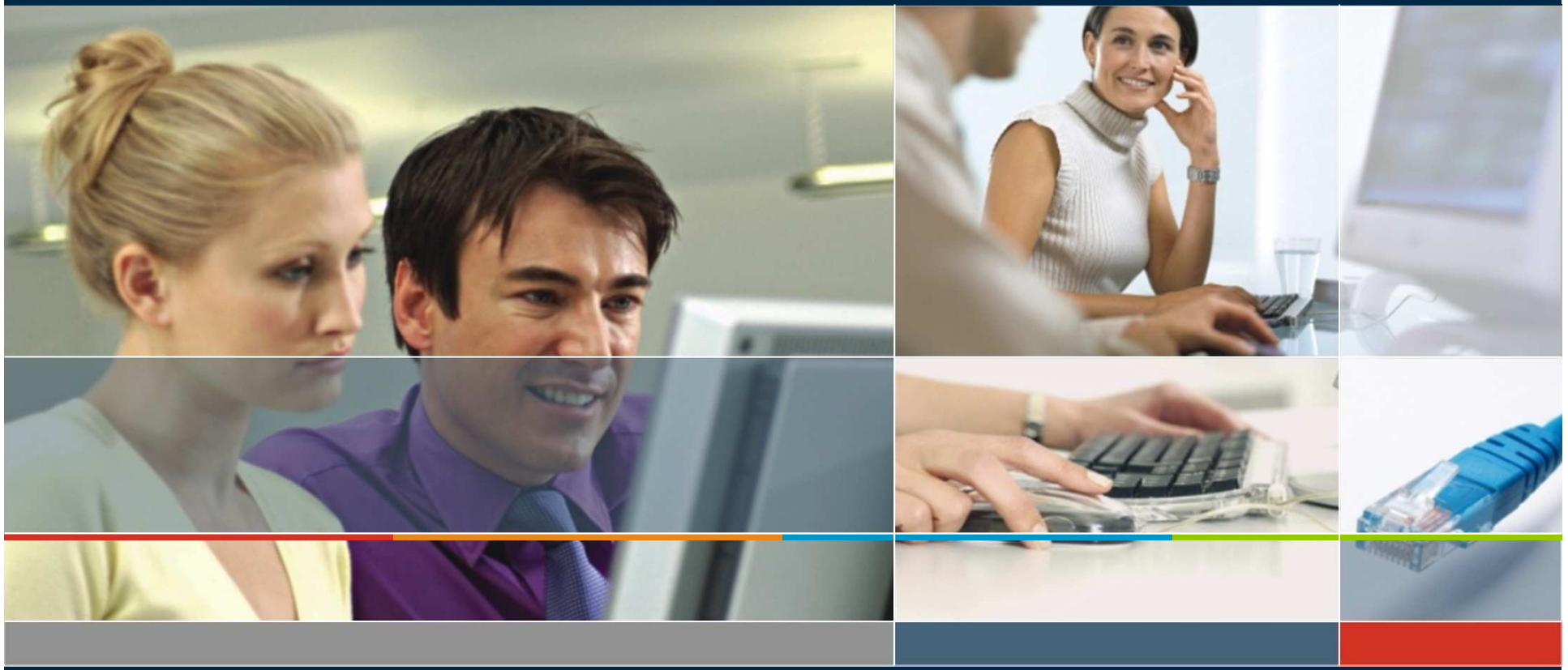
Organiza:

OWASP
The Open Web Application Security Project
Spain Chapter

Patrocina:

internet security auditors



Seguridad OWASP en la Certificación PA DSS de Aplicaciones de Pago

Abril 2011

Colabora:

FORTIFY
An HP Company

Asociación de Técnicos de Informática

c. Santander, 101. Edif. A. 2º I E-08030 Barcelona I Tel.: +34 93 305 13 18 I Fax: +34 93 278 22 48
Pº. de la Castellana, 164-166. Entlo. 1ª I E-28046 Madrid I Tel.: +34 91 788 57 78 I Fax: +34 91 788 57 01
info@isecauditors.com I **www.isecauditors.com**

ÍNDICE

1 Introducción

1.1. Contenidos

01

Introducción

Resumen de la Presentación

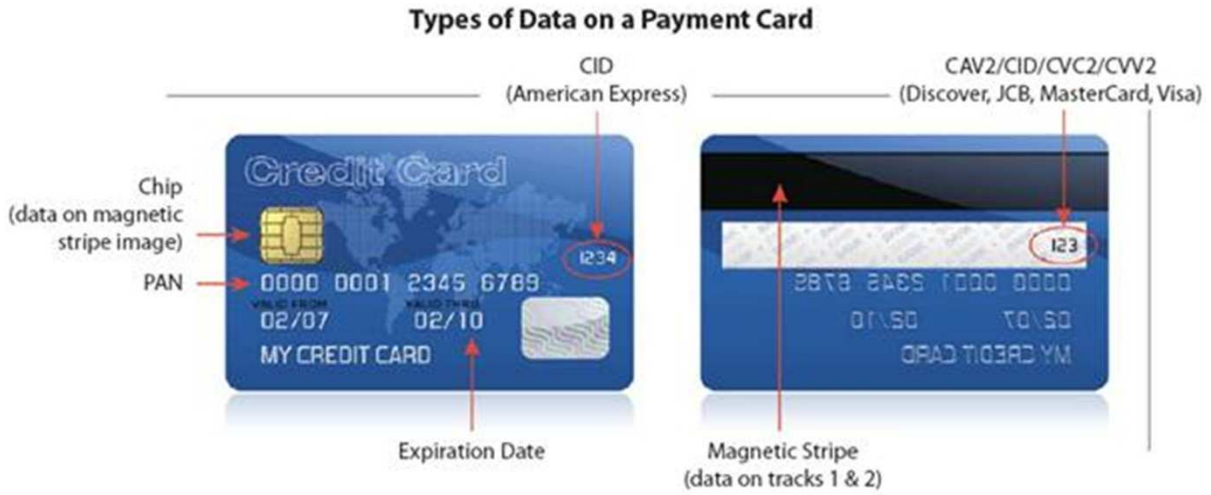
- **Bloque 1**
  - Análisis del Tipo de Datos
  - Amenazas existentes
  - Compromisos de seguridad
- **Bloque 2**
  - Explicación de PA DSS
  - Tipo de Auditoría y Experiencias
- **Bloque 3**
  - Sinergias con OWASP
- **Bloque 4**
  - Conclusiones

1.2. Amenazas

Información == $$$

Los datos de la tarjeta de crédito / débito son los más buscados

- PAN – Fecha Caducidad – Nombre
- Banda magnética o Chip – Pistas1,2 – CVV2 – PINBLOCK



Mercado Underground

Carders: Criminales que trafican o explotan datos robados de tarjetas de pago.

