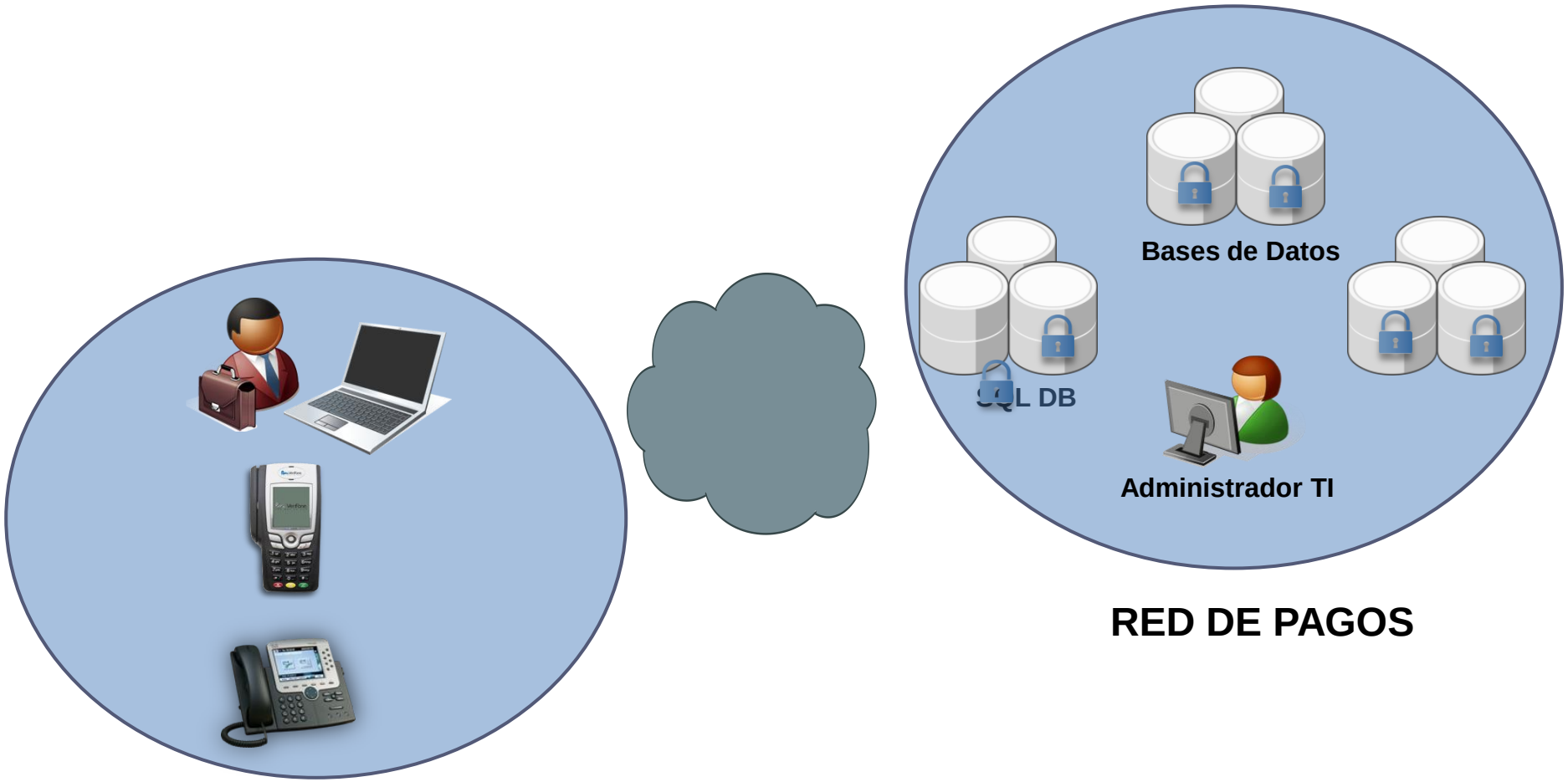
VISION SEGURIDAD EN PAGOS

JULIO 2012
BOGOTA, COLOMBIA

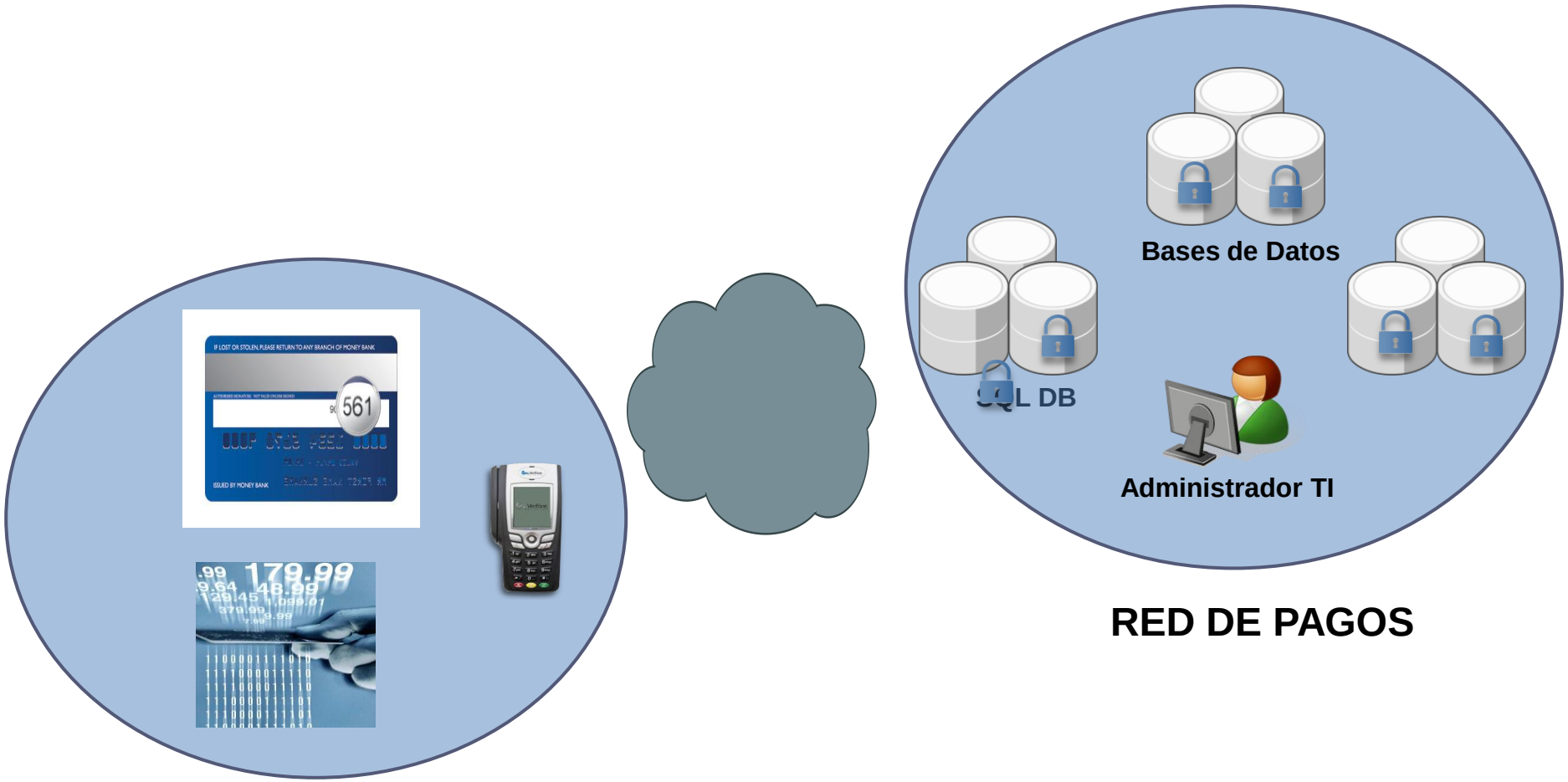
Guillermo Angarita Morris
PCI QSA, CISSP, CISA
guillermo.angarita@iqcol.com

