Strategos
Consulting Services

Cumplimiento del "Reglamento de Tarjetas de Crédito y Débito" de la SBS y las PCI DSS en el Perú 2015

Marzo 2015

Raúl Díaz

Strategos
Consulting Services

- Socio IT & Information Security Services, Strategos Consulting Services
- Asesor en Procesos MC, JNE y Leasing Total.
- ESAN
  - Candidato MBA
  - PAE Gestión de Seguridad de la Información
  - PEE Gerencia de Tecnologías de la Información
- Universidad de Lima
  - Ingeniero de Sistemas
- Certificaciones Internacionales:
  - ISO/IEC 27001 LA, CISA, ECSA, CEH, ECSP, CHFI, CPTE, ISF ISO/IEC 27002, ITIL(F), COBIT
- Consultoría de Gestión de TI, Riesgos y Seguridad de la Información en:
  - Perú, Argentina, Colombia, Honduras, Chile, Bolivia.
- Instructor en ECCouncil (Seguridad Informática) en:
  - Perú, Venezuela, Chile, Argentina, Honduras, México, Ecuador, Colombia, Brasil.

Agenda

Strategos
Consulting Services

- Fraude
- Rol Adquiriente y Emisor
- Res. 6523-2013 SBS “Reglamento de Tarjetas de Crédito y Débito”
  - Estructura
  - Alcance
  - Tiempo de implementación
  - EMV
- PCI DSS
  - Empresas certificadas PCI DSS
  - Aplicabilidad
  - Requisitos
  - Metodología
  - Cambios versión 2 a 3
- Nuestros servicios profesionales

