internet security auditors

INFORMÁTICA El Corte Inglés

PCI DSS – PA DSS

Sinergias entre PCI DSS y PA DSS: cómo sacar partido de PA DSS para facilitar el Cumplimiento y Certificación PCI DSS.

2ª JORNADA SOBRE SEGURIDAD EN MEDIOS DE PAGO

JOSÉ GARCÍA GONZÁLEZ
PCI Manager/Consultor CEX de MM. PP.
Informática el Corte Inglés (IECI)

conexflow

INDICE

- PCI DSS y PA DSS.
- Cómo se interrelacionan.
- Qué queda cubierto con PA DSS.
- Hacia dónde hay que ir.
- Estructura de la norma PCI DSS.
- Por dónde empezar.
- Cómo abordar el estándar.

PA DSS Y PCI DSS

PA DSS (Payment Aplications Data Security Standard)

- Desarrollos de software que almacenen, procesen o transmitan datos de titulares de tarjeta bajo licencia.
- La aplicación recibe datos de titulares de tarjeta de un datáfono u otro dispositivo y comienza la transacción.
- La aplicación funciona bajo entornos PCI DSS.
- PCI SSC no envía correos sobre la actualización de la norma.
- En Octubre se ha presentado la versión 2.0.

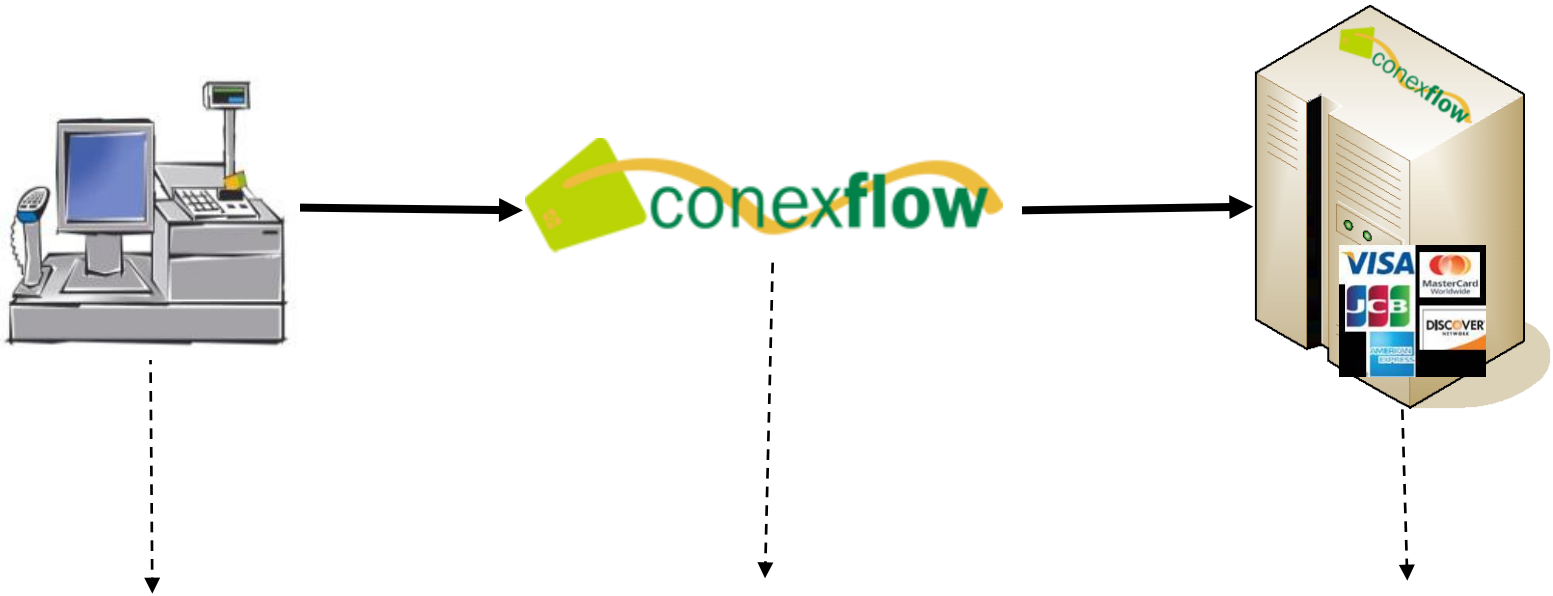
PA DSS Y PCI DSS (II)

PCI DSS (Payment Card Industry Data Security Estándar):

- Define medidas de protección para la infraestructura que interviene en el tratamiento, procesamiento, transmisión y almacenamiento de información de tarjetas de pago.
- El objetivo de la norma es prevenir el fraude y cualquier tipo de acciones malintencionadas sobre los datos de titulares de tarjeta.
- Cumplir con PCI DSS implica un proceso continuo de implantación y gestión de controles de seguridad que minimicen al máximo los riesgos potenciales de pérdida de datos de titulares de tarjeta.
- PCI SSC no envía correos sobre la actualización de la norma.

