Curso: (30227) Seguridad Informática

Fernando Tricas García

Departamento de Informática e Ingeniería de Sistemas
Universidad de Zaragoza
http://webdiis.unizar.es/~ftricas/
http://moodle.unizar.es/
ftricas@unizar.es

Tema Gestión del riesgo

Fernando Tricas García

Departamento de Informática e Ingeniería de Sistemas
Universidad de Zaragoza
http://webdiis.unizar.es/~ftricas/
http://moodle.unizar.es/
ftricas@unizar.es

Departamento de Informática e Ingeniería de Sistemas
Universidad Zaragoza

Gestión del riesgo

- Seguridad:

  prevención, contabilidad, auditoría, vigilancia, privacidad, confidencialidad,...

- Pero queremos:

  funcionalidad, ergonomía, eficiencia, a tiempo, simplicidad,...

¿Entonces?

Departamento de Informática e Ingeniería de Sistemas
Universidad Zaragoza

Gestión de riesgos

- Hay que pensar en términos de gestión de riesgos
- Sólo si entendemos el contexto de un 'compromiso', podemos tomar una decisión inteligente.
- La gestión de riesgos tiene que ver con la seguridad (security), la confiabilidad (reliability), y la incocuidad (safety).

Resumen

- Primero, la calidad
  - Modelo de espiral
    1. Requerimientos
    2. Identificación de riesgos
    3. 'Resolución' de los riesgos
  - U otros, claro...

La construcción de programas seguros tiene mucho que ver con la disciplina y la 'formalidad' pero cuidado ...
Además del proceso, es fundamental comprender lo que se tiene entre manos.

Requerimientos

- Identificar las necesidades de seguridad
  - Mal: 'la aplicación utilizará criptografía cuando sea conveniente'
  - Mejor: 'los números de las tarjetas de crédito deben protegerse contra escuchas'

Requerimientos

- Identificar las necesidades de seguridad
  - Mal: 'la aplicación utilizará criptografía cuando sea conveniente'
  - Mejor: 'los números de las tarjetas de crédito deben protegerse contra escuchas'
- Deben proporcionar un marco consistente de análisis.
- Una buena especificación proporciona una visión general del sistema.
  - ¿Qué hace?
  - ¿Por qué lo hace?
  - Debería ser tan formal como sea posible (sin olvidar que su misión es la de facilitar la comprensión del sistema).

Evaluación de riesgos

- El sistema más seguro del mundo es ....

http://www.youtube.com/watch?v=uqQwY-T6tE0

Otro:

http://www.youtube.com/watch?v=_3syp77QPts

Evaluación de riesgos

- La evaluación de riesgos tiene que ver con la especificación del sistema
- Durante el desarrollo pueden aparecer nuevos riesgos.
- No todos los riesgos son iguales

Ya se puede evaluar!

Departamento de Informática e Ingeniería de Sistemas
Universidad Zaragoza

Además

Diseño seguro

- La seguridad debería tenerse presente en todas las fases del desarrollo
- Ninguno de los sistemas operativos mas conocidos fueron diseñados con la seguridad como objetivo
  - Flujo de datos
  - Usuarios, papeles, derechos. Explícitos e implícitos.
  - Relaciones de confianza
  - Soluciones potenciales a cualquier problema conocido.

Dos aspectos fundamentales:

- Desarrollo cuidadoso
- Auditoría del código

Además

Pruebas

- El sistema funcionando
- Observación cercana
- Experiencia
- Probar 'buscando debilidades'
- ¿Se usa todo el código? ('code coverage')

Departamento de Informática e Ingeniería de Sistemas
Universidad Zaragoza

Gestión de riesgos en la práctica

- Los programadores: “No es mi trabajo”
- Departamento de seguridad: “revisión al final”
- Pruebas de “caja negra” (poco eficaces)
- “Equipo rojo” (alguien intenta atacarnos)
  - No encontrar problemas no significa que no los haya
  - No es interesante para el equipo

Análisis de Riesgos

Terminología

- **Activos** ('assets') lo que es valioso para nosotros
  - hardware
  - software
  - datos e información (datos internos del negocio, documentos de diseño, contenido digital, datos de clientes, ...)
  - reputación
- **Vulnerabilidades** ('vulnerabilities') debilidades o fallos que podrían ocasionar problemas en nuestros activos
- **Amenazas** ('threats')

Cont.

Departamento de Informática e Ingeniería de Sistemas
Universidad Zaragoza

Análisis de Riesgos

Terminología

- **Impacto** valor de los activos + criticidad de las vulnerabilidades
- **Riesgos** ('risks'): probabilidad × impacto
  - Daño potencial
  - Reproducibilidad
  - Explotabilidad
  - ¿A quién afecta?
  - ¿Es fácil de descubrir?
- **Contramedidas o salvaguardas**

Departamento de Informática e Ingeniería de Sistemas
Universidad Zaragoza

Entonces ...