- Están atacando:
  - Comerciantes tradicionales.
  - Comerciantes con comercio electrónico.
  - Procesadores y agentes.
- Están buscando:
  - Software que almacena datos sensibles de tarjetas de pago.
  - Información personal para cometer robo de identidad.
  - Información de las pistas y números de cuenta de las tarjetas de pago.
- ¿Qué hacen con esto?
  - Revender estos datos a compradores en el mercado negro.
  - Compra en línea.
  - Mostrar el "premio" a la escena hack para ganar "respeto".

1.2. Amenazas

Mercado Underground

- Carding Forums (DumpsMarket, CarderPortal, Shadowcrew, CarderPlanet…)
- Formas de Pago (Liberty Reserve, WebMoney, Western Union, Money Gram , Paypal…)
- Controlados por los Administradores del Foro (Calidad de producto, membresías, reputación, análisis de reputación de vendedores...)

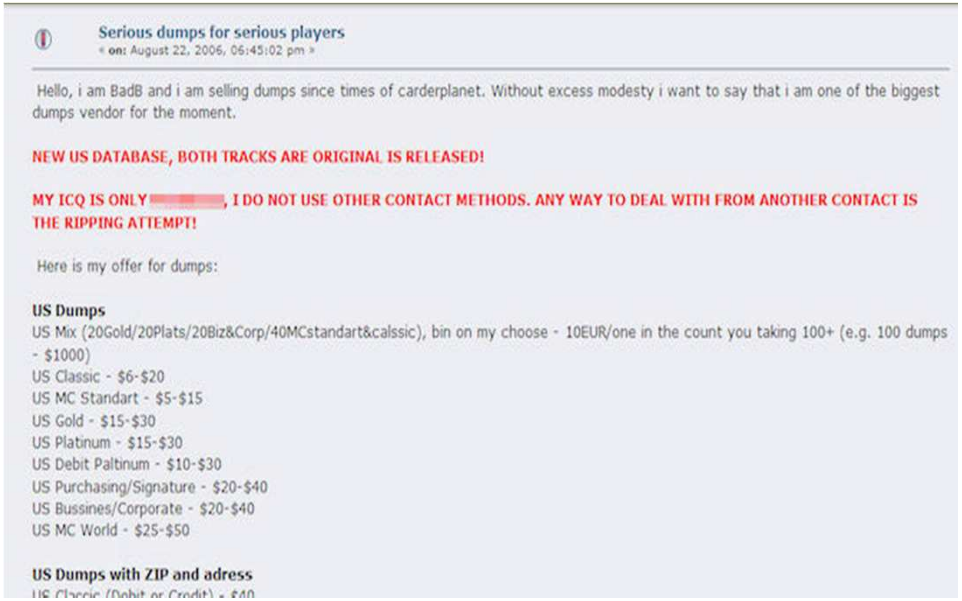
- Tecnologías usadas
  - Proxy's anónimos
  - VPN's
  - ICQ
  - …

Euro Visa | MasterCard Classic – Standart	20$
Euro Visa | MasterCard Gold – Premier – Platinum	25$
Euro Visa | MasterCard Business – Signature – Corporate – World – Purchasing	30$
Euro AMEX Green – Optima – Gold – Platinum	30$

1.2. Amenazas

Mercado Underground

- **Política de Reemplazo**
  - Precios más caros pero con garantías
- **Palabras claves**
  - dumps, carder, cvv, embossed, hologram



Serious dumps for serious players
« on: August 22, 2006, 06:45:02 pm »

Hello, i am BadB and i am selling dumps since times of carderplanet. Without excess modesty i want to say that i am one of the biggest dumps vendor for the moment.

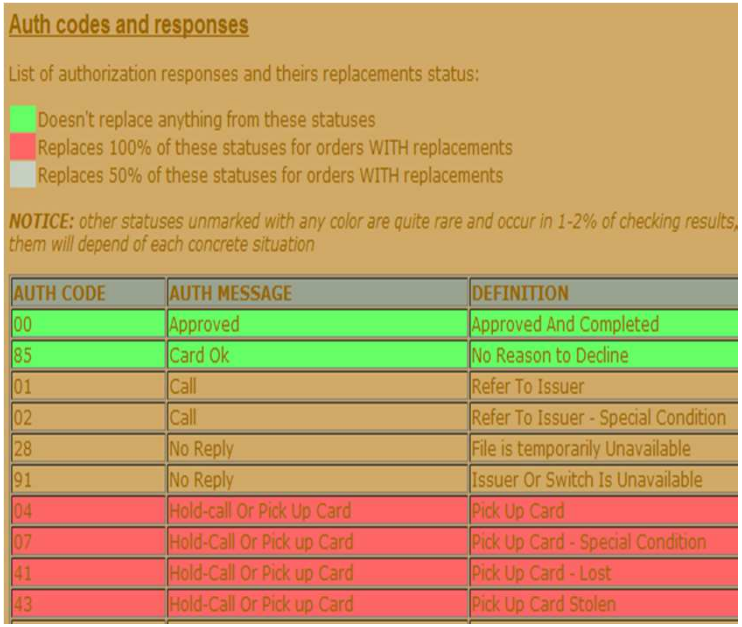
NEW US DATABASE, BOTH TRACKS ARE ORIGINAL IS RELEASED!

MY ICQ IS ONLY [redacted], I DO NOT USE OTHER CONTACT METHODS. ANY WAY TO DEAL WITH FROM ANOTHER CONTACT IS THE RIPPING ATTEMPT!

