abertis autopistas

acesa·aucat·aulesa·aumar·avasa·castellana·iberpistas

PCI-DSS
PA-DSS

Análisis del Repositorio de Datos (CardHolder Data Matrix) y Adaptación a la Normativa

Mario Rueda Zambrana.
Responsable de Seguridad de la Información.
Gerencia de Calidad y Desarrollo Operativo.
abertis Autopistas España

Proyecto de adecuación a la normativa PCI-DSS

Índice

1 Marco normativo.

Objeto.

Informar, formar y concienciar sobre:

- La estrategia de seguridad de **abertis Autopistas** con respecto al entorno PCI DSS.
- Definir las líneas generales de actuación para evitar amenazas y reaccionar ante incidentes de seguridad que afecten al entorno PCI DSS.
- Definir el cumplimiento obligatorioi para todos los empleados y colaboradores internos y/o externos.

Sin una política y procedimientos documentados no es posible garantizar la seguridad del entorno y por tanto cumplir con PCI DSS.

1 Marco normativo.

Alineamiento.

- Revisar qué políticas, procedimientos, instrucciones técnicas existentes y adaptarlas a PCI DSS.
- Alinear con otros estándares y normas existentes (ISO 27001, LOPD).
- Documentar todo requerimiento para facilitar su cumplimiento permanentemente.
- Establecer revisiones y actualizaciones periódicas.

1 Marco normativo.

Normativas.

- Control de Acceso.
- Criptografía y Gestión de Claves.
- Gestión de Terceras Partes.
- Roles y Responsabilidades.
- Tratamiento de la Información.
- Monitorización y Auditoría.
- Seguridad de las Plataformas.
- Uso de Recursos Críticos.
- …

1 Marco normativo.

Tabla de correlación.

Permite tener presente la afectación de un cambio en el cumplimiento de los distintos estándares:

- A nivel documental facilitando la integración en el SGI.
- En la implementación de soluciones o ejecución de proyectos.

Normativa PCI DSS abertis Autopistas	Requerimiento PCI DSS	ISO 27001
9.1. Gestión de los Activos de la Información	9.9.1, 12.3.3, 12.3.4, 12.3.7	A.7.1.1, A.7.1.2, A.10.7.1, A.10.7.3, A.11.2.2
9.1.1. Responsabilidad e Inventariado de Activos	9.9.1, 12.3.3, 12.3.4, 12.3.7	A.7.1.1, A.7.1.2, A.10.7.1, A.10.7.3, A.11.2.2
9.2. Tratamiento de datos relativos a las Tarjetas de Pago	3.1, 3.2, 3.2.1, 3.2.2, 3.2.3, 3.3, 3.4, 3.4.1, 4.2	A.10.7.2, A.10.7.3, A.12.3.1, A.15.1.1, A.15.1.4, A.15.2.1, A.15.2.2
9.3. Acceso Lógico a la Información	7.1, 7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.2, 7.2.2, 7.2.3	A.11.1.1, A.11.2.2, A.11.2.4, A.11.6.1
9.4.2. Destrucción Física	9.10, 9.10.1, 9.10.2	A.10.7.2
10.1. Monitorización y Control del Acceso Físico	9.1, 9.1.1, 9.1.2, 9.1.3, 9.2, 9.3, 9.3.1, 9.3.2, 9.3.3, 9.5, 9.7, 9.7.2, 9.8	A.9.1.2, A.9.1.3, A.9.1.4, A.9.1.5, A.9.2.1, A.10.5.1, A.10.7.1, A.10.7.3, A.10.8.1, A.10.8.2, A.10.8.3

2 Repositorio de datos.

Propósito:

- Identificar/inventariar todos los posible repositorios de datos de titulares de tarjetas de pago.

Problemáticas:

- Aplicaciones satélites desarrolladas
- por los propios usuarios.
- Filosofía opuesta en el desarrollo y las
- bases de datos, **cuántos más datos mejor**!
- Múltiples departamentos, usuarios, aplicaciones y canales de transmisión de datos.

2 Repositorio de datos.

Conceptos básicos.

- Almacenar la **menor cantidad de datos que sea posible**. La información que se almacene debe seguir las **políticas de retención y eliminación**, y estar inventariada adecuadamente.
- Aquellos **datos de tarjeta** que sean almacenados, **deberán permanecer ilegibles** mediante mecanismos como el **cifrado** o el **truncado**.
- Siempre que deban **visualizarse** datos de tarjetas mediante alguna aplicación, solo deberán mostrarse **los primeros 4 y últimos 6 dígitos del PAN**.

2 Repositorio de datos.

Conceptos básicos.

- Se **prohíbe** el **almacenamiento de datos sensibles** tras el proceso de autorización, **aunque estén cifrados** y en cualquier tipo de soporte de almacenamiento

		Data Element	Storage Permitted	Render Stored Account Data Unreadable per Requirement 3.4
Account Data	Cardholder Data	Primary Account Number (PAN)	Yes	Yes
		Cardholder Name	Yes	No
		Service Code	Yes	No
		Expiration Date	Yes	No
	Sensitive Authentication Data[1]	Full Magnetic Stripe Data[2]	No	Cannot store per Requirement 3.2
		CAV2/CVC2/CVV2/CID	No	Cannot store per Requirement 3.2
		PIN/PIN Block	No	Cannot store per Requirement 3.2

2 Repositorio de datos.

Conceptos básicos.