- Comprender el contexto del negocio
- Identificar los riesgos del negocio y los técnicos (y relacionarlos entre sí).
- Sintetizar y ordenar los riesgos (¿Qué haremos primero?) Probabilidad, gravedad, cantidad, ...
- Definir la estrategia de mitigación
- Hacer los cambios y validar
- Medir e informar

Repetir

Departamento de Informática e Ingeniería de Sistemas
Universidad Zaragoza

Análisis de Riesgos

No sólo los del negocio

- Requisitos de seguridad
  - Consideraciones contractuales
  - Consideraciones financieras y económicas
  - Legales y regulatorios (LOPD, LISI, LSSI, otras ...)
  - Otros (PCI, CC, ...)

Algunas referencias pueden ser normativas mas o menos establecidas, no sólo legales, sino de certificaciones, usos y costumbres, ...

Análisis de Riesgos

No sólo los del negocio

- Requisitos de seguridad
  - Consideraciones contractuales
  - Consideraciones financieras y económicas
  - Legales y regulatorios (LOPD, LISI, LSSI, otras ...)
  - Otros (PCI, CC, ...)

Algunas referencias pueden ser normativas mas o menos establecidas, no sólo legales, sino de certificaciones, usos y costumbres, ...

- Las decisiones
  - 'tiene que tener'
  - 'debería tener'
  - 'estaría bien que tuviera'

La ley

LOPD

Ley Orgánica de Protección de Datos establece:

- Responsable del fichero.
  - Empresa responsable de datos de empleados y clientes
  - Autónomo responsable de datos de sus clientes
  - Organismos públicos responsables de los datos de sus administrados
- Datos personales: nombre, apellidos, fechas, direcciones, teléfonos, fotografías, ...
- Ficheros automatizados y no automatizados (papel)
- Nivel alto, medio, básico
  - ALTO: salud, política, sindicatos, sexo, religión
  - MEDIO: datos económicos, saldos, pagos, situación financiera,...
  - BAJO: el resto; nombre, apellido, dirección, teléfono, ...

¡Sanciones!

La ley

LSSI

Ley de Servicios de la Sociedad de la Información y Comercio Electrónico

- Obligaciones de información (denominación social, NIF, domicilio, dirección de correo electrónico, teléfono o fax) ...
- Trámites electrónicos (Si procede)
  - Regula el comercio y los ISP
  - Obligatoriedad de guardar acceso de los usuarios
  - Identificación de sitios web

`http://www.lssi.es/`

Leyes

- Ley de Firma Digital
- Ley Administración Electrónica
- Ley General de Telecomunicaciones
- Factura Electrónica

...

Cronología legal

Year	Industry & Government Reactions	Industry or Criteria
1995	European Privacy Law	Protects the privacy of individuals when their data is processed or transmitted
1996	HIPAA – Health Insurance Portability and Accountability Act	Healthcare
1996	Economic Espionage Act	Makes the theft or misappropriation of trade secrets involving commercial information, not classified or national defense information, a federal crime
1999	GLBA - Gramm-Leach-Bliley Act	Financial Services
2002	FISMA - Federal Information Security Management Act	US Federal Government
2002	SOX - Sarbanes-Oxley	Public Companies
2003	CA SB 1386 - California Senate Bill 1386 (40+ states have followed suit)	Requiring organizations that maintain personal information about individuals to inform those individuals if the security of their information is compromised
2004	Basel II	Financial Services
2006	PCI DSS – Payment Card Industry Data Security Standard	Companies processing credit card data
2006	NERC CIPS – North American Electric Reliability Corporation Critical Infrastructure Protection Standards	Electric Power
2008	Red Flags Rule	Financial Services
2009	HITECH - Health Information Technology for Economic and Clinical Health Act	Healthcare

Algún detalle

- SOX (Sarbanes-Oxley Act)
  (Empresas cotizadas en bolsa en USA)
- HI PAA (Health Insurance Portability and Accountability Act)
  - HITECH Act: Privacy requirementes

  Sanidad (cercana a la LOPD)
- Basel II
  Basilea. Bancos.

Seguridad y calidad en la sociedad de la Información
Mariano Gómez Benito

http://jcel.unizar.es/jcel08/doc/JCEL08_Seguridad_Calidad_Sociedad_Informacion.pdf

PCI DSS

Payment Card Industry Data Security Standard

- VISA 15 de diciembre de 2004
  - 'Payment Card Industry. Data Security Standard'
  - Versión 1.0
  - (PCI 1.0 Master Card Internacional. Enero 2005)
- PCI DSS 3.0, noviembre de 2013.
  - PCI DSS 1.1, septiembre de 2006.
  - PCI DSS 1.2, 1 de octubre de 2008.
  - PCI DSS 2.0, 28 de octubre de 2010.

`https://www.pcisecuritystandards.org/`
`https://www.pcisecuritystandards.org/popups/pcirocks.php`
`http://www.youtube.com/watch?v=xpfCr4By71U`

`https://www.pcisecuritystandards.org/security_standards/documents.php`

PCI: índice

PCI Data Security Standard – High Level Overview

Build and Maintain a Secure Network	**1.** Install and maintain a firewall configuration to protect cardholder data **2.** Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	**3.** Protect stored cardholder data **4.** Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	**5.** Use and regularly update anti-virus software or programs **6.** Develop and maintain secure systems and applications
Implement Strong Access Control Measures	**7.** Restrict access to cardholder data by business need to know **8.** Assign a unique ID to each person with computer access **9.** Restrict physical access to cardholder data
Regularly Monitor and Test Networks	**10.** Track and monitor all access to network resources and cardholder data **11.** Regularly test security systems and processes.
Maintain an Information Security Policy	**12.** Maintain a policy that addresses information security for all personnel.