Fraude

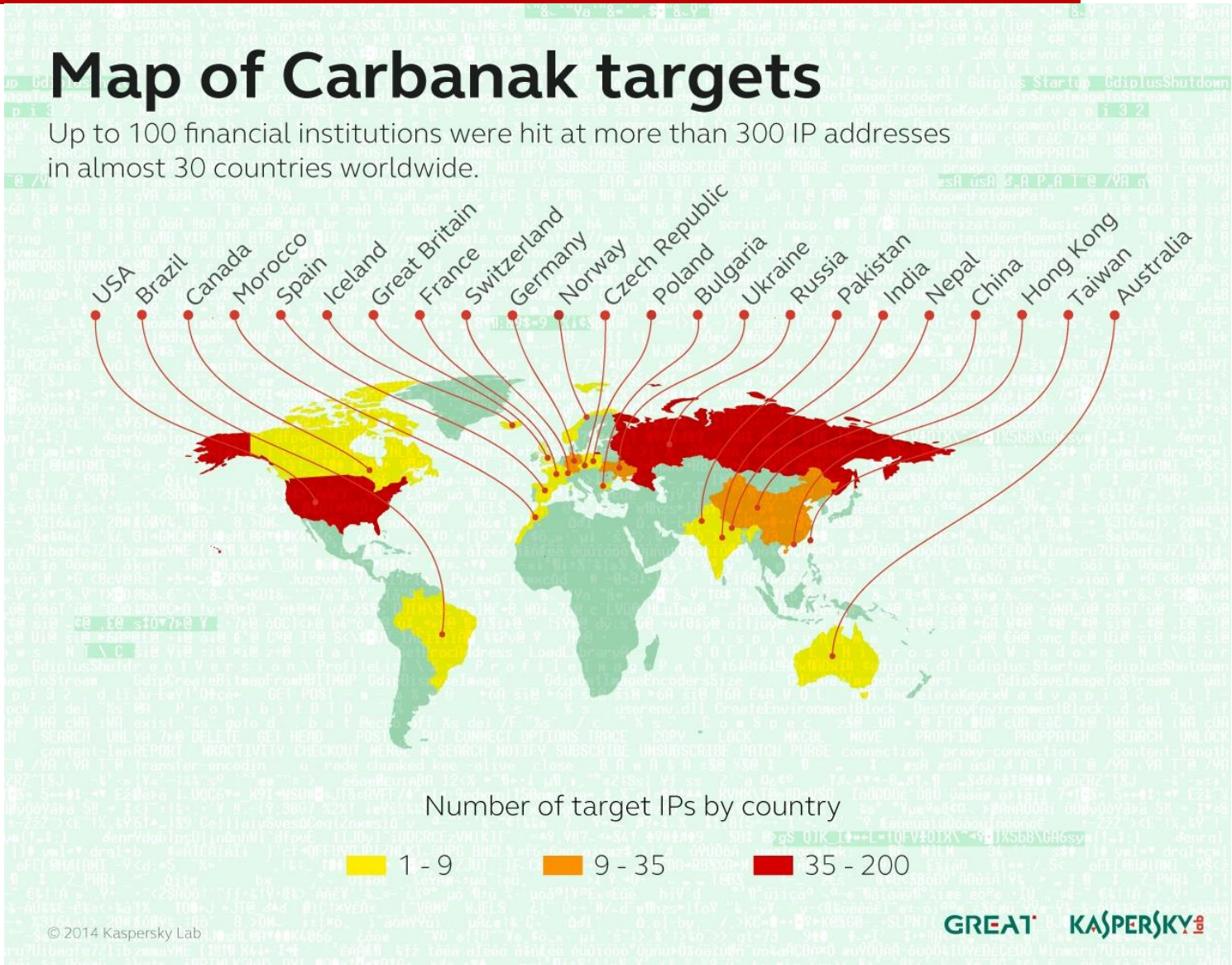
Fraudes

Strategos
Consulting Services

- Diciembre 2013, Robo de 40 millones de tarjetas (Target) - BlackPOS
- Julio 2011, Robo 7 millones de soles (Banco de la Nación) – Switch Transaccional
- 1 billón de dólares de 100 bancos en el mundo - Carbanak