Here is my offer for dumps:

US Dumps
US Mix (20Gold/20Plats/20Biz&Corp/40MCstandart&calssic), bin on my choose - 10EUR/one in the count you taking 100+ (e.g. 100 dumps - $1000)
US Classic - $6-$20
US MC Standart - $5-$15
US Gold - $15-$30
US Platinum - $15-$30
US Debit Paltinum - $10-$30
US Purchasing/Signature - $20-$40
US Bussines/Corporate - $20-$40
US MC World - $25-$50

US Dumps with ZIP and adress
US Classic (Debit or Credit) - $40



Auth codes and responses

List of authorization responses and theirs replacements status:

Doesn't replace anything from these statuses
Replaces 100% of these statuses for orders WITH replacements
Replaces 50% of these statuses for orders WITH replacements

NOTICE: other statuses unmarked with any color are quite rare and occur in 1-2% of checking results, them will depend of each concrete situation

AUTH CODE	AUTH MESSAGE	DEFINITION
00	Approved	Approved And Completed
85	Card Ok	No Reason to Decline
01	Call	Refer To Issuer
02	Call	Refer To Issuer - Special Condition
28	No Reply	File is temporarily Unavailable
91	No Reply	Issuer Or Switch Is Unavailable
04	Hold-call Or Pick Up Card	Pick Up Card
07	Hold-Call Or Pick up Card	Pick Up Card - Special Condition
41	Hold-Call Or Pick up Card	Pick Up Card - Lost
43	Hold-Call Or Pick up Card	Pick Up Card Stolen

1.3. Compromisos

Octubre 2010 – Empresa Turismo New York

- Página Web comprometida mediante **SQL Injection**
- Acceso a datos desde 26 Septiembre 2010 a 19 Octubre 2010
- **110.000 datos de tarjeta** comprometidos
- La base de datos contenía:
  - Nombre
  - Dirección
  - Correo electrónico
  - **PAN**
  - Fecha caducidad
  - **CVV2**

Fuente: Department of Justice – New Hampshire (http://doj.nh.gov/consumer/pdf/twin_america.pdf)

1.3. Compromisos

Enero 2009 – Procesador de Pago

- Intrusión a través de **malware**
- **130 millones de tarjetas comprometidas**
- Costes de aproximadamente **60 millones de dólares**
- Alrededor de 250.000 negocios afectados
- La empresa descubrió la intrusión a partir de alertas de las marcas de pago (VISA, Mastercard, …)
- Presentó un plan de medidas de seguridad a aplicar

Fuente: U.S. Department of Justice (http://www.justice.gov/opa/pr/2009/August/09-crm-810.html)

1.3. Compromisos

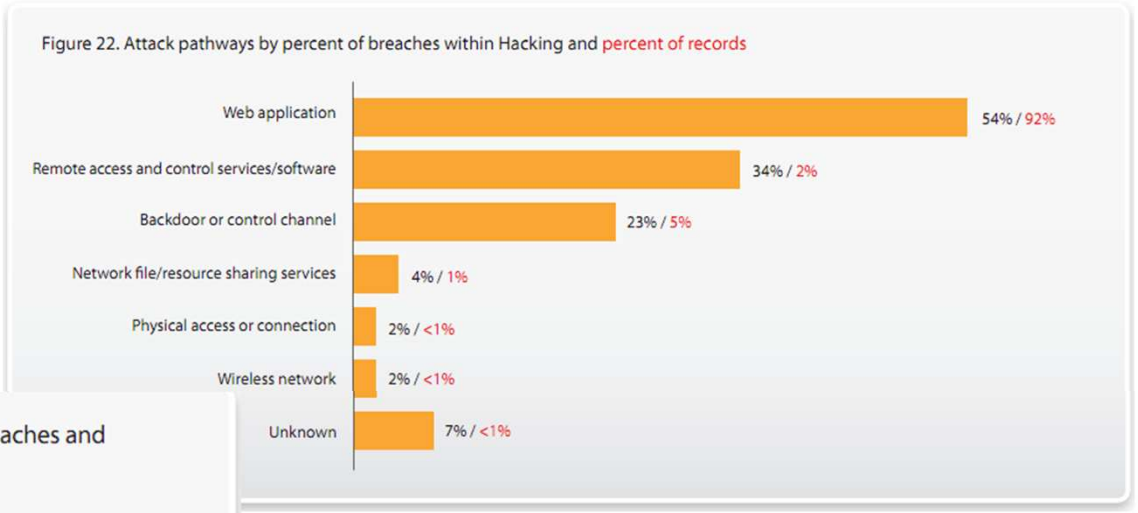
01

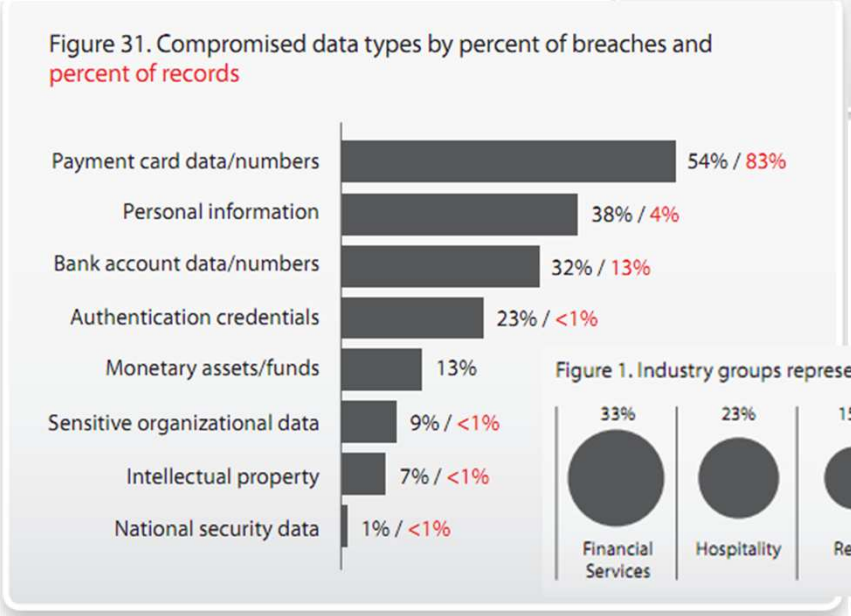
Introducción

1.1. Contenidos
1.2. Amenazas
1.3. Compromisos

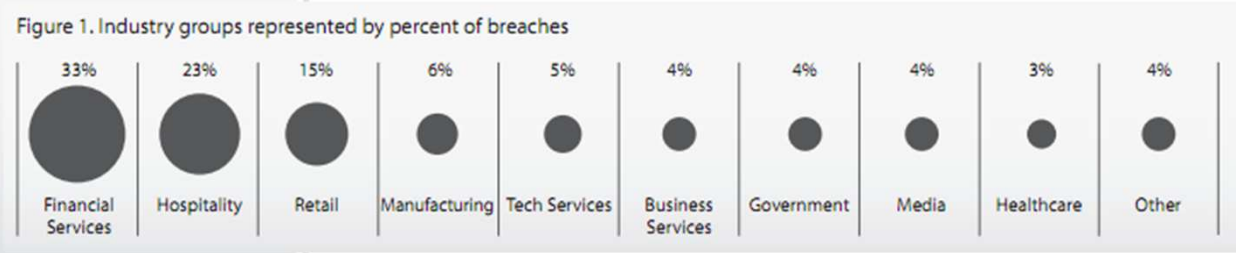
Algunas Estadísticas

Desde 2008 las Aplicaciones WEB en 1ª posición de la lista





Datos de Tarjeta de Pago Destacan, así como las industrias que trabajan con esta información