COMO SE INTERRELACIONAN (I)

- El proceso simplificado …



El usuario hace una compra

La aplicación almacena, procesa, transmite los datos de tarjeta

Los sistemas del comercio o del proveedor de servicio procesan, almacenan o trasmiten los datos de tarjeta

COMO SE INTERRELACIONAN (II)

- PA DSS está formada por requerimientos de PCI DSS reestructurados y orientados al desarrollo seguro de aplicaciones (exceptuando los requerimientos 7.2 y 13).
- Desarrollar una aplicación para luego certificarla por PA DSS implica conocer la norma PCI DS.
- De hecho, las máquinas donde se prueba la aplicación PA DSS deben cumplir con PCI DSS en relación a:
  - Bastionado de las máquinas.
  - Política de cuentas de usuario y contraseñas.
  - Configuración segura de las comunicaciones.
  - Correlación de logs.
  - Desarrollo seguro de aplicaciones.

QUE QUEDA CUBIERTO CON PA DSS (I)

PA DSS v2.0	
Apartados	**Requerimientos**
Construir y Mantener una Red Segura	1. No retenga toda la banda magnética, el código de validación de la tarjeta ni el valor (CAV2, CID, CVC2, CVV2), ni los datos de bloqueo del PIN. 2. Proteja los datos del titular de la tarjeta que fueron almacenados. 3. Provea las funciones de autenticación segura. 4. Registre la actividad de la aplicación de pago. 5. Desarrolle aplicaciones de pago seguras. 6. Proteja las transmisiones inalámbricas. 7. Pruebe las aplicaciones de pago para tratar las vulnerabilidades. 8. Facilite la implementación de una red segura. 9. Los datos de titulares de tarjetas nunca se deben almacenar en un servidor conectado a Internet. 10. Facilite actualizaciones de software remotas y seguras. 11. Cifre el tráfico sensitivo de las redes públicas. 12. Cifre el acceso administrativo que no sea de consola. 13. Mantenga la documentación instructiva y los programas de capacitación para clientes, revendedores e integradores.
ANEXO A	Resumen de contenidos para la guía de implementación de las PA DSS.
ANEXO B	Confirmación de la configuración específica del laboratorio de pruebas de la evaluación de las PA DSS.

QUE QUEDA CUBIERTO CON PA DSS (II)

- Si bien es cierto que PA DSS aplica a un número menor de departamentos y procesos, el trabajo realizado por IECISA cubre los siguientes apartados de PCI DSS:
  - Desarrollo de software.
  - Gestión de parches y actualizaciones.
  - Almacenamiento y destrucción de datos de tarjeta.
  - Gestión de claves criptográficas.
  - Gestión de cambios.
  - Política de usuarios y contraseñas.

HACIA DONDE HAY QUE IR

- En el negocio de medios de pago, IECISA tiene un doble papel como proveedor de servicios:
  - Como desarrollador de software, desarrollar una aplicación segura.
  - Como valor añadido a la aplicación, IECISA ofrece a sus clientes la posibilidad de administrar y alojar la aplicación Conexflow en su Centro de Operaciones y Redes, permitiéndoles desentenderse en gran medida de PCI DSS.
- Este doble papel empuja a IECISA a obtener la certificación PCI DSS como “Shared Hosting Provider”.

CORE
CENTRO DE OPERACIONES Y REDES

ESTRUCTURA DE LA NORMA PCI DSS

PCI DSS v1.2	
Principios	**Requerimientos**
Construir y Mantener una Red Segura	1. Instalar y mantener un cortafuegos y su configuración para proteger la información de tarjetas. 2. No emplear parámetros de seguridad y usuarios del sistema por defecto.
Proteger los Datos de Tarjetas	3. Proteger los datos almacenados de tarjetas. 4. Cifrar las transmisiones de datos de tarjetas en redes abiertas o públicas.
Mantener un Programa de Gestión de Vulnerabilidades	5. Usar y actualizar regularmente software antivirus. 6. Desarrollar y mantener de forma segura sistemas y aplicaciones.
Implementar Medidas de Control de Acceso	7. Restringir el acceso a la información de tarjetas según la premisa “need–to–know”. 8. Asignar un único ID a cada persona con acceso a computadores. 9. Restringir el acceso físico a la información de tarjetas.
Monitorizar y Testear Regularmente las Redes	10. Auditar y monitorizar todos los accesos a los recursos de red y datos de tarjetas. 11. Testear de forma regular la seguridad de los sistemas y procesos.
Mantener una Política de Seguridad de la Información	12. Mantener una política que gestione la seguridad de la información.
ANEXO A	Requisitos PCI DSS adicionales para proveedores de hosting compartido.