CANALES

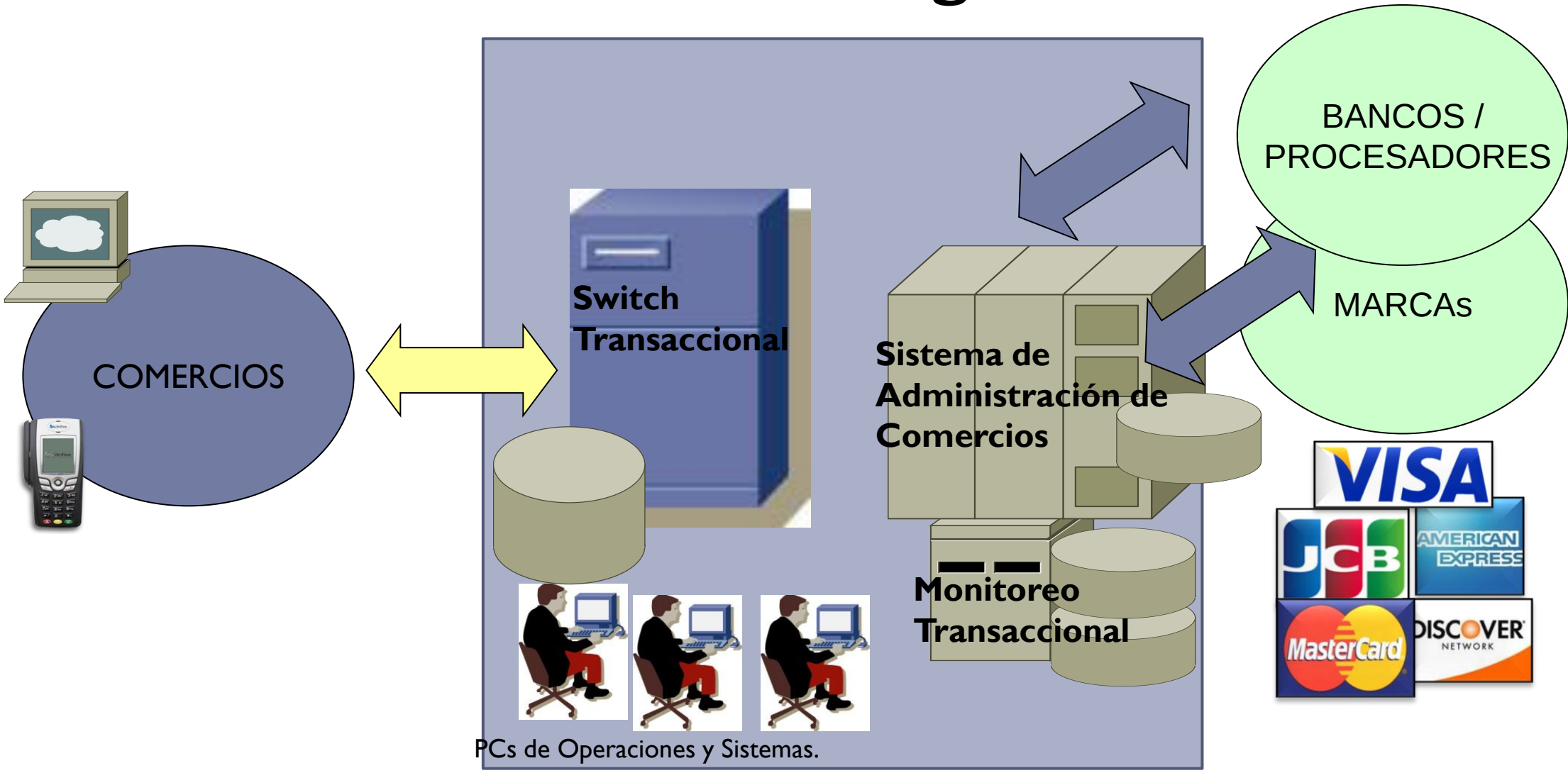


RED DE PAGOS

MEDIOS DE PAGO



Pasarela de Pagos



Industria de medios de pago con Tarjeta

Red de la marca de Tarjetas

Es un miembro de:

Es un miembro de:

Adquirente

Puede o no ser el mismo

Emisor

Recibe requerimientos de autorizaciones y provee servicios de procesamiento a:

Proveedores de Servicio

Emite tarjetas a:

Comercios

Utiliza la tarjeta para compra de

Bienes y servicios

Tarjetahabiente

(CP, CNP)

COMPROMISO DE INFORMACION

http://www.verizonbusiness.com/about/events/2012dbir/index.xml

REPORTE VERIZON

855 incidentes, 174 millones de registros comprometidos

AFP AUSTRALIAN FEDERAL POLICE

POLITIE Korps landelijke politiediensten

IRISS Irish Reporting and Information Security Service

PCeU Police Central e-crime Unit

- Arab Spring,
- Occupied Wall Street
- Los Indignados
- HackTivismo

Quién está tras las brechas ?