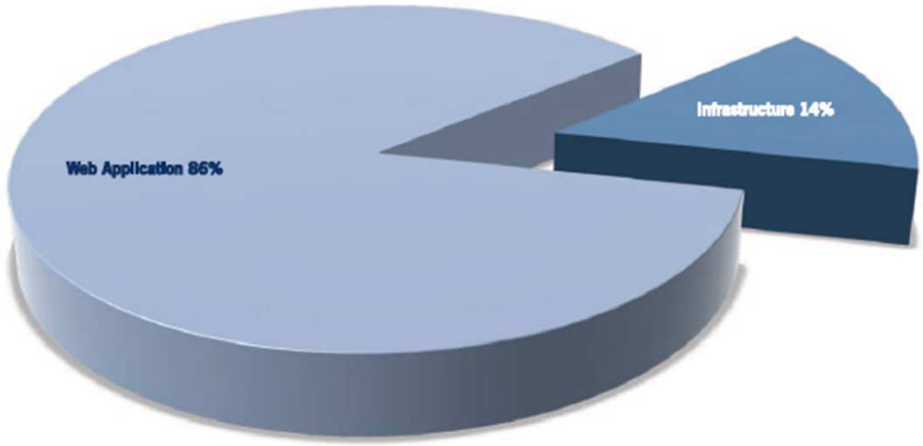


Fuente: Verizon 2010 Data Breach Investigations Report (http://www.verizonbusiness.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf)

1.3. Compromisos

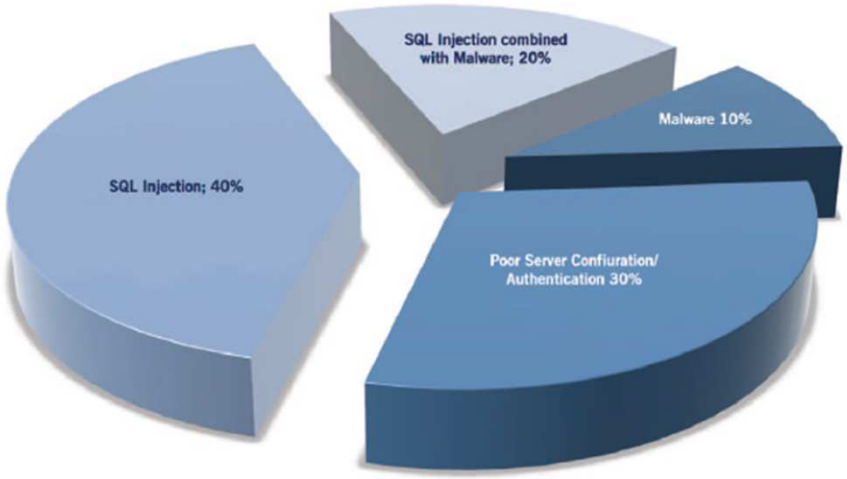
Algunas Estadísticas Más

INFRASTRUCTURE VS APPLICATION



Areas of the compromised systems exploited.

VULNERABILITY LEADING TO DATA COMPROMISE



Vulnerability or exploit used to compromise the system.

Fuente: UK Security Breach Investigations Report 2010 by 7safe (http://www.7safe.com/breach_report/)

