internet security auditors

Caixa Penedès

2ª JORNADA SOBRE SEGURIDAD

EN MEDIOS DE PAGO

PCI DSS
PA DSS

MARCO NORMATIVO. SEPARACIÓN DE FUNCIONES ENTRE CAIXA PENEDÈS Y SERINCEP

JORDI SOLÀ SEBASTIÀ
RESP. DPTO.SEGURIDAD LÓGICA
CAIXA PENEDÈS

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

Estructura organizativa en materia de Seg. Lógica

Año 2002:

- Área de Informática:
  - Dpto. de Desarrollo
  - Dpto. de Explotación
  - **Dpto. de Seguridad y Calidad Interna**
  - Dpto. de Sistemas y Nuevas Tecnologías

Año 2008:

- Área de Seguridad:
  - Dpto. de Prevención del Fraude
  - Dpto. de Seguridad Física
  - **Dpto. de Seguridad Lógica**

Equipos implicados en materia de seguridad lógica

- Dpto. de Seguridad Lógica (Área de Seguridad).
- Comité de Seguridad de la Información:
  - Jefe del Área de Seguridad
  - Jefe del Área de Informática
  - Jefe del Dpto. de Auditoría Interna
  - Jefe del Dpto. de Explotación Informática
  - Jefe del Dpto. de Racionalización y Métodos (Área Organización)
  - Jefe del Dpto. de Seguridad Lógica
  - Resp. de empresas del Grupo (Serincep, Grupo Asegurador)
- SerinCEP
- Otros departamentos (Formación, RRHH, Asesoría Jurídica, ...)
- Proveedores externos.

Cumplimiento normativa PCI DSS

- Durante los años 2008 y 2009, se han realizado por parte del dpto. de Seguridad Lógica con los consultores de la empresa Internet Security Auditors, y con el soporte de los Dptos. de Medios de Pago y, Análisis y Desarrollo Informático, las siguientes **fases del proyecto:**

  - **Fase I: Análisis de Situación actual de cumplimiento.**
  - **Fase II: Evaluación del Riesgo.**
  - **Fase III: Programa para el cumplimiento.**

- Actualmente se está trabajando, junto con los consultores, en la **Fase IV- Implantación de Requerimientos**: Marco normativo, Gestión de cortafuegos y routers, Configuración segura de equipos, Gestión de actualizaciones de seguridad, Gestión de medios de almacenaje, Programa de auditorías, Gestión de incidentes de seguridad, Gestión de la seguridad con proveedores, …

Política de Seguridad de la Información (pre PCI DSS)

La política de seguridad de la información está formada por 10 documentos.

El primer documento es el de '**Política de Seguridad de la Información**' como un documento de alto nivel, que se sustenta en otros documentos que tratan aspectos específicos de la seguridad de la información:

- ✓ Código de conducta.
- ✓ Política de acceso remoto.
- ✓ Política de Internet.
- ✓ Política de correo electrónico.
- ✓ Política de contraseñas.
- ✓ Política de clasificación de la información.
- ✓ Política de dispositivos portátiles.
- ✓ Política de seguridad física.
- ✓ Política con empresas externas.

Política de Seguridad de la Información (post PCI DSS)

Actualmente está siendo revisada, modificada y ampliada debido a PCI DSS:

- Política de Seguridad de la Información
- Código de conducta.
- Política de acceso remoto.
- Política de Internet.
- Política de correo electrónico.
- Política de contraseñas.
- Política de clasificación *y tratamiento* de la información.
- Política de dispositivos portátiles.
- Política de seguridad física *y lógica*.
- Política con empresas externas.
- *Política de actualizaciones de seguridad y desarrollo seguro.*
- *Política de configuración y endurecimiento de los sistemas informacionales.*
- *Política de criptografía y claves criptográficas.*
- *Política de formación i contratación.*
- *Política de monitorización y auditoría de los sistemas de información.*

Documentación generada - I

Gestión de cortafuegos y routers

- Procedimiento gestión de componentes de red en entornos PCI DSS
- 487-003-GS - Cisco IOS.
- 487-003-GS - Cortafuegos Cisco (ASA-FWSM-PIX).

Definición del Estándar de Configuración Segura de Equipos

- Guía de seguridad de servidores i servicios Windows 2008 amb IIS 7.
- Guía de seguridad de servidores i servicios HPUX 11i.
- Guía de seguridad de servidores i servicios Red Had Enterprise Linux 5.0 i 5.1 .
- Política de auditoría en entornos Windows.
- Guía de seguridad de servidores i servicios IIS 6.0, per a sistemas Windows 2003
- Guía de seguridad de servidores i servicios Apache
- Procedimiento para la configuración segura de equipos en entornos PCI DSS
- …

Documentación generada - II

Mejoras en la gestión de actualizaciones de seguridad

- Procedimiento para la gestión de actualizaciones de seguridad en entornos PCI DSS.

Cumplimentar el Programa de Auditorias

- Revisión de tareas periódicas en entornos PCI DSS
- Tareas periódicas mantenimiento en entornos PCI DSS

Gestión de Incidentes de Seguridad

- Procedimiento de respuesta a incidentes i comunicación mascas de pago

Gestión de la Seguridad con Proveedores

- Requerimientos para los proveedores PCI DSS
- Procedimiento para la contratación de proveedores

Caixa Penedès - SerinCEP

Caixa Penedès – Entidad financiera

Serincep – Empresa prestadora de servicios → Presta servicio de outsourcing a varias Entidades (entre ellas Caixa Penedès).

Objetivo

El cumplimiento por parte de Caixa Penedès implica el cumplimiento por parte de Serincep y otras empresas (Sermepa, …) como prestadores de servicios.

Retos

Definir claramente los límites entre las entidades y SerinCEP.
Acotar que servicios realizan las entidades internamente y que servicios les son prestados por SerinCEP.

Caixa Penedès - SerinCEP

Básicamente la **separación de servicios** se dividió en dos bloques:

- Aspectos técnicos: sistemas compartidos (Storages, sistemas de Internet, …), sistemas propios por entidad (Servidores, Aplicaciones Departamentales, Correo, …), …
- Aspectos organizativos: políticas, contratos, propiedad del hardware, outsourcing de servicios, …

Puntos clave

- Acordar y definir, una vez realizado un inventario de procesos, servidores y aplicaciones donde residen y quien es el responsable (entidad o prestadora);
- El cumplimiento de requerimientos en Caixa Penedès ha supuesto el cumplimiento en SerinCEP
- Es cada una de las entidades responsable de que sus prestadoras cumplan con la normativa;
- El cumplimiento por parte de SerinCEP no conlleva el cumplimento por parte de las entidades debido a los servicios propios que cada una realiza;

Gracias por su atención

Jordi Solà (Responsable del Dpto. de Seguridad Lógica)

Màrius Torres (Analista Seguridad del Dpto. de Seguridad Lógica)

internet security auditors

Caixa Penedès

2ª JORNADA SOBRE SEGURIDAD

EN MEDIOS DE PAGO

PCI DSS
PA DSS

PREGUNTAS

miércoles, 10 de Noviembre de 2010

Hotel Holiday Inn (Madrid)