Requirement 6

'Develop and maintain secure applications'

- Aplicar parches (6.1)
  - Se puede utilizar una aproximación 'risk based' (1 mes - 3 meses)
- Establecer un procedimiento para identificar **y asignar un nivel de riesgo a las** vulnerabilidades que se descubran. (6.2)
  - En negrita es sólo 'best practice' se considerará requisito en 2012

Requisito 6: Desarrolle y mantenga sistemas y aplicaciones seguras

Las personas sin escrúpulos utilizan las vulnerabilidades de seguridad para obtener acceso privilegiado a los sistemas. Muchas de estas vulnerabilidades se pueden subsanar mediante parches de seguridad proporcionados por los proveedores. Las entidades que administran los sistemas deben instalar estos parches. Todos los sistemas importantes deben poseer la última versión de los parches adecuados para estar protegidos contra la explotación de los datos de los titulares de las tarjetas y el riego que representan los delincuentes y el software malicioso.

Nota: Los parches de software adecuados son aquéllos que se evaluaron y probaron para confirmar que no crean conflicto con las configuraciones de seguridad existentes. En el caso de las aplicaciones desarrolladas internamente por la institución, es posible evitar numerosas vulnerabilidades mediante la utilización de procesos estándares de desarrollo de sistemas y técnicas de codificación segura.

Requisitos de las DSS de la PCI	Procedimientos de prueba	Implementado	No implementado	Fecha objetivo y comentarios
6.1 Asegúrese de que todos los componentes de sistemas y software cuenten con los parches de seguridad más recientes proporcionados por los proveedores. Instale los parches importantes de seguridad dentro de un plazo de un mes de su lanzamiento. *Nota: Las organizaciones pueden tener en cuenta la aplicación de un enfoque basado en el riesgo a los efectos de priorizar la instalación de parches. Por ejemplo, al priorizar infraestructura de importancia (por ejemplo, dispositivos y sistemas públicos, bases de datos) superiores a los dispositivos internos menos críticos a los efectos de asegurar que los dispositivos y los sistemas de alta prioridad se traten dentro del periodo de un mes y se traten dispositivos y sistemas menos críticos dentro de un periodo de tres meses.*	**6.1.a** En el caso de la muestra de componentes del sistema y del software relacionado, compare la lista de parches de seguridad instalados en cada sistema con la última lista de parches de seguridad proporcionados por el proveedor a los efectos de confirmar que los actuales parches proporcionados por los proveedores están instalados.			
	6.1.b Evalúe las políticas relacionadas con la instalación de parches de seguridad a fin de establecer que solicitan la instalación de todos los nuevos parches de seguridad relevantes dentro de un plazo de un mes.			
6.2 Establezca un proceso para identificar las vulnerabilidades de seguridad recientemente descubiertas (por ejemplo, suscríbase a los servicios de alerta disponibles de forma gratuita . a través de Internet). Actualice las normas de configuración conforme al Requisito 2.2 de las DSS de la PCI para subsanar cualquier otro problema de vulnerabilidad.	**6.2.a** Consulte al personal responsable para controlar que se implementan procesos para identificar nuevas vulnerabilidades de seguridad.			
	6.2.b Controle que los procesos para identificar nuevas vulnerabilidades de seguridad incluyan el uso de fuentes externas de información sobre vulnerabilidades de seguridad y la actualización de las normas de configuración de sistemas revisadas en el Requisito 2.2 a medida que se encuentren nuevos problemas de vulnerabilidad.			

Requirement 6

'Develop and maintain secure applications'

- Desarrollar basándose en las 'mejores prácticas' de la industria e incluyendo el desarrollo seguro a través del ciclo completo de desarrollo. (6.3)
  - Eliminar cuentas de la aplicación, identificadores, claves y elementos de prueba antes de que la aplicación esté activa y disponible.
  - Revisar código a medida (interno y externo) antes de ponerlo en producción, para identificar problemas de codificación.
- Seguir procedimientos para cambios de programas y de configuraciones. (6.4)
  - Separación entre pruebas y producción, control de cambios, documentación de impactos ...