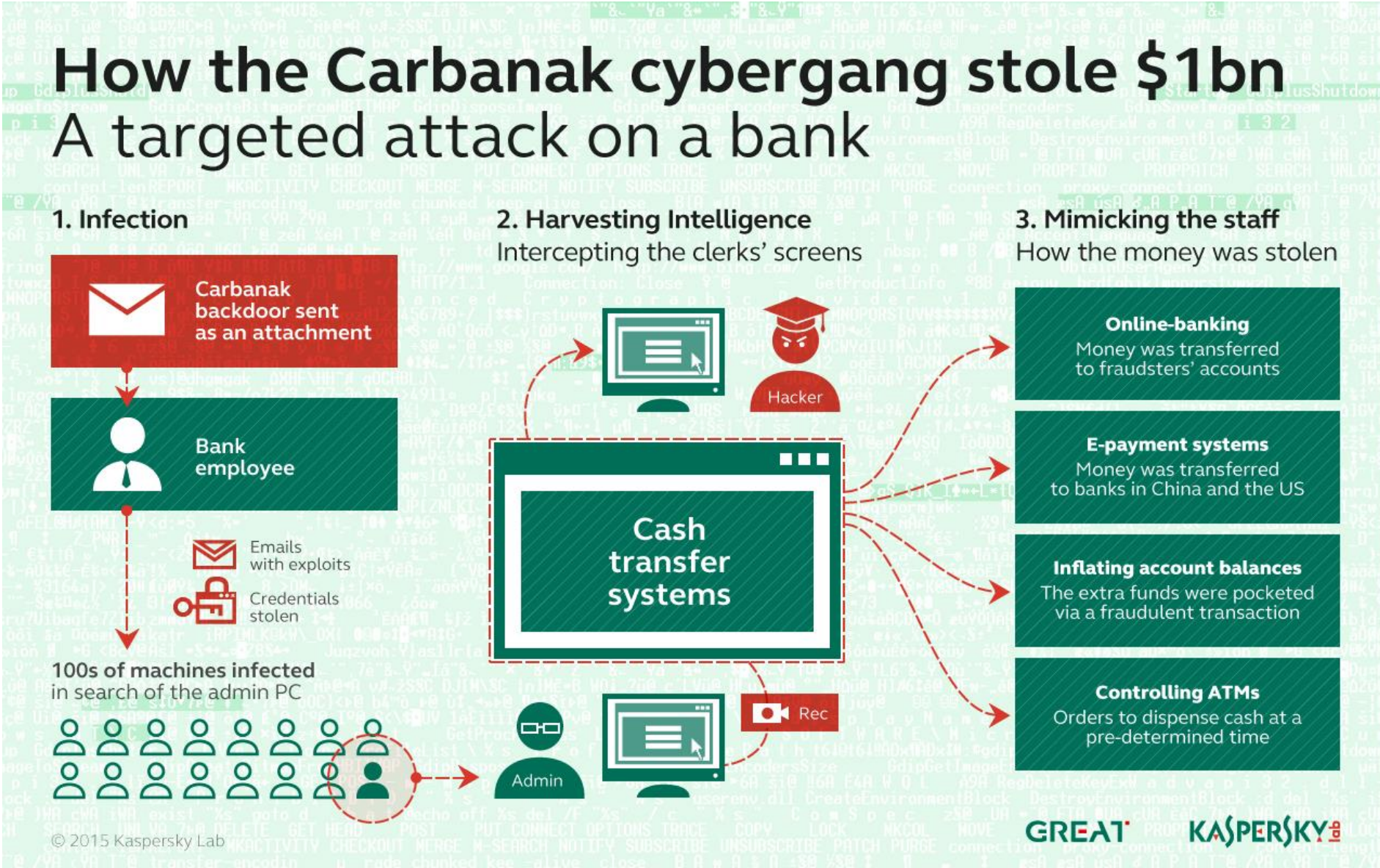
Fraude - Carbanak

Strategos
Consulting Services



Fraude - Carbanak

Strategos
Consulting Services



Fraude - Asbanc

Strategos
Consulting Services

Asbanc: Más de un millón de tarjetas que circulan en el mercado ya cuentan con chip de seguridad

Jueves, 04 de septiembre del 2014

ECONOMÍA

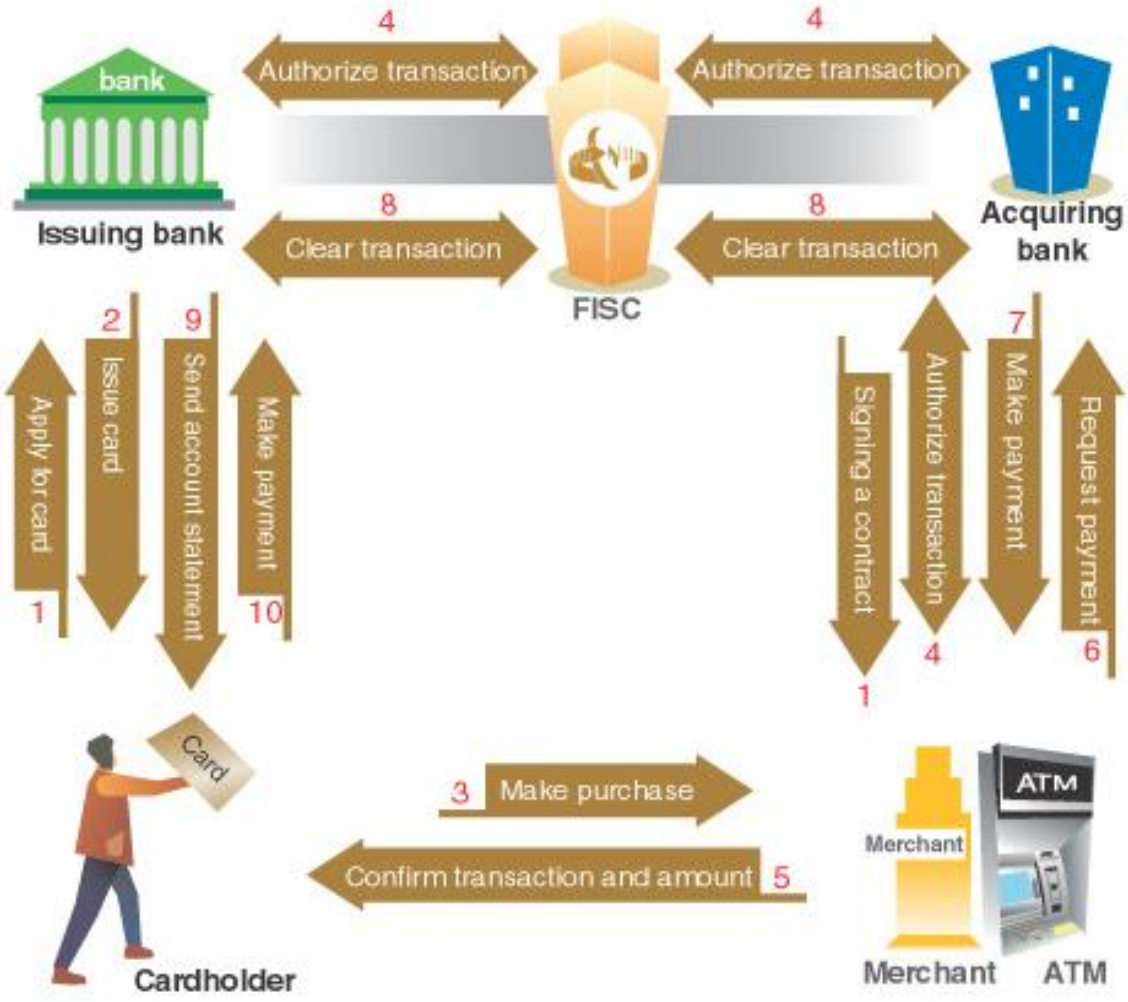
17:20

Este **sistema de seguridad** otorga una mayor garantía a los usuarios frente a los delitos de falsificación y/o clonación de tarjetas y permite almacenar mayor información.