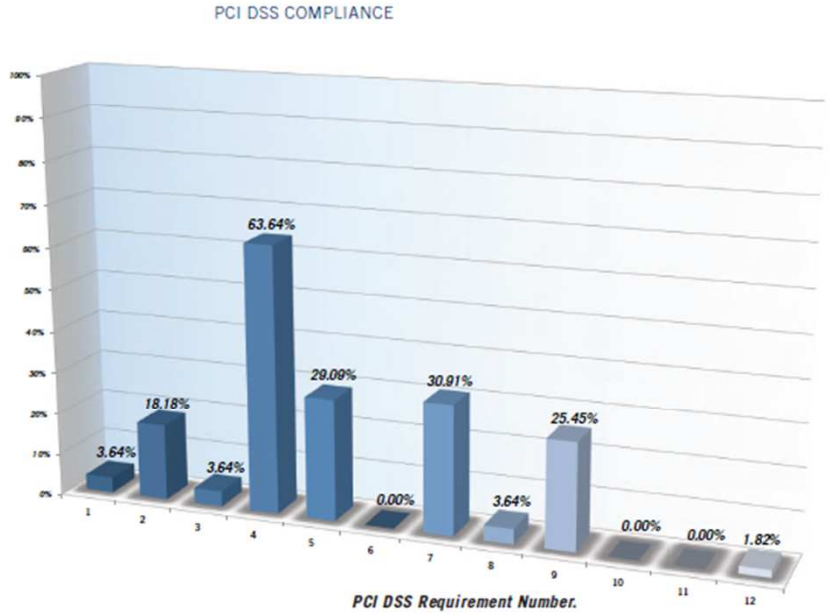
1.3. Compromisos

01

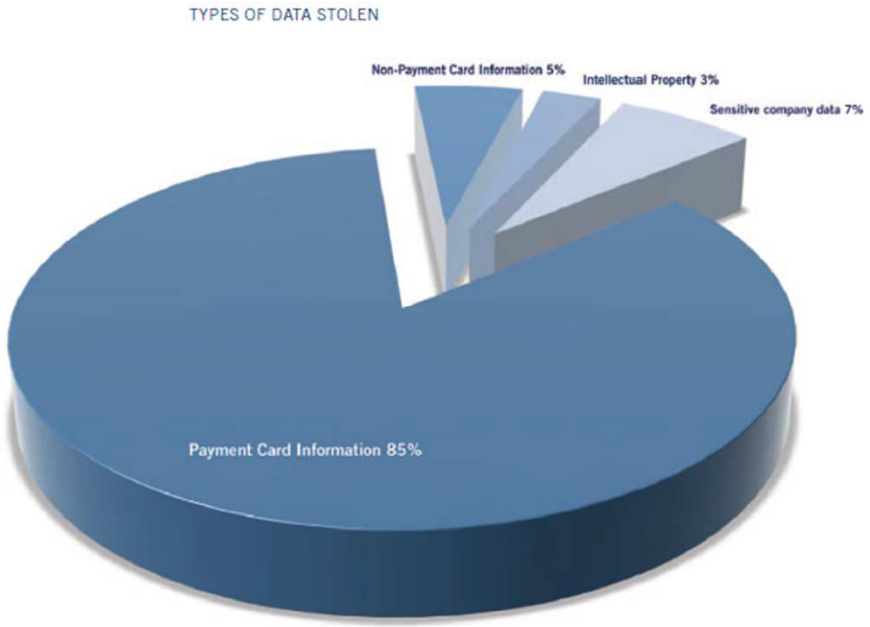
Introducción

1.1. Contenidos
1.2. Amenazas
1.3. Compromisos

Algunas Estadísticas Más



The percentage of individual PCI DSS Requirements met overall by organisations suffering cardholder data breaches.



Types of data stolen from the organisations investigated.

Fuente: UK Security Breach Investigations Report 2010 by 7safe (http://www.7safe.com/breach_report/)

2 PA DSS
[Payment Application Data Security Standard]

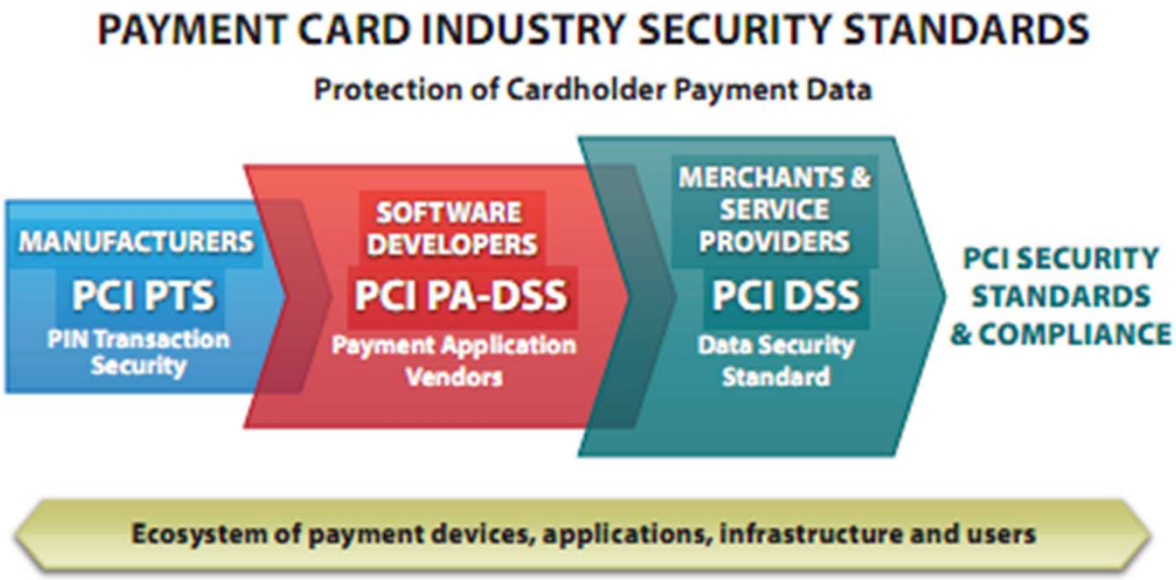
2.1. ¿Qué es?

Introducción a PA DSS

- Estándar de Seguridad -> Aplicaciones de Pago
- Versión Actual 2.0 (En vigor desde Enero 2011)
- Gestionado por el PCI SSC (Payment Card Industry Security Standards Council)

2.1. ¿Qué es?

Estándares Disponibles



- **3 estándares de Seguridad bajo el PCI SSC**
  - Dispositivos PIN → **PCI PTS**
  - Aplicaciones de Pago → **PA-DSS**
  - Cualquier entidad que almacene, procese o transmita detos de tatjetas de pago → **PCI DSS**

2.1. ¿Qué es?

Aplicación de PA DSS

- Empresas de Desarrollo e Integradores de **Aplicaciones de Pago:**
  - Almacenen, procesen o trasmitan datos de tarjeta como parte del proceso de Autorización o Liquidación.
  - Vendidas, distribuidas o licenciadas a terceros.
- **No aplica a:**
  - Desarrollos a medida para un único cliente.
  - Desarrollos propios (in-house)

2.1. ¿Qué es?

02

PA DSS

2.1. ¿Qué es?
2.2. Experiencias

Web PCI SSC

- Lista de Aplicaciones de Pago Validadas
- Profesionales Cualificados para realizar las auditorías (PA-QSAs)

Validated Payment Applications

Search by Company Name, Application Name, or Application Type. last

Company | Search | Clear

Acceptable for New Deployments | Acceptable for Pre-Existing Deployments

New customers may purchase and deploy this product. Revalidation of these applications is required annually

Results: **800** Page: 1 **2** 3

Company	Validation Notes	Deployment Notes	Revalidation Date	Expiry Date
12:51:58 LLC				
MWPOS **Version #:** 1.3.1 **App Type:** POS Face to Face **Target Market:** Restaurants **Reference #:** 10-08.00314.001	Validated According to PA-DSS *(PA-DSS v1.2)*	Acceptable for New Deployments	10 Feb 2011	2 Oct 2013

Description Provided by Vendor: MWPOS is a Linux-based payment application used to provide credit card authorization. The capable of performing card present credit transactions only. The application retains and encrypts (AES 256-bit) the PAN in a SQ

Payment Application QSAs

• Export

Payment Application Qualified Security Assessor (PA-QSA) companies are organizations that have been qualified by the Council to have their employees assess compliance to the PCI PA-DSS standard. Payment Application Qualified Security Assessors are employees of these organizations who have been certified by the Council to validate an entity's adherence to the PCI PA-DSS.

Please note, the PCI Security Standards Council maintains an in-depth program for security companies seeking to be certified as Payment Application Qualified Security Assessors (PA-QSAs), as well as to be re-certified as PA-QSAs each year.

Certification and re-certification indicate only that the applicable PA-QSA has successfully met all PCI Security Standards Council requirements to perfom PCI data security assessments, and the PCI Security Standards Council does not endorse these security solution providers or their business processes or practices.