Requirement 6

'Develop and maintain secure applications'

- Desarrollar aplicaciones siguiendo consejos sobre codificación segura. (6.5)
  - Cita el proyecto OWASP. Si aparece el 'Top 10' (y fija como estándar el último vigente en cada momento)

    `http://www.owasp.org/`
  - Han añadido SANS CWE Top 25, CERT Secure Coding y lo que llaman 'industry best practices'

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
6.5.1 Injection flaws, particularly SQL injection. Also consider OS Command Injection, LDAP and XPath injection flaws as well as other injection flaws.	**6.5.1** Injection flaws, particularly SQL injection. (Validate input to verify user data cannot modify meaning of commands and queries, utilize parameterized queries, etc.)			
6.5.2 Buffer overflow	**6.5.2** Buffer overflow (Validate buffer boundaries and truncate input strings.)			
6.5.3 Insecure cryptographic storage	**6.5.3** Insecure cryptographic storage (Prevent cryptographic flaws)			
6.5.4 Insecure communications	**6.5.4** Insecure communications (Properly encrypt all authenticated and sensitive communications)			
6.5.5 Improper error handling	**6.5.5** Improper error handling (Do not leak information via error messages)			
6.5.6 All "High" vulnerabilities identified in the vulnerability identification process (as defined in PCI DSS Requirement 6.2). ***Note:*** *This requirement is considered a best practice until June 30, 2012, after which it becomes a requirement.*	**6.5.6** All "High" vulnerabilities as identified in PCI DSS Requirement 6.2.			
Note: *Requirements 6.5.7 through 6.5.9, below, apply to web applications and application interfaces (internal or external):*				
6.5.7 Cross-site scripting (XSS)	**6.5.7** Cross-site scripting (XSS) (Validate all parameters before inclusion, utilize context-sensitive escaping, etc.)			
6.5.8 Improper Access Control (such as insecure direct object references, failure to restrict URL access, and directory traversal)	**6.5.8** Improper Access Control, such as insecure direct object references, failure to restrict URL access, and directory traversal (Properly authenticate users and sanitize input. Do not expose internal object references to users.)			
6.5.9 Cross-site request forgery (CSRF)	**6.5.9** Cross-site request forgery (CSRF). (Do not reply on authorization credentials and tokens automatically submitted by browsers.)			

Requirement 6

'Develop and maintain secure applications'

- Para aplicaciones web de cara al público, ocuparse de las nuevas amenazas y vulnerabilidades de manera constante y asegurarse de que están protegidas contra ataques conocidos
  - Mediante revisión manual o automatizada
    o bien
  - Mediante un cortafuegos de aplicación (WAF, web application firewall)

Requirement 7

- Restringir el acceso a los datos sólo para quien realmente lo necesite.
  - Limitar el acceso a los recursos sólo a quien lo necesite
  - Establecer mecanismos que limiten el acceso basado en lo que el usuario necesita saber.

'Need to know'

El acceso sólo se permite con el menor nivel de acceso necesario para desarrollar un trabajo relacionado con el negocio.

Departamento de Informática e Ingeniería de Sistemas
Universidad Zaragoza

Requirement 8

- Asignar un identificador único a cada persona con acceso.
  - Identificador único
  - Identificación por clave, biometría, ...
  - Autentificación doble factor para acceso remoto de empleados
  - Claves cifradas en tránsito y almacenamiento
  - Asegurar identificación y gestión adecuada de claves para usuarios y administradores (no consumidores).

Requisitos de las PCI DSS	Procedimientos de prueba
8.4 Deje ilegibles todas las contraseñas durante la transmisión y el almacenamiento en todos los componentes del sistema mediante una sólida criptografía (se define en *Glosario de términos, abreviaturas y acrónimos de las PCI DSS*).	**8.4.a** A modo de muestra de componentes del sistema, examine los archivos de las contraseñas para verificar que las contraseñas sean ilegibles durante la transmisión y el almacenamiento.
	8.4.b Sólo para el caso de proveedores de servicio, observe los archivos de contraseñas para verificar que las contraseñas para clientes estén cifradas.
8.5 Asegúrese de que sean correctas la autenticación del usuario y la administración de contraseñas de usuarios no consumidores y administradores en todos los componentes del sistema de la siguiente manera:	**8.5** Revise los procedimientos y entreviste al personal para verificar que se implementen los procedimientos de autenticación de usuarios y administración de contraseñas del siguiente modo:

Requirement 9, 10 , 11

- Restringir el acceso físico a los datos de los clientes
- Seguir y vigilar los accesos a los recursos de la red y datos de los clientes
- Comprobar regularmente los sistemas de seguridad y los procesos

PCI en el mundo real

Una 'fotografía'

'Verizon 2014 PCI Compliance Report'

