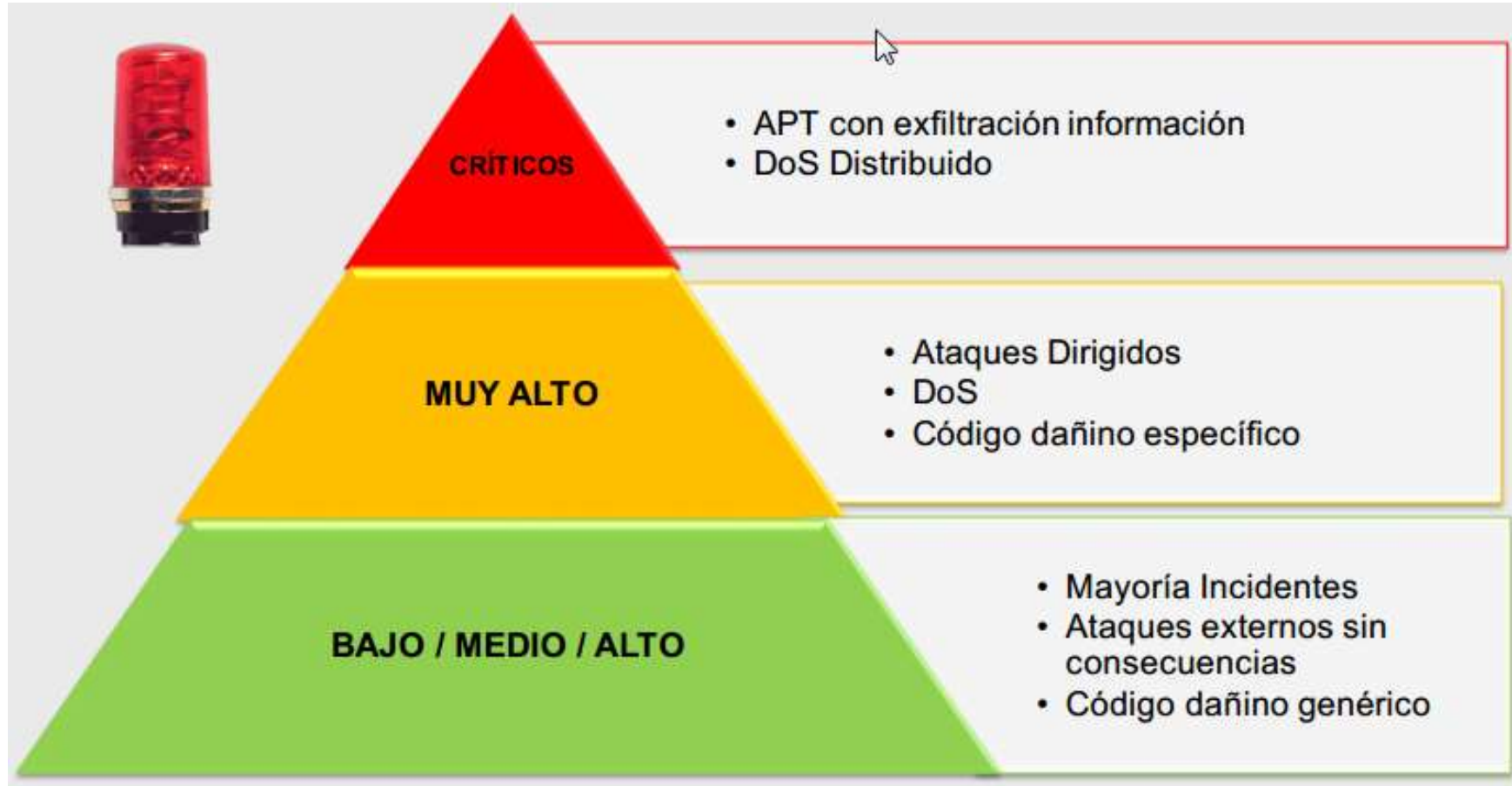
- Objetivo : Comunicaciones , obtención de información, propaganda o financiación, Ataque a Infraestructuras críticas
- ETA , organizaciones de apoyo y Grupos Yihaidistas

Riesgos para las empresas



(fuente: CCN - Centro Criptológico Nacional, Ene-2013)

Riesgos para las empresas



(fuente: CCN - Centro Criptológico Nacional, Ene-2013)

Sectores que reciben más ataques en ESPAÑA



(fuente: CCN - Centro Criptológico Nacional, Ene-2013)

Protección Infraestructuras Críticas:



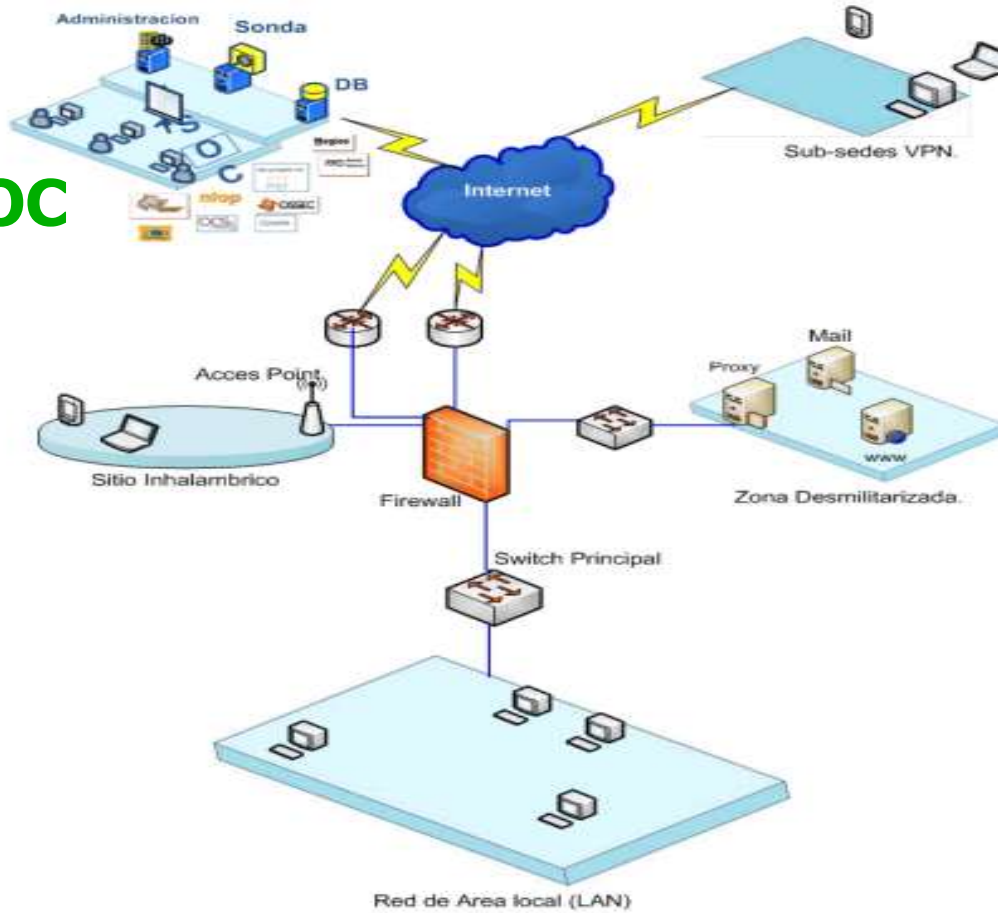
Soluciones actuales:

SOC (*Security Operation Center*): Servicio remoto de monitorización y gestión de las alertas de seguridad (2013)

- Integrado con el Centro Nacional de Respuesta a Incidentes en Infraestructuras Críticas de CNPIC-INTECO
- Gestión Remota de equipos de seguridad distribuidos
- Monitorización y vigilancia activa de las infraestructuras críticas
- Respuesta ante incidentes
- Servicio certificado ISO-20000 e ISO-27001

Protección Infraestructuras Críticas:

SOC



PROTOTIPO DE RED PARA IMPLEMENTACION DE UN SOC REMOTO, TOMANDO COMO BASE EL OSSIM, COMO PLATAFORMA DE GESTION



Evidencias Digitales: “All you need is *Logs*” ([The Beatles](#))

*“Logs, logs, logs...
All you need is logs, logs.
Logs is all you need”*

(casi) **todo lo que un perito informático necesita
está en los logs**



¡MUCHAS GRACIAS!

Para contactar:



<http://www.informatica-forense.es>



javier.pages@informatica-forense.es



<https://plus.google.com/114594286707524576385>



<http://inforesnes.blogspot.com.es/>



<https://www.linkedin.com/in/javierpages>
<https://www.linkedin.com/company/informatica-forense-s.l.>



<https://www.facebook.com/javier.pageslopez>
<https://www.facebook.com/pages/Informática-Forense-SL/100204923472919>



<http://www.scoop.it/t/informatica-forense>