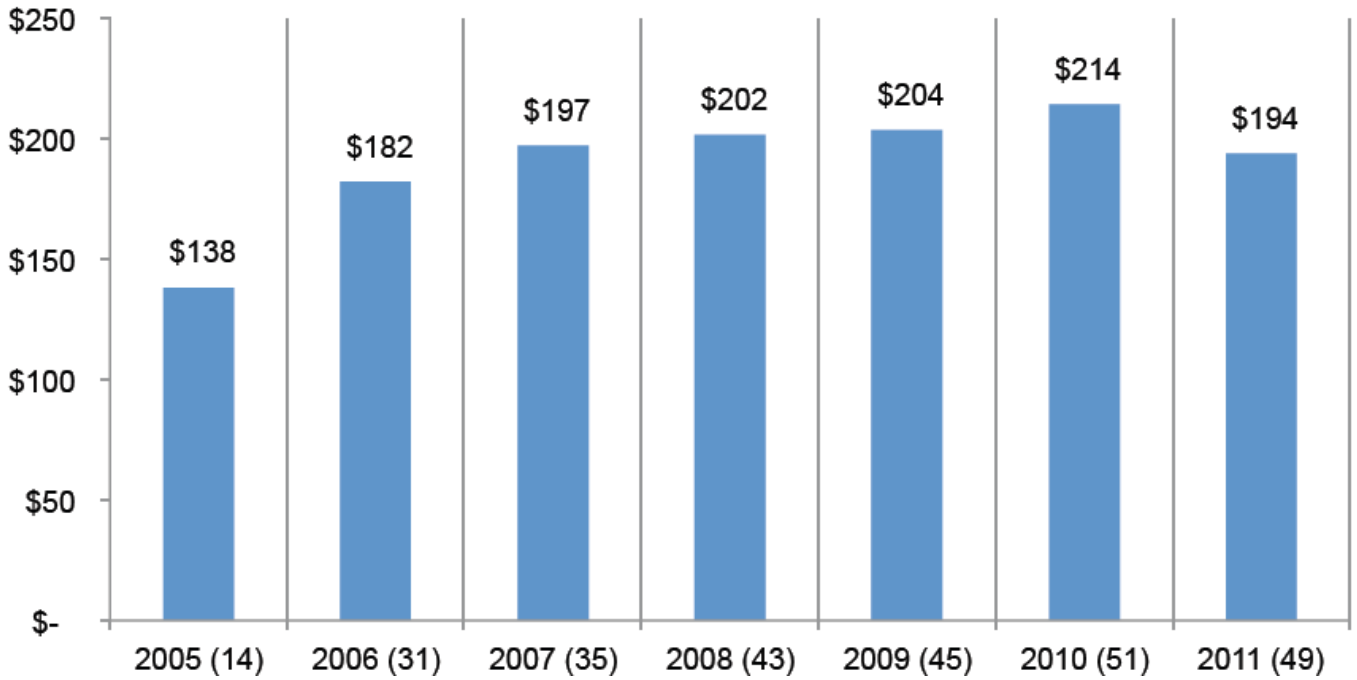
- 98% es de origen externo
- 4% fue causado por personal interno
- <1% implicó socios de negocio
- 58% del total de robo de datos está vinculado a grupos activistas

Cómo ocurrió la brecha ?

- 5% involucró mal uso de privilegios
- 81% resultó de algún tipo de hacking
- 69% utilizó malware
- 10% implicó ataques físicos
- 7% utilizó tácticas sociales

2011 Costo de una Brecha de Datos

Ponemon Institute LLC



Cyber Liability Insurance,

Who and How much Pays, When Your Data Goes Missing?

Es inherentemente difícil asignar un valor económico a algunos tipos de información que son sujetos a robo

PRIMERAS INICIATIVAS DE SEGURIDAD

3D-Secure →

SET → SET fue desarrollado por **SETco** (VISA y MASTER) X.509

EMV → Europay, MasterCard y Visa. Chip & PIN.
Interoperabilidad de tarjetas IC.