- Protocolos de transmisión como telnet, HTTP o FTP no son válidos.
- Los requerimientos de almacenamiento afectan a cualquier tipo de soporte (papel, cintas, DVD's…).
- El cifrado de los datos implica una **gestión de claves de cifrado**, para la que se requieren ciertos **requerimientos** referentes a la fortaleza de las claves, cambio periódico, su almacenamiento y distribución, revocado y destrucción, así como responsabilidades para su custodia y protección.

2 Repositorio de datos.

Acciones realizadas.

1. **Identificar todos los sistemas que almacenan, procesan o transmiten datos de tarjeta**.
   - Analizar y entender los procesos que obtienen datos de titulares de tarjeta de pago.
   - Entrevistas con los responsables de los departamentos.
   - Análisis de los usos de los datos de tarjeta.
   - Datos compartidos entre procesos y/o departamentos.
   - Ejecución de herramientas y scripts para la localización de datos “desconocidos”.

2 Repositorio de datos.

Acciones realizadas.

2. **Análisis individual de cada repositorio identificado**:
   - Origen (Cómo se han obtenido los datos).
   - Datos obtenidos (PAN, Service Code, Fecha Caducidad…)
   - Función y Justificación de negocio.
   - Periodo de retención.
   - Control de acceso a datos.
   - Transmisión de datos entre procesos.
   - Método de borrado utilizado.
   - Formato en el que se almacenan y medidas de protección aplicadas (tipo de cifrado…).
   - Dispositivos, Sistemas y Aplicaciones relacionadas.

2 Repositorio de datos.

Acciones realizadas.

2. Análisis individual de cada repositorio identificado:

- Dando como resultado la Matriz de Datos.

Almacenamiento		
Datos de tarjeta almacenados	**Ubicación de información almacenada**	**Controles de almacenamiento**
☐ Personal Account Number (PAN) ☐ CVV2 ☐ Fechar de Expiración ☐ Datar personalar del titular de la tarjeta ☐ Banda Magnética ☐ Código de servicio ☐ PIN / PINBLOCK	☐ Barer de datar internar ☐ Ficherar propiar de la aplicación ☐ Ficherar de registra (logr) de la aplicación ☐ Ficherar de depuración de la aplicación ☐ Otra Ubicación - Describir:	☐ Cifrada ☐ Hash ☐ Truncamienta ☐ Enmarcaramienta ☐ Ura de Takenr ☐ Texta clara

Control de Acceso		Hardening	Desarrollo	RETENCIÓN	LOGS	Owner
¿Cuál es el control de acceso implementado para ingresar a los servicios del aplicativo (usuario interno, usuario propio del aplicativo, etc.)?	**¿Cada uno de los usuarios del aplicativo es único o existen cuentas compartidas?**	**Guía de hardening aplicada**	**Desarrollo del aplicativo**	**Periodo de retención de datos de tarjetas**	**Controles de gestión de log implementados?**	**Persona de contacto (responsable)**
☐ Urusria interna ☐ Urusria Propia del Aplicativo ☐ Otra tipa de urusria. Describir: ☐ No hay interacción con urusriar			☐ Dararralla interna ☐ Dararralla interna (rub-cantratada) ☐ Dararralla externa			

que permite :

- **afrontar una auditoría.**
- **tener control sobre los datos.**
- **estudiar acciones para acotar el entorno.**

2 Repositorio de datos.

Acciones realizadas.

3. Estudio de la necesidad:
    - Una vez identificados todos los repositorios de datos, es posible determinar la necesidad de su existencia, valorando:
        - Eliminación del fichero o campo en la aplicación/BBDD.
        - Integración de funcionalidades en menos aplicaciones.
        - Uso de técnicas para reducir el alcance como:
            - Truncado de datos.
            - Enmascaramiento.
            - Tokenización.
        - Cambios en los procesos de negocio, para eliminar la necesidad de trabajar con datos de tarjeta.
        - Uso de protocolos de transmisión distintos.

2 Repositorio de datos.

Beneficios obtenidos.

- **Concienciación** debido a las reuniones y consultas realizadas.
- **Eliminación** de aplicaciones satélites, listados y repositorios individuales.
- **Mejoras en el desarrollo**, al incorporar en el proceso decisiones críticas como el enmascaramiento de datos, estudiar la necesidad de almacenar datos de tarjeta, etc.
- Estudio de los tiempos y justificaciones de **retención** de datos.
- Minimización de riesgos
  - Saber con determinación donde hay datos críticos.
  - A medida que crecen los repositorios de datos, los riesgos son cada vez mayores.
  - A mayor cantidad de datos comprometidos, mayores son las consecuencias del compromiso (multas, penalizaciones).
  - Limitar el uso de tecnologías de mensajería para el tratamiento de datos de tarjeta de pago.
  - Menor acceso a datos, y más controlado.

2 Repositorio de datos.

Recomendaciones.

- Reducir los repositorios de datos al mínimo realmente imprescindible.
- **Si no lo necesitas, no lo almacenes!**
- Impedir la extracción de datos mediante listados, documentos ofimáticos, etc., a través de las aplicaciones corporativas.
- Lanzar **procesos automáticos** periódicamente para el **descubrimiento** de **datos** de tarjeta **no autorizados**.
  - Expresiones regulares.
  - Formula de Luhn.

¿PREGUNTAS?

MUCHAS GRACIAS

Análisis del Repositorio de Datos (CardHolder Data Matrix) y Adaptación a la Normativa

Mario Rueda Zambrana.
Responsable de Seguridad de la Información.
Gerencia de Calidad y Desarrollo Operativo.
abertis Autopistas España