POR DONDE EMPEZAR (I)

- Eliminar los datos prohibidos:
  - El contenido de la banda magnética (p.e.: Pista1, Pista2), CVV2 y PIN BLOCKs no deben retenerse tras la autorización de la transacción.
  - En este sentido, Conexflow v4.0 no almacena los datos sensibles de la tarjeta.

		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

POR DONDE EMPEZAR (II)

- Eliminar los datos de tarjeta no necesarios:
  - Almacenar la menor cantidad de datos que sea posible, en el menor número de ubicaciones posibles, de forma ilegible.
  - La información que se almacene debe seguir las políticas de retención y eliminación, y estar inventariada → Matriz de Datos de Tarjeta.
  - Esto también afecta al papel.

SI NO ES NECESARIO ALMACENAR EL PAN MEJOR ELIMINARLO

POR DONDE EMPEZAR (III)

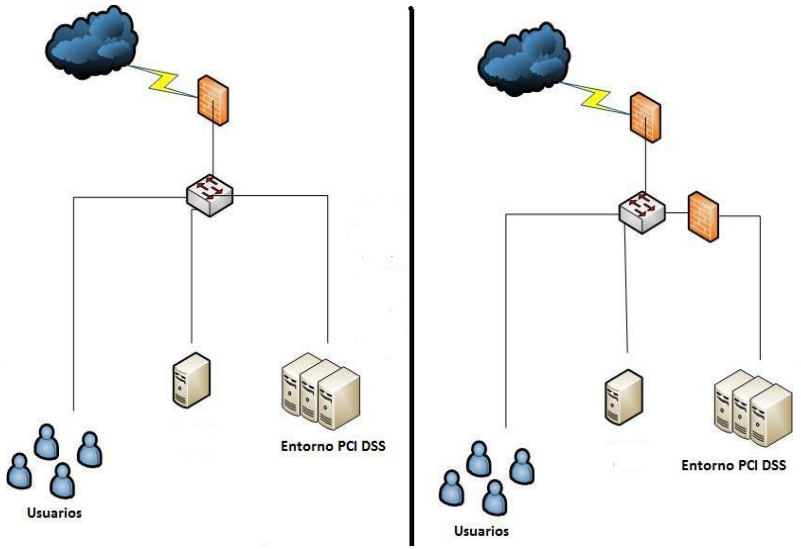
- Proteger los datos de tarjeta utilizando aplicaciones seguras de pago:
  - Utilizar aplicaciones certificadas por PA DSS garantiza que:
    - La aplicación ha sido desarrollada con una metodología de desarrollo seguro del software.
    - Cumple con todas las exigencias de los fabricantes de tarjeta.
    - Una preocupación menos para la empresa de cara a la certificación.

POR DONDE EMPEZAR (IV)

- Proteger los sistemas que procesan, almacenan o transmiten los datos de tarjeta de acuerdo al estándar PCI DSS v2.0:
  - Establecer una Política de Seguridad.
  - Cumplir con el estándar.
  - Formar a los empleados.
  - Validar el cumplimiento en los sistemas donde se almacena, procesa o trasmiten datos de titulares de tarjetas de pago.

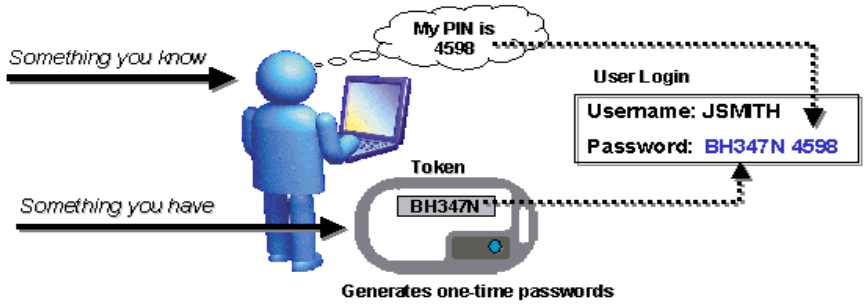
POR DONDE EMPEZAR (V)