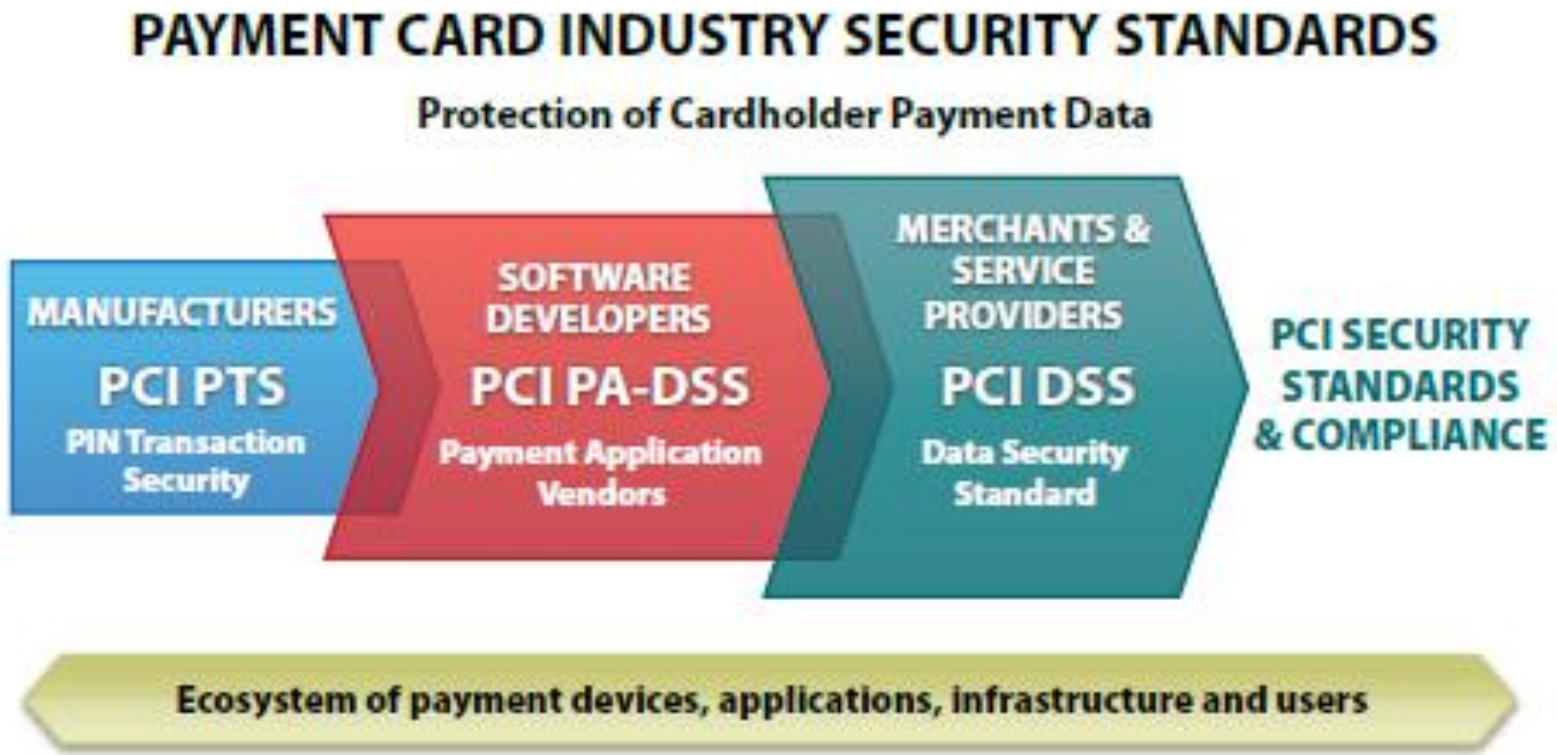
PCI SSC

Fundado en 2006

Foro global abierto para el continuo desarrollo, mejora, almacenamiento, divulgación e implementación de **normas de seguridad para la protección de datos de tarjetahabiente**.