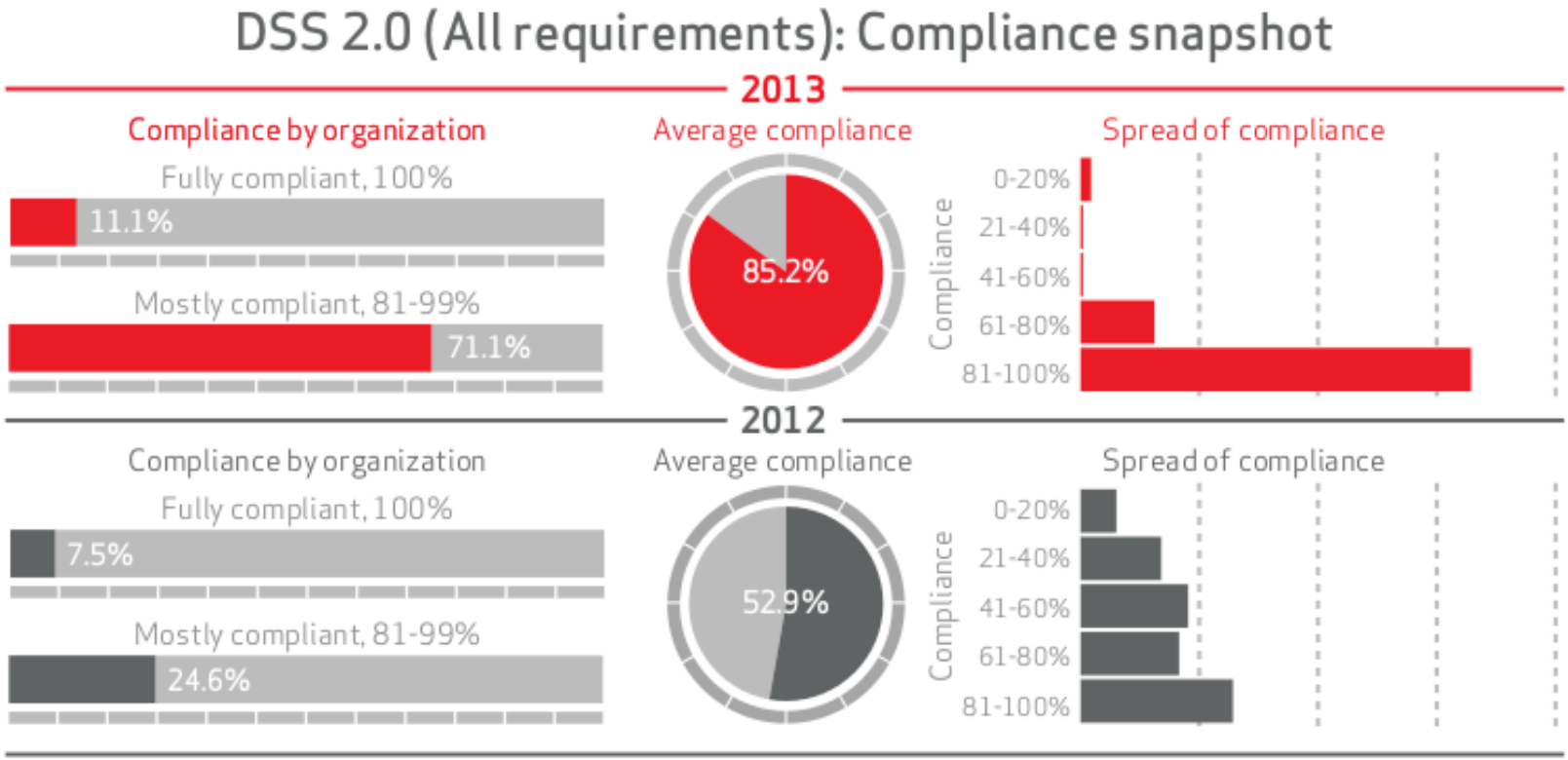

Figure 5: Snapshot for all requirements; dataset 2012 and 2013

`http://www.verizonenterprise.com/pcireport/2014/`

PCI en el mundo real

Por requisto

Summary of compliance by requirement

(l) = lowest (h) = highest

Req	Fully compliant		Mostly compliant		Average compliance	
	2012	2013	2012	2013	2012	2013
1	26.4%	64.4% ▲	17.0%	8.9% ▼	55.0%	86.4% ▲
2	22.6%	51.1% ▲	18.9%	20.0% ▲	53.9%	81.4% ▲
3	17.0%	68.9% ▲	13.2%	6.7% ▼	45.5%	79.3% ▲
4	34.0%	68.9% ▲	**(h) 20.8%**	6.7% ▼	61.2%	87.8% ▲
5	30.2%	80.0% ▲	17.0%	11.1% ▼	64.3%	95.9% ▲
6	22.6%	68.9% ▲	13.2%	13.3% ▲	51.4%	87.4% ▲
7	**(h) 41.5%**	73.3% ▲	11.3%	4.4% ▼	**(h) 66.6%**	86.8% ▲
8	22.6%	62.2% ▲	**(h) 20.8%**	15.6% ▼	58.0%	84.1% ▲
9	35.8%	**(h) 86.7%** ▲	15.1%	**(l) 4.4%** ▼	61.9%	**(h) 94.9%** ▲
10	20.8%	60.0% ▲	17.0%	17.8% ▲	46.9%	82.2% ▲
11	**(l) 11.3%**	**(l) 40.0%** ▲	**(l) 7.5%**	**(h) 28.9%** ▲	**(l) 38.9%**	**(l) 74.6%** ▲
12	30.2%	73.3% ▲	13.2%	11.1% ▼	54.8%	89.7% ▲
Overall	7.5%	11.1% ▲	24.6%	71.1% ▲	52.9%	85.2% ▲