- Segmentación de Red:
  - Permite reducir el alcance, costes y envergadura de la auditoría.
  - Sin una segmentación adecuada, toda la red y sistemas de IECISA o del cliente deberían cumplir con PCI DSS.
  - Instalar protección perimetral.
  - ¿Cómo segmentar la red?
    - Utilizando dispositivos que aíslen eficazmente los datos de tarjeta del resto de la red: cortafuegos, equipos de red, listas de control de acceso robustas …



POR DONDE EMPEZAR (VI)

- Restringir el acceso al entorno PCI DSS:
  - **Control de Acceso Lógico:** Definir matriz de privilegios por cada componente de sistema, esto servirá como procedimiento para garantizar el acceso según el need-to-know e incluir qué puesto de trabajo tiene acceso y en qué condiciones.



  - **Control de Acceso Físico:** Las áreas donde se procesan (CPD) y almacenan los datos de tarjeta deben tener controles de acceso físico y cámaras de seguridad que monitoricen el acceso a estas instalaciones.

POR DONDE EMPEZAR (VII)

- Configuración Segura de Equipos:
  - Elaborar guías de bastionado para todos los componentes del sistema.
  - Establecer un proceso de actualización de parches.
  - Establecer procesos de detección de nuevas vulnerabilidades.
  - Instalar antivirus en servidores y equipos de usuarios
- Monitorización de los Eventos de Seguridad:
  - Instalar una plataforma de correlación de logs que rastree cualquier acción que ocurra dentro del entorno PCI DSS.

POR DONDE EMPEZAR (VIII)

- Gestión de Copias de Seguridad:
  - Las copias de seguridad del entorno PCI DSS deben ser protegidas de accesos no deseados y de amenazas medioambientales.
- Gestión de las Comunicaciones:
  - Utilizar protocolos de comunicación seguros cuando los datos viajen por redes no confiables.
  - Restringir al máximo el tráfico entrante/saliente del entorno PCI DSS.
- Desarrollo Seguro de Aplicaciones:
  - Conexflow.

POR DONDE EMPEZAR (IX)

- Gestión de la Seguridad:
  - Establecer una Política de Seguridad que cubra todos los requerimientos de PCI DSS.
  - Realizar un Análisis de Riesgos todos los años.
  - Elaborar procedimientos que regulen la relación con los proveedores de servicios del entorno PCI DSS.
  - Establecer procesos de detección y respuesta ante incidentes de seguridad relacionados con los datos de tarjeta.
  - Diseñar un Plan de Formación y Concienciación para el personal que trabaje en el entorno PCI DSS.
  - Definir los roles y responsabilidades del personal que trabaja en el entorno PCI DSS.
  - Establecer procedimientos de seguridad de operativa diaria.
  - Establecer un procedimiento de gestión de cambios.

POR DONDE EMPEZAR (X)

- Auditorías y Revisiones Periódicas:
  - Pasar la auditoría anual de certificación/recertificación.
  - Realizar los escaneos de vulnerabilidades internos y externos (los externos sólo podrán ser realizados por ASVs) trimestrales o tras un cambio significativo en el entorno PCI DSS.
  - Escaneos wifi trimestrales.
  - Realizar un test de penetración interno y externo anualmente o tras un cambio significativo en el entorno PCI DSS.
  - Revisar la Política de Seguridad y procedimientos anualmente.
  - Realizar un inventario de soportes extraíbles anualmente.
  - Realizar una vez al año un Análisis de Riesgos.
  - Revisión semestral de las reglas de los firewalls.
  - Revisar el estado de las cuentas de usuarios trimestralmente.
  - Revisión diaria de los logs.

EN RESUMEN

- PA DSS facilita la implantación de PCI DSS pero no lo garantiza.
- Asegura que los datos son procesados y almacenados en los sistemas de forma segura.
- Abordar la certificación PCI DSS exige un esfuerzo grande y mayor número de recursos.
- Para implantar PCI DSS es necesario el apoyo de la dirección.

PCI + PA-DSS Compliance
Security You Can Trust

internet security auditors

INFORMÁTICA El Corte Inglés

PCI DSS – PA DSS

PREGUNTAS

2ª JORNADA SOBRE SEGURIDAD EN MEDIOS DE PAGO

JOSÉ GARCÍA GONZÁLEZ
PCI Manager/Consultor CEX de MM. PP.
Informática el Corte Inglés (IECI)

conexflow