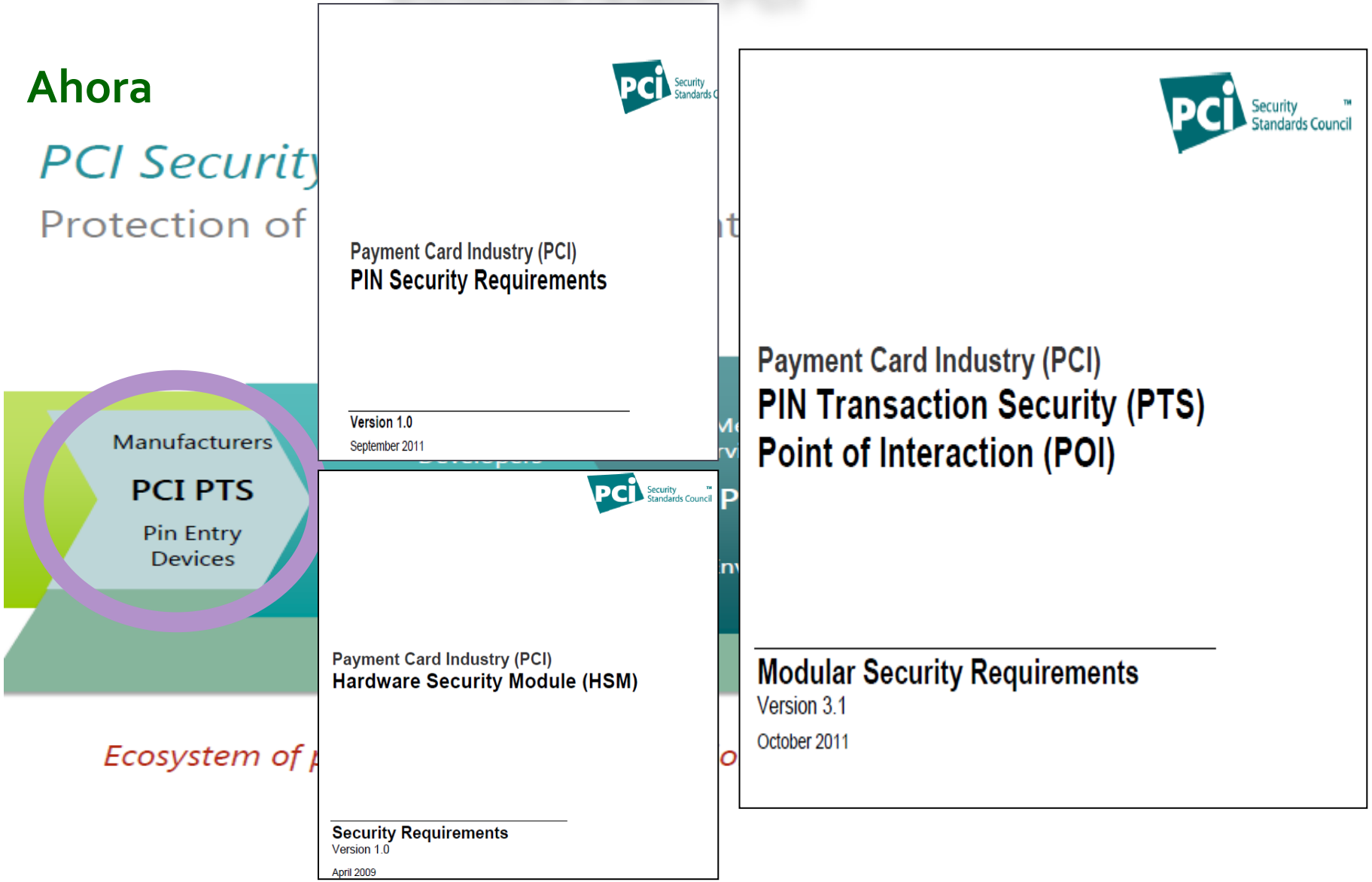
ECOSISTEMA PCI

Antes...



ECOSISTEMA PCI

Ahora



PCI-DSS

- **P**ayment **C**ard **I**ndustry **D**ata **S**ecurity **S**tandards

- Norma de seguridad que deben cumplir las organizaciones que Procesan, Transportan