Although the PCI Security Standards Council strives to ensure that the list of Payment Application Qualified Security Assessors linked to this page is current, the list is updated frequently and the PCI Security Standards Council cannot guaranty that the list is current at all times. Accordingly, each time a client engages a PA-QSA, the client is advised to check this list on a regular basis to ensure that its PA-QSA has successfully maintained its status as a Payment Application Qualified Security Assessor.

Search by Company Name, Place of Business, Servicing Market and Supported Languages.

Company Name | Internet Security Auditors ✓ | Search | Clear

Results: **1** Page: 1

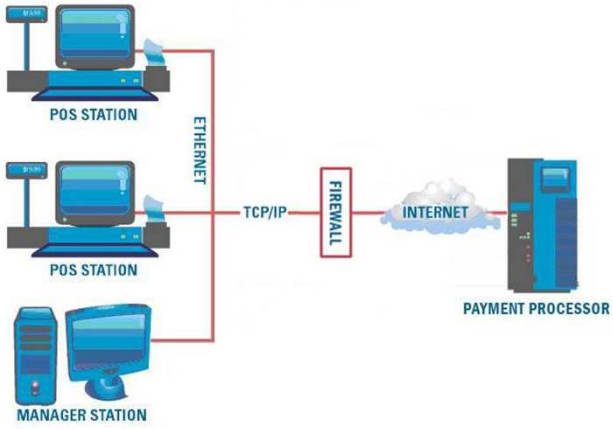
Company	Place of Business	Primary Contact	Servicing Markets	Supported Languages
Internet Security Auditors	Spain	Daniel Fernandez Bleda pcidss@isecauditors.com 34-93-305-13-18	Europe	English, Spanish

2.1. ¿Qué es?

02

PA DSS

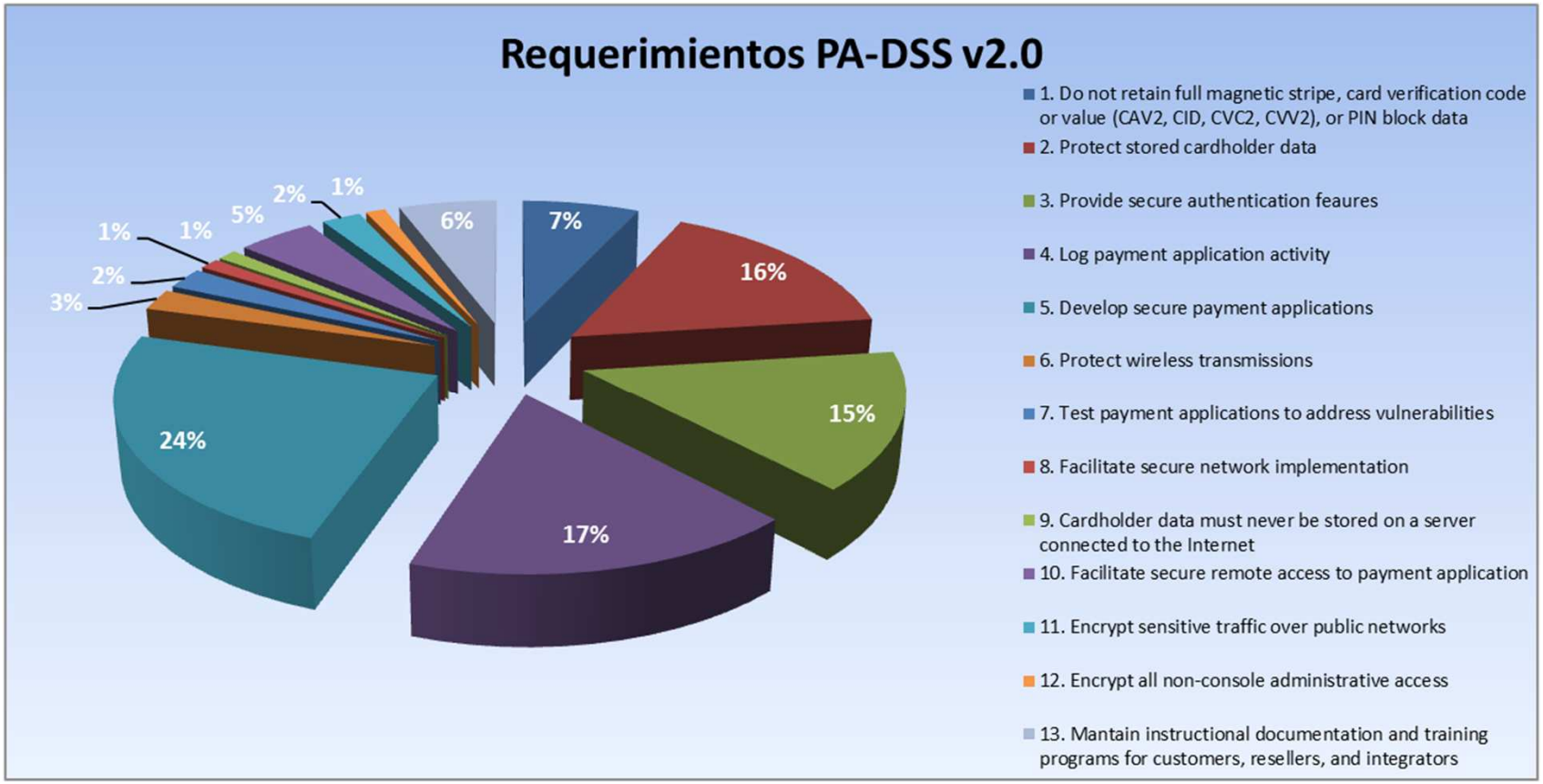
Ejemplos



2.1. ¿Qué es?

Visión Global

La mayor parte de los requerimientos están relacionados con las buenas prácticas en el desarrollo seguro de código



2.1. ¿Qué es?

