internet security auditors

cajaRioja

2ª JORNADA SOBRE SEGURIDAD

EN MEDIOS DE PAGO

PCI DSS
PA DSS

REQUISITOS Y PASOS PARA AVANZAR EN EL CUMPLIMIENTO PCI

CARLOS PRIETO LEZAUN
RESPONSABLE DE SEGURIDAD
CAJA RIOJA

miércoles, 10 de Noviembre de 2010
Hotel Holiday Inn (Madrid)

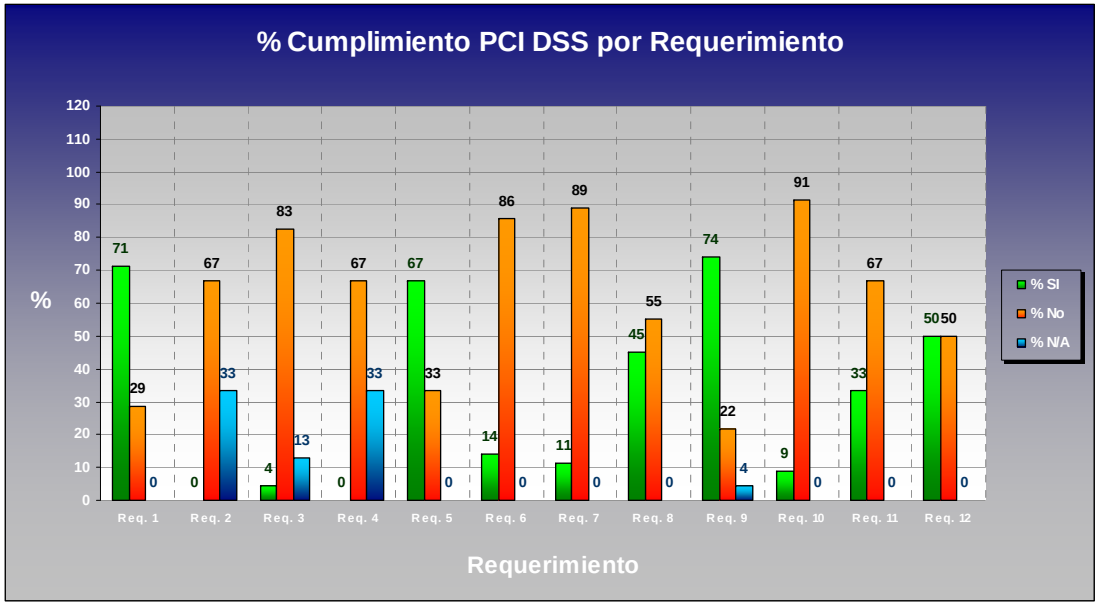
Concienciación

Apoyo de la Dirección: La Dirección debe dar la importancia que tiene al cumplimiento PCI, mostrando su apoyo con un mensaje claro a todos los agentes internos y externos para que trabajen en la línea necesaria para alcanzar el cumplimiento.

En nuestro caso tenemos implementado un SGSI y en las reuniones del Comité de Seguridad, entre otro temas, se sigue la evolución del cumplimiento PCI.

Foto Inicial

Hay que saber cómo estamos. ¿Cuál es nuestro alcance?, ¿dónde están los datos susceptibles de cumplimiento PCI?, ¿en qué servidores?, ¿por qué líneas de comunicaciones circulan?, ¿quién accede a ellos?.....



Para ello nuestra experiencia nos demostró que es indispensable una consultoría externa por una empresa experta en cumplimiento PCI. Con la ayuda del QSA conseguimos una foto de partida que nos permitió platearnos los siguientes pasos sin que éstos fueran a ciegas o descoordinados.

Líder y Plan Inicial

Una vez conocida la situación real de partida, es **imprescindible asignar un responsable que lidere y coordine las acciones necesarias**. Para ello este responsable con la colaboración de personas involucradas directamente en el cumplimiento PCI (medios de pago, cajeros, comunicaciones, sistemas medios) elaborará un plan que será validado por la Dirección.

En Caja Rioja el Comité de Seguridad designó al responsable y le encomendó la elaboración del plan. El plan elaborado, contando con la opinión y experiencia de otros afectados, fue presentado al Comité de Seguridad para su aceptación. Paralelamente existen reuniones de coordinación más operativas.

Seguimiento y Vigilancia

El plan debe seguirse, analizar sus desviaciones, solucionar los problemas que surjan, y replanificar si fuera necesario. Pero tan importante como el plan es estar vigilantes, concienciar e implementar mecanismos de control para que nuevos productos, desarrollos, compra de equipamiento, etc.. no provoque un nuevo incumplimiento de PCI.

¿QSA o ISA?

En nuestro caso muchos de los desarrollos están en ATCA que cumple PCI. A nivel interno se ha realizado una concienciación al departamento de Organización y Sistemas que interviene en las decisiones de compras, desarrollos, etc.. Para que se tenga en cuenta la seguridad y los cumplimientos regulatorios o legales (PCI, LOPD, MIFID, etc..) en los requisitos.

Requerimientos

Requerimientos del programa

- **Construir y mantener una red segura**
  - Req. 1: Instalar y mantener un firewall
  - Req. 2: No usar passwords ni otros parámetros de sistema definidos por el fabricante
- **Proteger los datos del titular**
  - Req. 3: Proteger datos almacenados
  - Req. 4: Encriptar la transmisión de datos de titulares a través de redes abiertas
- **Llevar a cabo un programa de gestión de la vulnerabilidad**
  - Req. 5: Usar antivirus y actualizarlo regularmente
  - Req. 6: Desarrollar y mantener aplicaciones y sistemas seguros
- **Implementar medidas robustas de control de acceso**
  - Req. 7: Restringir el acceso a los datos de titulares sólo cuando sea necesario
  - Req. 8: Asignar identificadores únicos
  - Req. 9: Restringir el acceso físico a los datos de titulares
- **Monitorizar regularmente las redes**
  - Req. 10: Tracear y monitorizar todos los accesos a los datos de titulares
  - Req. 11: Probar regularmente todos los sistemas y procesos de seguridad
- **Mantener una política de seguridad**
  - Req. 12: mantener una política de seguridad

220 Sub-requerimientos

Problemas y soluciones

Cajeros

Router y Switch

Bases de datos

Procedimientos y documentación

Auditoría

Relación con terceros

Redes WIFI

¿Medidas compensatorias convencerán al QSA?

Muchas Gracias !!!

Carlos Prieto Lezaun

cprieto@cajarioja.es

cprietolezaun@yahoo.es

internet security auditors

cajaRioja

2ª JORNADA SOBRE SEGURIDAD

EN MEDIOS DE PAGO

PCI DSS
PA DSS

PREGUNTAS

miércoles, 10 de Noviembre de 2010

Hotel Holiday Inn (Madrid)