Figure 7: Summary by requirement; dataset 2012 and 2013

PCI en el mundo real

El sexto

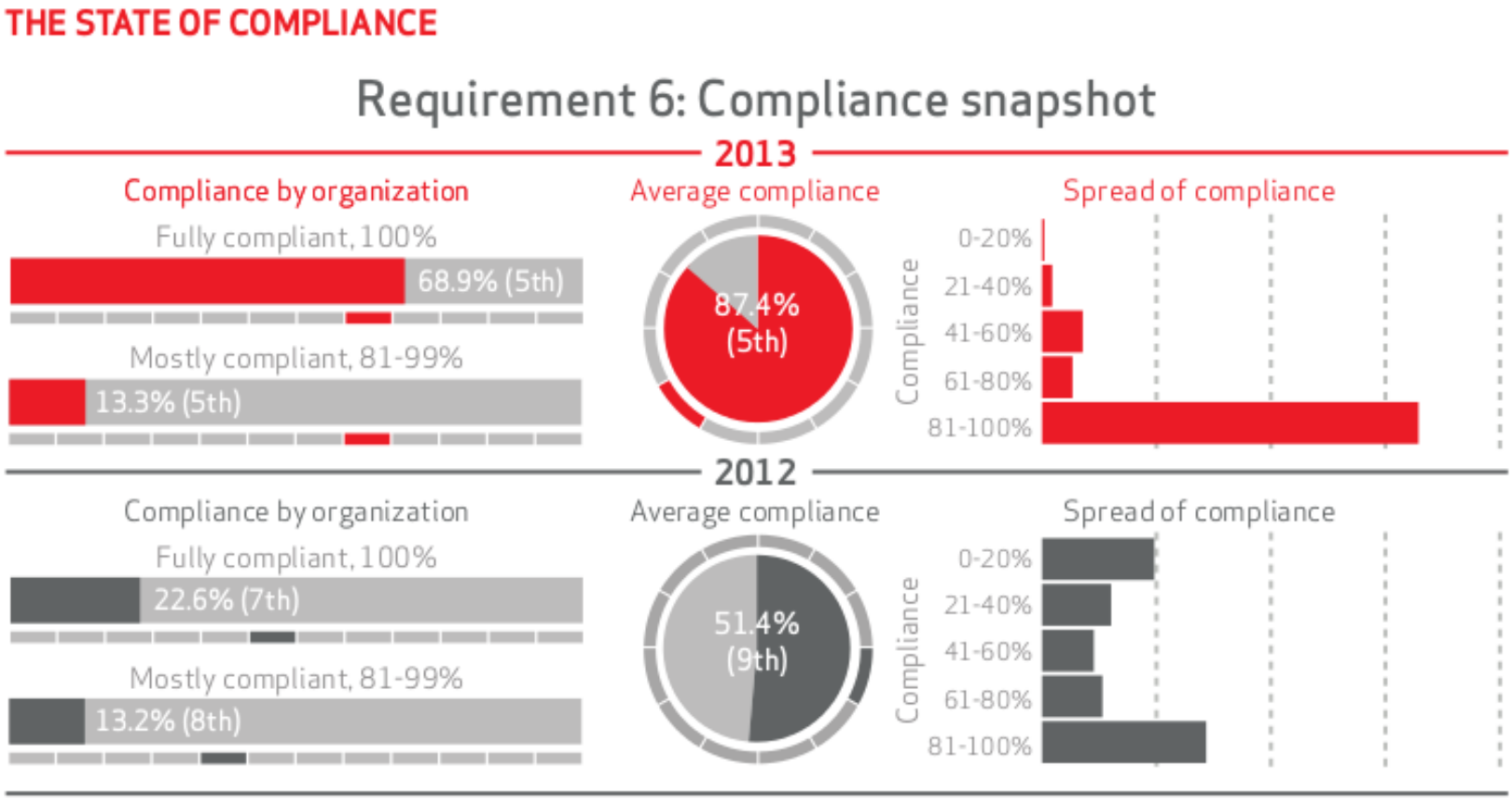

Figure 15: Snapshot for Requirement 6; dataset 2012 and 2013

PCI en el mundo real

Patch management can be a major headache for a large organization, that's why they often delay updates for as long as possible – many organizations skipped Windows Vista entirely, and 95 % of the world's ATMs still run Windows XP. After June 30, 2012 the guidance within DSS control 6.2 specifying a risk ranking based on the Common Vulnerability Scoring System (CVSS) from the Forum of Incident Response Security Teams (FIRST) came into effect. This provides a "universal, open and standardized method for rating IT vulnerabilities," enabling companies to effectively prioritize the testing and deployment of patches. We believe that this contributed to the significant improvement in compliance with this requirement in 2013.

PCI en el mundo real

Principales retos:

- Patch management
- Change management
- Secure code development
  Controls 6.3 and 6.5 govern secure code development, such as mandating code security reviews. Building security and compliance into the software development lifecycle requires a new set of skills; organizations need developers to:
  - Be aware of common and emerging coding vulnerabilities (such as found in the OWASP 2013 Top 10 and SANS Top 20)
  - Be able to identify and fix insecure code
  - Document coding standards and best practices
  - Follow testing procedures and checklists
- Cloud and web application firewalls

Recomendaciones del Banco Central Europeo

31 de enero de 2013: 'ECB releases final Recommendations for the security of internet payments and starts public consultation on payment account access services'

`http://www.ecb.europa.eu/press/pr/date/2013/html/pr130131_1.en.html`

Recommendations for the Security of Internet Payments.