Resumen Requerimientos

1. Do not retain full magnetic stripe, card verification code or value (CAV2, CID, CVC2, CVV2), or PIN block data

- Almacenamiento Datos confidenciales de Autenticación
- Borrado seguro
- Pruebas Forenses

2. Protect stored cardholder data

- Cifrado, Truncado, One-way hashes…
- Claves de Cifrado
- Visualización de Datos de Tarjeta
- Periodo de retención y eliminación de datos

Resumen Requerimientos

3. Provide secure authentication features

- Cuentas de usuario
- Directivas de contraseñas

4. Log payment application activity

- Registros de auditoria (logs)

5. Develop secure payment applications

- Metodología de desarrollo seguro
- Revisión de código
- Gestión de cambios
- Identificación de servicios, puertos, protocolos estrictamente necesarios.
- Pruebas funcionales y de seguridad

Resumen Requerimientos

6. Protect wireless transmission

- Uso de redes inalámbricas

7. Test payment applications to address vulnerabilities

- Identificación y clasificación de vulnerabilidades
- Diseño e implementación de parches de seguridad
- Control de Integridad y distribución segura

8. Facilitate secure network implementation

- Implementar en redes seguras y PCI DSS compliant

9. Cardholder data must never be stored on a server connected to the Internet

- Almacenamiento de Datos en la red interna

Resumen Requerimientos

10. Facilitate secure remote access to payment application

- Acceso Remoto y Doble factor autenticación
- Distribución de actualizaciones remotamente

11. Encrypt sensitive traffic over public networks

- Envío de datos a través de redes públicas

12. Encrypt all non-console administrative access

- Uso de protocolos seguros para los accesos administrativos

13. Mantain instructional documentation and training programs for customers, resellers, and integrators

- Guía de Implementación y Formación

2.1. ¿Qué es?

3 Hitos

- **Guía de Implementación**
- **Laboratorio de Pruebas**
- **Auditoría de Cumplimiento**

Técnicas de Auditoría

- **Análisis Forenses**
  - Almacenamiento de datos de tarjeta de pago
- **Observación de Procesos**
  - Metodología de desarrollo seguro
  - Revisión de código
  - Distribución de software
- **Pruebas de Integridad**
  - Análisis de Código
  - Reversing
- **Entrevistas**
  - Conocimientos en codificación segura
- **Cumplimiento Técnico**
  - Control de Acceso
  - Criptografía
  - Registro de Auditoría
- **Pruebas Funcionales**

2.2. Experiencias

Deficiencias Comunes

- **Inexistencia de procesos formales**
  - Revisión de Código
  - Pruebas de Seguridad (no únicamente Funcionales)
  - Circuitos de Aprobación Formal
  - Clasificación del riesgo a nuevas vulnerabilidades

- **Equipos de desarrollo pequeños**

- **Controles de Integridad**
  - Software Firmado Digitalmente
  - One-way hashes
  - Software Protectors – packers (Themida, Armadillo…)

2.2. Experiencias

Deficiencias Comunes

- **Control de Excepciones**
  - Errores no controlados pueden provocar el almacenamiento de datos de tarjeta de pago en ubicaciones no autorizadas (coredumps, fichero de paginación, etc.)

- **Poco conocimiento de los estándares**
  - PCI DSS → Laboratorio de Pruebas
    - Antivirus
    - Parches de Seguridad
    - Bastionado
  - PA DSS → Requerimientos de la aplicación
    - Nivel de los registros de auditoría y Centralización de logs
    - Borrado Seguro y Tiempo de Retención
    - Autenticación Segura (usuarios nominales, directivas…)
    - Gestión Claves de Cifrado

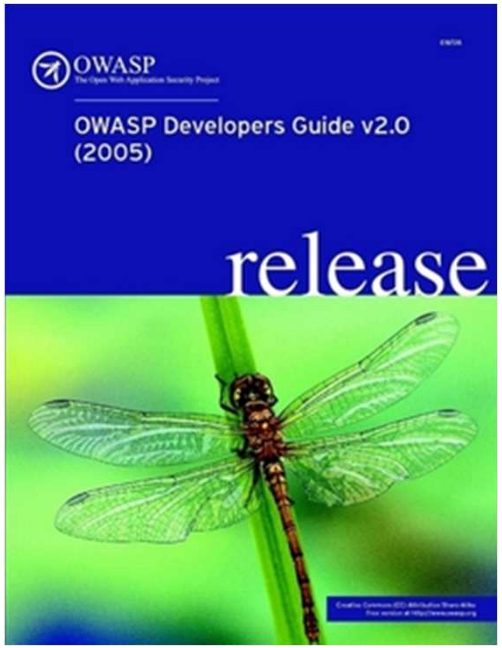
3 Relación con OWASP

Referencia a OWASP

- Tanto en las versiones anteriores de PCI DSS y PA-DSS como en las actuales se hace referencia directa a la OWASP:
  - *Develop applications based on secure coding guidelines. Cover prevention of common coding vulnerabilities in software development processes.*
    - OWASP Guide - Requerimiento 6.5 PCI DSS
    - *OWASP Top 10 – Requerimiento 5.2 PA-DSS*

3. Relación con OWASP

OWASP Development Guide

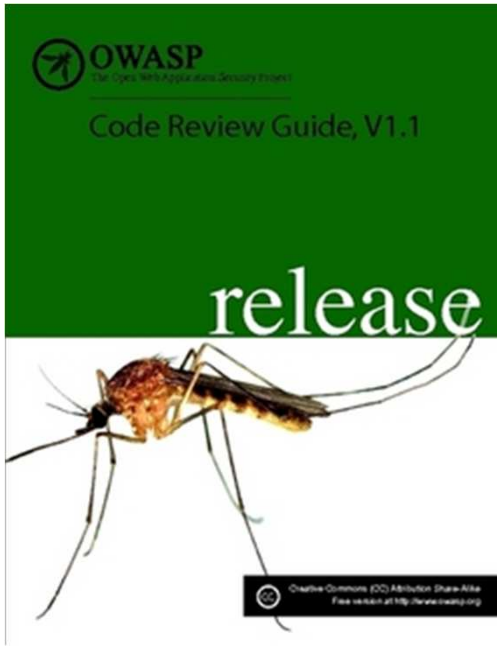


- Inclusión Requerimientos de PCI DSS → PA-DSS.
- **Requerimiento 5 PA-DSS**
  - Develop secure payment applications

Contenidos:

- Arquitectura y Diseño de Seguridad
- Principios de Codificación Segura
- Modelado de Riesgo de Amenaza
- Manejando Pagos en el comercio electrónico

OWASP Code Review Guide



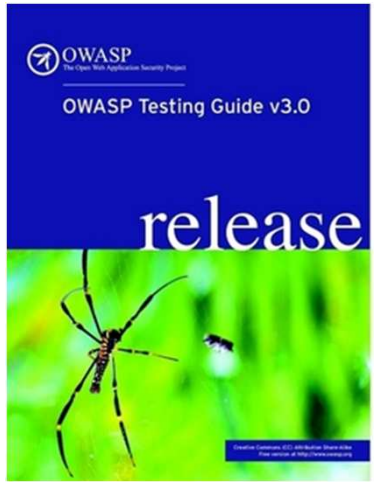
- **Requerimiento 5.1.4 PA-DSS**
  - Review of payment application code prior to release to customers after any significant change, to identify any potential coding vulnerability.
  - Alineado con Requerimiento 5.1.4 PCI DSS

Controles Técnicos a Revisar:

- Authentication
- Authorization
- Session Management
- Input Validation
- Error Handling
- Cryptography
- Data/Input Validation
- Logging/auditing
- Overruns and Overflows
- Code Injections
- Cross-site scripting
- Crosss-Stite Request Forgery
- Race Conditiosn

OWASP Testing Guide

- Primera versión en 2004, próximamente versión 4.
- Qué, Cuando y Cómo?
- **Requerimiento 7 PA-DSS**
  - Test payment applications to address vulnerabilities
- Recomendación de herramientas para las pruebas.