o Almacenan datos de titulares de tarjeta (CHD).
- Es la mejor línea de Defensa contra la Exposición y compromiso de los datos de tarjetahabiente.

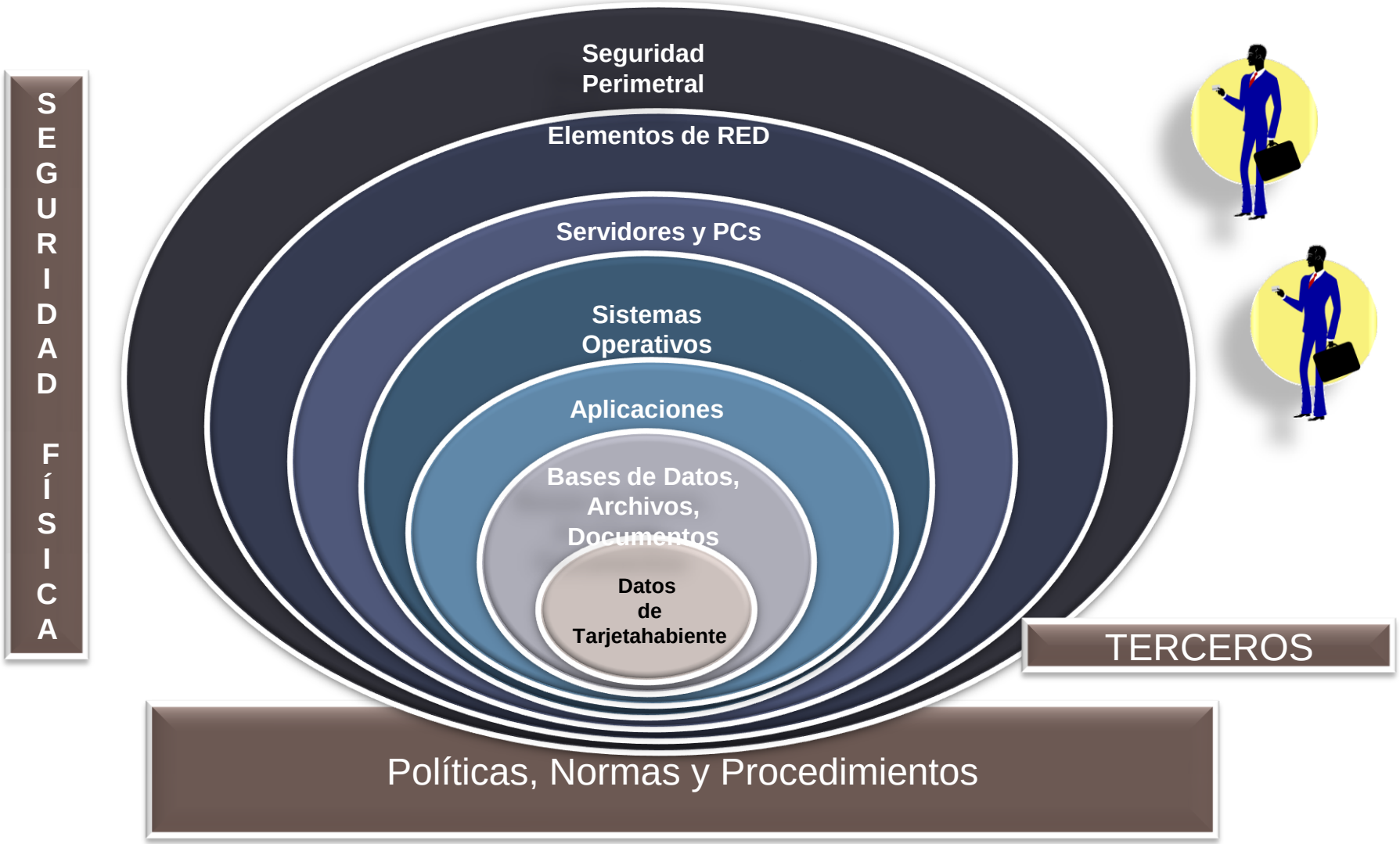
Payment Card Industry (PCI)
Data Security Standard