`http://www.ecb.europa.eu/pub/pdf/other/`

`recommendationssecurityinternetpaymentsoutcomeofpcfinalversionafterpc201301en.pdf`

Departamento de Informática e Ingeniería de Sistemas
Universidad Zaragoza

BCE. Recomendaciones

1. Governance
2. Risk assessment
3. Incident monitoring and reporting
4. Risk control and mitigation
5. Traceability
6. Initial customer identification, information
7. Strong customer authentication
8. Enrolment for and provision of authentication tools and/or software delivered to the customer
9. Log-in attempts, session time out, validity of authentication
10. Transaction monitoring
11. Protection of sensitive payment data
12. Customer education and communication
13. Notifications, setting of limits
14. Customer access to information on the status of payment initiation and execution

Departamento de Informática e Ingeniería de Sistemas
Universidad Zaragoza

Certificaciones

- Asociadas a personas:
  - CISA (Certified Information Systems Auditor),
  - CISM (Certified Information Security Manager),
  - CISSP (Certified Information Systems Security Professional), ...
- Asociadas a sistemas y organizaciones: ISO 27001
- Asociadas a productos: CC, ITSEC

ISO 27001

- ISO 27001: proporcionar un modelo para establecer, implementar, operar, monitorizar, revisar, mantener y mejorar el sistema de gestión de seguridad de la información (ISMS).
  - Management Responsibility
  - Internal Audits
  - ISMS Improvement
  - Annex A - Control objectives and controls
  - Annex B - OECD principles and this international standard
  - Annex C - Correspondence between ISO 9001, ISO 14001 and this standard

ISO 27002

- ISO 27002: principios y guías para iniciar, implantar, mantener y mejorar la gestión de la seguridad de la información dentro de una organización. Objetivos de control y controles.
  - Structure
  - Risk Assessment and Treatment
  - Security Policy
  - Organization of Information Security
  - Asset Management
  - Human Resources Security
  - Physical Security
  - Communications and Ops Management
  - Access Control
  - Information Systems Acquisition, Development, Maintenance
  - Information Security Incident management
  - Business Continuity
  - Compliance

Criterios comunes (Common Criteria)

- Gobierno USA + 'Smart Card Security User's Group' han trabajado en la creación de un sistema estandarizado para el diseño y evaluación de sistemas críticos respecto a la seguridad.
- También hay iniciativas europeas, pero son convergentes

Criterios comunes

Los criterios comunes

- Canadian Trusted Computer Products Evaluation
- European Union's Information Technology Security Evaluation Criteria (ITSEC)
- The US Federal Criteria

Los criterios comunes (*Common Criteria*) están diseñados para crear un estándar internacional (ISO 15408, versión 3.1).

`http://www.niap-ccevs.org/cc-scheme/`
`http://www.commoncriteriaportal.org/`

Criterios Comunes

- Criterios Comunes, versión 3.1
  - Tres partes:
    - Parte 1: Introduction and general model
    - Parte 2: Security functional requirements
    - Parte 3: Security assurance requirements

    $\longrightarrow$ más de 600 páginas
  - Conjunto de clases, familias, y componentes $\rightarrow$ combinadas proporcionan un perfil adecuado para cualquier producto (hw, fw, sw).
  - Reutilización

Criterios comunes

Metodología común de evaluación (Common Methodology for Information Technology)

- Mas de 400 páginas
- Definición de cómo evaluar un producto

Algunos problemas

- Poco interés de la industria
- 'Común' no es normalmente suficiente cuando hablamos de seguridad

Algunos problemas

- Poco interés de la industria
- 'Común' no es normalmente suficiente cuando hablamos de seguridad

- *Vamos a adoptar las mejores prácticas de nuestra industria. Como todos los demás.*
- *Si todos lo hacen, las mejores prácticas son lo mismo que la mediocridad.*
- *¡Basta de hacer que la mediocridad parezca mala;*
- *Lo siento...*

Algunos productos certificados

Producto	Nivel de Seguridad	Fecha del certificado
Microsoft Windows Mobile 6.5	EAL4+	05-FEB-10
Apple Mac OS X 10.6	EAL3+	08-JAN-10
Microsoft Windows Mobile 6.1	EAL4+ ALC_FLR.1	17-SEP-09
Windows Vista Enterprise	EAL4+ ALC_FLR.3	31-AUG-09
Windows Server 2008 Standard Edition		
Windows Server 2008 Enterprise Edition		
Windows Server 2008 Datacenter Edition		
Microsoft Windows Vista and Windows Server 2008	EAL1	17-SEP-08
Red Hat Enterprise Linux Version 5.1	EAL4+ ALC_FLR.3	21-APR-08
Microsoft Windows 2003 and Microsoft Windows XP	EAL4+ ALC_FLR.3	01-APR-07

`http://www.poderpda.com/noticias/que-nivel-de-seguridad-tiene-tu-sistema-operativo/`