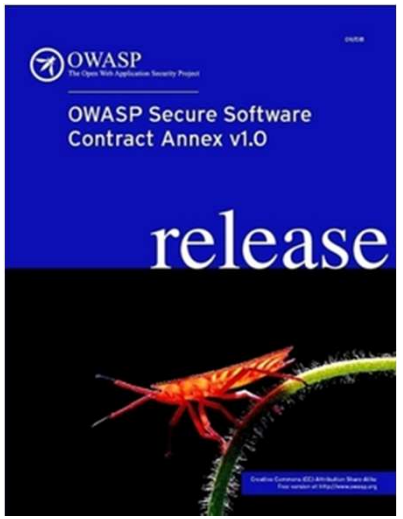


- Information Gathering
- Config. Management Testing
- Business Logic Testing
- Authentication Testing
- Authorization Testing
- Session Management Testing
- Data Validation Testing
- Denial of Service Testing
- Web Services Testing
- Ajax Testing
- Encoded Appendix

3. Relación con OWASP

Múltiples Recursos Disponibles

- OWASP Secure Coding Practices Quick Reference Guide
- OWASP Code Review Top 9
- OWASP Application Security Verification Standard Project
- OWASP Top Ten Project
- OWASP Secure Software Contract Annex
- OWASP Backend Security
- …



4 Conclusiones

4. Conclusiones

Aplicabilidad

- **No todas las aplicaciones de pago son aplicaciones WEB**
  - Clientes pesados para TPV's
- **Procedimientos y guías OWASP siempre se pueden extrapolar a otro tipo de aplicaciones.**
  - Siempre hay excepciones
- **Estándar para aplicaciones de pago**
  - Otras muchas aplicaciones críticas no reguladas
- **Subcontratación de desarrollo de aplicaciones**
  - ¿Qué garantías tenemos en cuanto a seguridad?
  - ¿Qué pasaría si se requirieran auditorías de cumplimiento como PA-DSS?
  - Test de Intrusión, Escaneo de vulnerabilidades…

4. Conclusiones

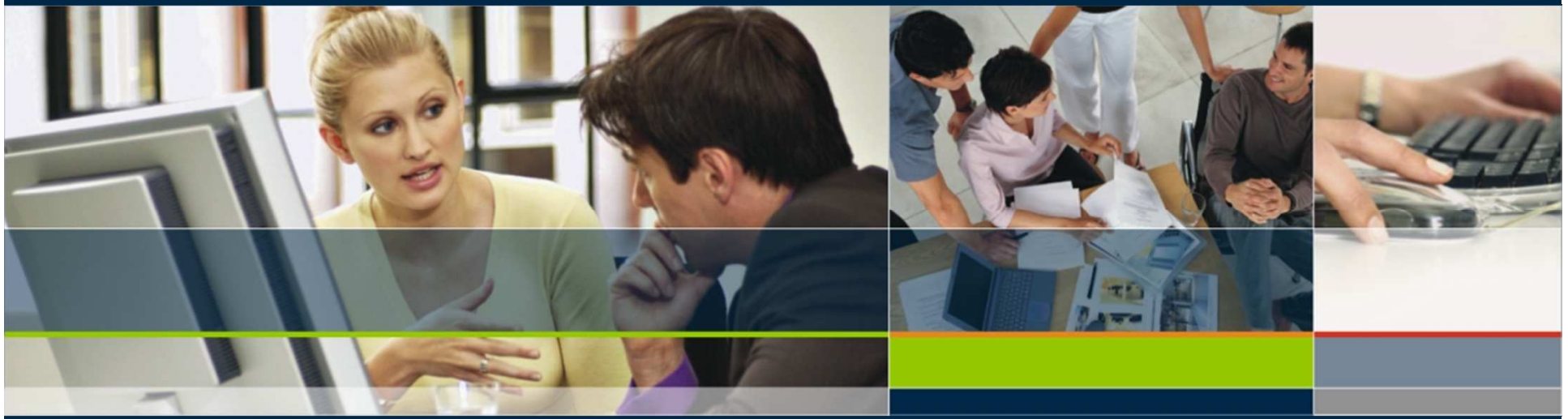
Cuanto Antes Mejor

- Implementar una metodología de desarrollo seguro es sin ningún tipo de duda una **INVERSIÓN SEGURA**
  - Reducción de Riesgos y Costes
  - Aumentar la Confianza de los Clientes
  - Facilidad para la superación de auditorías (PA DSS, PCI DSS, ISO 27001…)
- Recomendable el uso de **Herramientas automatizables**
  - Revisión de Código
  - Pruebas de Seguridad
- Imprescindible **Formación**
  - Entender la problemática y las soluciones
- No es necesario reinventar la rueda, existen múltiples recursos que pueden ayudar a **adaptar los procedimientos existentes**.

OWASP
The Open Web Application Security Project
Spain Chapter

¿PREGUNTAS?

internet
security
auditors



Marc Segarra López
Consultor en Seguridad
CISA, CISSP, PCI QSA, PCI PA QSA, BSI ISO27001 Lead Auditor
msegarra@isecauditors.com

c/ Santander, 101. Edif. A. 2º
E-08030 Barcelona
Tel.: +34 93 305 13 18
Fax: +34 93 278 22 48

Pº de la Castellana, 164-166. Entlo. 1ª
E-28046 Madrid
Tel.: +34 91 788 57 78
Fax: +34 91 788 57 01

www.isecauditors.com

ati
Asociación de Técnicos de Informática

FORTIFY
An HP Company

Su Seguridad es Nuestro Éxito