Requirements and Security Assessment Procedures
Version 1.2
October 2008

PCI DSS ver 1.0 de Enero de 2005 es la evolución del más maduro estandar de VISA.
PCI DSS ver 1.1 válido a partir de Septiembre del 2006
PCI DSS ver 1.2 válido a partir de Octubre 2008
PCI DSS Ver 2.0 válido a partir de Enero de 2011.

Nota: Aplica a organizaciones que Aceptan, capturan, almacenan, transmiten o procesan datos de tarjetahabiente

PCI DSS ES DEFENSA EN PROFUNDIDAD



REQUERIMIENTOS DE PCI DSS

PCI DSS	
SECCIONES	**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.

PA - DSS

- Conjunto de Requerimientos para los fabricantes de software de Aplicaciones de Pago, para facilitar el cumplimiento de la norma PCI DSS.

PCI Security Standards Council

Payment Card Industry (PCI)
Payment Application Data Security Standard

Requirements and Security Assessment Procedures
Version 2.0
October 2010

Ejemplos de Aplicaciones PA:

- Gateways
- POS Suite
- POS Admin
- POS Face to Face
- Payment Back Office
- Payment Gateway/Switch
- Payment Switching
- Shopping Cart

PTS

Payment Card Industry (PCI)

PIN Transaction Security (PTS)