Requisitos para cada nivel

Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Configuration management	ACM_AUT				**1**	1	**2**	2
	ACM_CAP	**1**	**2**	**3**	**4**	4	**5**	5
	ACM_SCP			**1**	**2**	**3**	3	3
Delivery and operation	ADO_DEL		**1**	1	**2**	2	2	**3**
	ADO_IGS	**1**	1	1	1	1	1	1
Development	ADV_FSP	**1**	1	1	**2**	**3**	3	**4**
	ADV_HLD		**1**	**2**	2	**3**	**4**	**5**
	ADV_IMP				**1**	**2**	**3**	3
	ADV_INT					**1**	**2**	**3**
	ADV_LLD				**1**	1	**2**	2
	ADV_RCR	**1**	1	1	1	**2**	2	**3**
	ADV_SPM				**1**	**3**	3	3
Guidance documents	AGD_ADM	**1**	1	1	1	1	1	1
	AGD_USR	**1**	1	1	1	1	1	1
Life cycle support	ALC_DVS			**1**	1	1	**2**	2
	ALC_FLR							
	ALC_LCD				**1**	**2**	2	**3**
	ALC_TAT				**1**	**2**	**3**	3
Tests	ATE_COV		**1**	**2**	2	2	**3**	3
	ATE_DPT			**1**	1	**2**	2	**3**
	ATE_FUN		**1**	1	1	1	**2**	2
	ATE_IND	**1**	**2**	2	2	2	2	**3**
Vulnerability assessment	AVA_CCA					**1**	**2**	2
	AVA_MSU			**1**	**2**	2	**3**	3
	AVA_SOF		**1**	1	1	1	1	1
	AVA_VLA		**1**	1	**2**	**3**	**4**	4

Departamento de Informática e Ingeniería de Sistemas
Universidad Zaragoza

Criterios comunes: conclusiones

- Mejor un estándar flojo que nada
- Los gobiernos parece que están apoyando este tipo de iniciativas
- En todo caso . . .

Cuidado

Departamento de Informática e Ingeniería de Sistemas
Universidad Zaragoza

Microsoft Software Development Cycle

`http://www.microsoft.com/sdl`

Versión 5.0

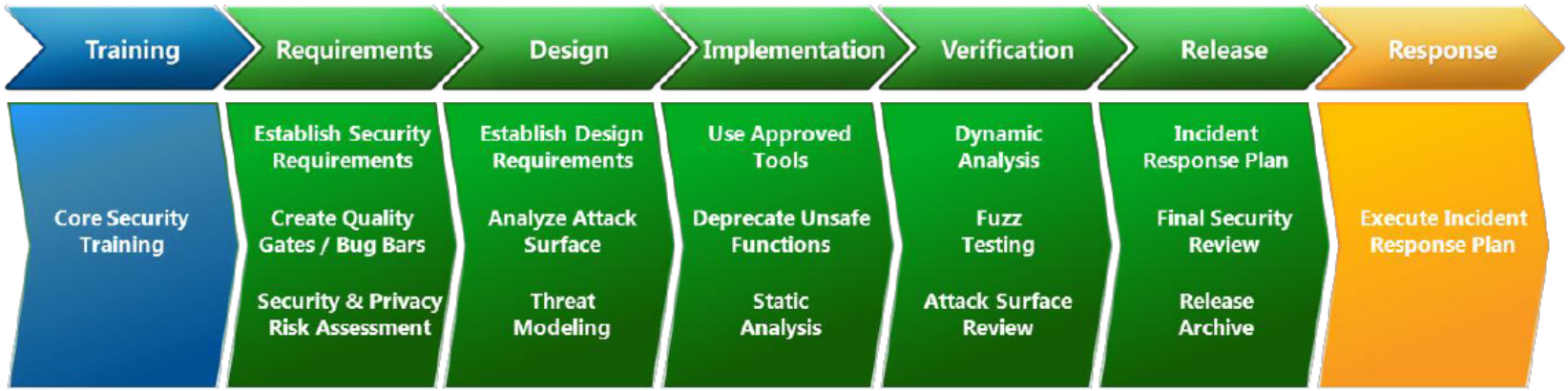

Figure 2: The Microsoft Security Development Lifecycle - Simplified

BSIMM (Building Security In Maturity Model)

`http://www.bsi-mm.com/`

Versión 2.0 (Acaban de sacar la versión 4)
Actividades relacionadas con la seguridad del software tomadas de empresas reales y organizadas para determinar nuestro estado y las posibilidades para evolucionar.

Gary McGraw, Brian Chess, Sammy Migues

The Software Security Framework (SSF)			
Governance	**Intelligence**	**SSDL Touchpoints**	**Deployment**
Strategy and Metrics	Attack Models	Architecture Analysis	Penetration Testing
Compliance and Policy	Security Features and Design	Code Review	Software Environment
Training	Standards and Requirements	Security Testing	Configuration Management and Vulnerability Management

SAMM (Software Assurance Maturity Model)

`http://www.opensamm.org/`

Versión 1

Marco abierto para ayudar a las organizaciones a formular y desarrollar estrategias de diseño seguro.

OWASP