



2ª JORNADA SOBRE SEGURIDAD


EN MEDIOS DE PAGO

**PCI DSS**  
**PA DSS**

**CAMINO HACIA LA CERTIFICACIÓN EN  
PCI-DSS ADQUIRIENTE**

**JORDI SERRACANTA MARCET**  
DIRECTOR DE MEDIOS DE PAGO  
BANCA PRIVADA D'ANDORRA

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

- 
- ¿Qué es BPA?
  - Preparación
  - Definición de la afectación
  - Identificación
  - Entornos
  - Usuarios

## ¿Qué es Banca Privada d'Andorra?

- Banco creado en 1958
- Capital 100% andorrano
- 8 oficinas en Andorra
- 2003, expansión hacia nuevos mercados
- Filiales en Latinoamérica, España y Luxemburgo
- 5.000 tarjetas emitidas
- 2.000 comercios en adquisición
- Octubre 2009, inicio proyecto implantación PCI-DSS
- Diciembre 2010, finalización implantación, inicio certificación



## Preparación:

- Definir el alcance:

Identificar los procesos de la entidad a los que afecta PCI-DSS

- Definir las áreas implicadas y las personas responsables en el proyecto

- Organización y tecnología
- Medios de pago
- Seguridad física
- Control de riesgos IT

- Establecer un calendario

- Implantación y prioridades
- Seguimiento de la evolución

## Definición de la afectación:

- Aplicación bancaria
  - Transacciones
  - Listados
  - Correo físico
  - Contratos
  - Ubicaciones físicas
- Gestor del correo electrónico
- Proveedores
- Aplicaciones satélite, con acceso a datos de tarjetas
- Cajeros automáticos
  - Diarios electrónicos
  - Operaciones *off-line*
  - *Software* de detección de acciones no autorizadas

## Identificación:

- Trabajo de investigación para poder identificar dónde puede haber datos sensibles de tarjetas de crédito
  - Intervención del Departamento de Informática para poder explorar todos los sistemas e identificar la ubicación de los datos de tarjetas
- Aparecen datos sensibles por todas partes
  - Archivos en Excel, Word y otros formatos
- Almacenamiento de listados y documentación en papel

## Entornos:

### ■ Control en los 3 entornos

#### 1. Desarrollo

- Eliminación de datos de reales
- Creación de juegos de pruebas básicos
- Creación de procesos específicos para generar datos ficticios para pruebas masivas

#### 2. Preproducción o test

- Mismas adaptaciones que en producción

#### 3. Producción

- Control de acceso de los usuarios
- Cifrado de las tablas y de los ficheros
- Control de accesos auditable

## Impacto en el usuario:

- Cambio en el acceso a datos
  - Se puede acceder a datos de tarjetas, sin disponer del número completo
  - Acceder a los datos de forma distinta utilizando otras variables
- Formación
  - Continuada en normativa de PCI-DSS
  - Recordatorio de la prohibición de guardar datos de tarjetas de crédito
- Soporte
  - Dar soporte al resto de empleados desde el Departamento de Medios de Pago





MUCHAS GRACIAS



2ª JORNADA SOBRE SEGURIDAD

EN MEDIOS DE PAGO

PCI DSS  
PA DSS

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