Device Testing and Approval Program Guide

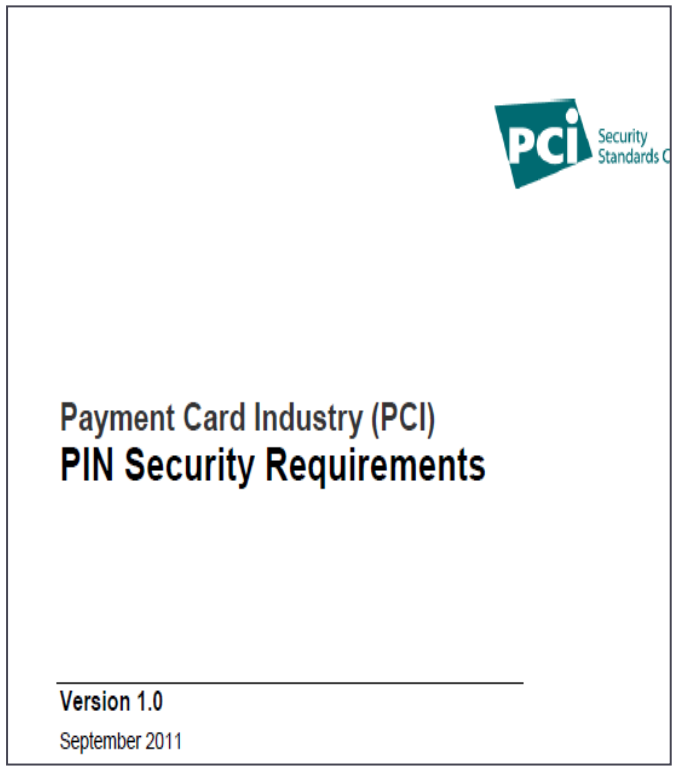
Version 1.0

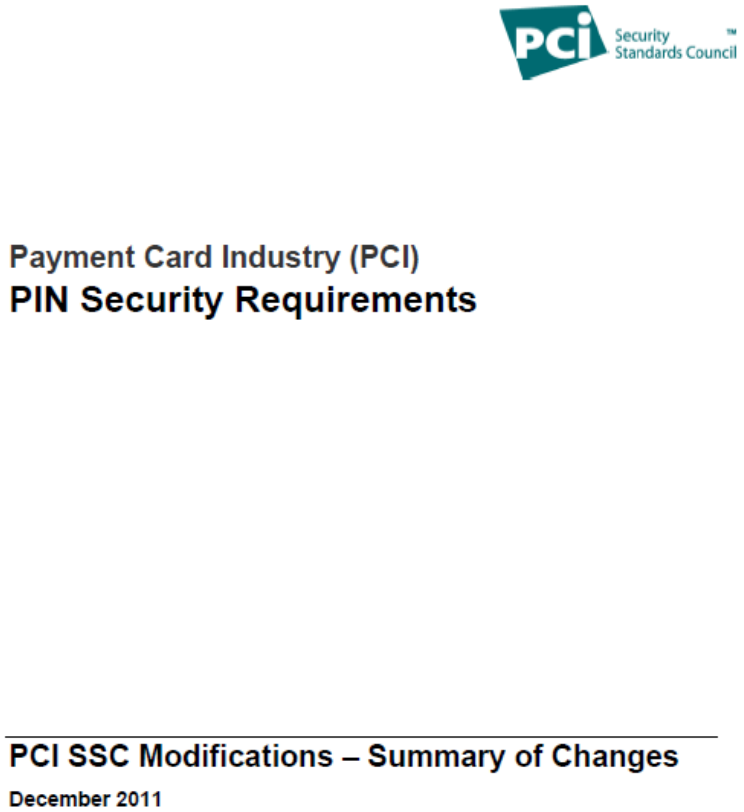
September 2010

Requerimientos para la Gestión y las Características del Dispositivo

PCI PIN Security Requirements

https://www.pcisecuritystandards.org/documents/PCI_PIN_Security_Modifications.pdf





La mejor forma de proteger algo… es no tenerlo

The Future of Money: How Mobile Payments Could Change Financial Services

March 22, 2012

http://financialservices.house.gov/News/DocumentSingle.aspx?DocumentID=286112

Pagos Moviles: Comprar productos o transferir dinero con un dispositivo móvil.
Diferentes tecnologías: Aún en Desarrollo.
Múltiples formas para iniciar pagos: SMS, Apps, **Chip NFC**

Google wallet

ISIS™

Múltiples Involucrados: Consumidores, Comercios, Procesadores, Wireless Carriers, Instituciones Financieras

ESCENARIOS PARA EL USO DE DISPOSITIVOS MOVILES

Dispositivos Móviles como Terminales POS

Dispositivos Móviles como Tarjeta de Pago

PCI Security Standards Council estableció el **Mobile Working Group**

PCI SSC Mobile Working Group

Se apalanca en:

- OWASP Mobile Project
- Global Platform
- GSMA
- BITS
- NIST
- ANSI/ISO

PCI SSC Mobile Working Group

General Purpose Smart Device

Dos Escenarios

- 1: Datos de Tarjetahabiente entran al dispositivo usando una solución de cifrado y es transmitida así a través del dispositivo móvil
  - El SmartPhone nunca tiene acceso al PANs en texto claro
- 2: Datos de Tarjetahabiente ingresan al dispositivo sin cifrar
  - El Smartphone tiene acceso al PAN en texto claro
  - Guía para proteger el PAN dentro de la aplicación instalada en el SmartPhone

GRUPOS DE INTERES

E-Commerce Merchants

Cloud (Virtualization Phase 2)

CONCLUSIONES

- Las normas PCI son consideradas mejores practicas de industria para la seguridad en pagos electrónicos. (No hay que inventar la rueda).
- La norma PCI hasta ahora no considera la seguridad del punto final (endpoint).
- La seguridad en pagos electrónicos debe cubrir a todos los miembros de la cadena de pagos.
- Los pagos móviles plantean retos en cuanto a la seguridad.

Facilitador:

Guillermo Angarita

CISSP, CISA , PCI QSA

Guillermo.angarita@iqcol.com