Rol Adquirente y Emisor

Rol Adquirente y Emisor

Strategos
Consulting Services



Reglamento de Tarjetas

Estructura

Strategos
Consulting Services

- Capitulo 1 – Aspectos Generales
  - Articulo 1- Alcance.
  - Articulo 2 – Definiciones.
  - Artículo 3 – Tarjeta de Crédito.
  - Artículo 4 – Tarjeta de Débito.
- Capitulo 2 – Disposiciones generales aplicables a tarjetas de crédito
  - Artículo 5 - Contenido mínimo de contrato.
  - Artículo 6 - Información mínima, condiciones y vigencia aplicable.
  - Artículo 7 - Servicios asociados a la tarjeta de crédito.
  - Artículo 8 - Tarjeta de crédito adicional.
  - Artículo 9 - Cargos.
  - Artículo 10 - Contenido mínimo de estado de cuenta.
  - Artículo 11 - Puesta a disposición o envió y recepción del estado de cuenta y procedimiento de reclamos.
- Capitulo 3 – Disposiciones generales aplicables a tarjetas de débito
  - Artículo 12 - Información mínima, condiciones y vigencia aplicable
  - Artículo 13 - Servicios asociados
  - Artículo 14 - Cargos
- Capítulo 4 – Otros aspectos aplicables a las tarjetas de crédito y débito
  - **Subcapítulo I – Medidas de seguridad aplicables**
    - **Artículo 15 - Medidas de seguridad incorporadas en las tarjetas (EMV)**
    - Artículo 16 - Medidas de seguridad respecto a los usuarios
    - Artículo 17 - Medidas de seguridad respecto al monitoreo y realización de las operaciones
    - **Artículo 18 - Medidas en materia de seguridad de la información (PCI DSS)**
    - Artículo 19 - Medidas de seguridad en los negocios afiliados
    - Artículo 20 - Requerimientos de seguridad en caso de subcontratación
  - Subcapítulo II - Obligaciones Adicionales
  - Subcapítulo III - Materia de supervisión
- Disposiciones Finales y Transitorias

Alcance

Strategos
Consulting Services

- “Empresas autorizadas a expedir y administrar tarjetas de crédito y débito”
  - Bancos (20)
  - Financieras (13)
  - Cajas Municipales (13)
  - Edpymes (11)
  - Procesadores (Visanet, Procesos MC, Unibanca, Alignet, Globokas)
  - Otros.

Tiempos de Adecuación

Strategos
Consulting Services

- Publicación 30 de Octubre 2013
- Desde el 31 de diciembre de 2014 las tarjetas serán emitidas con chip
- Desde el 31 de diciembre 2014 se deben cumplir los artículos 7°, 10°, 13°, el numeral 4 del artículo 16° y 17°.
- Plazo de adecuación del articulo 18 hasta el 31 de diciembre del 2015
- Desde el 31 de diciembre de 2015, *asegurar que las redes de cajeros automáticos puedan autenticar* las tarjetas con chip
- Desde el 31 de diciembre de 2015, las empresas que permitan la realización de operaciones sin utilizar chip, *deberán asumir los riesgos* y los costos de dichas operaciones, en caso no sean reconocidas por los usuarios.

SUPERINTENDENCIA
DE BANCA, SEGUROS Y AFP
República del Perú

Implicancias

Strategos
Consulting Services

- Los auditores de la SBS incluirán dentro de su programa de auditoría del 2016 los requisitos del reglamento, especialmente, el *artículo 18 - Medidas en materia de seguridad de la información (PCI DSS)*
- Las entidades financieras solicitaran el cumplimiento de las PCI DSS a sus proveedores de servicio.

SUPERINTENDENCIA
DE BANCA, SEGUROS Y AFP
República del Perú

EMV

Strategos
Consulting Services

- ***Europay, Matercard y Visa*** (EMV) es un estándar mundial de interoperabilidad entre el chip y el POS y ATMs para la autenticación de transacciones con tarjetas de crédito y débito.
- Publicado por primera vez en 1996.
- El chip tiene características similares al RFID

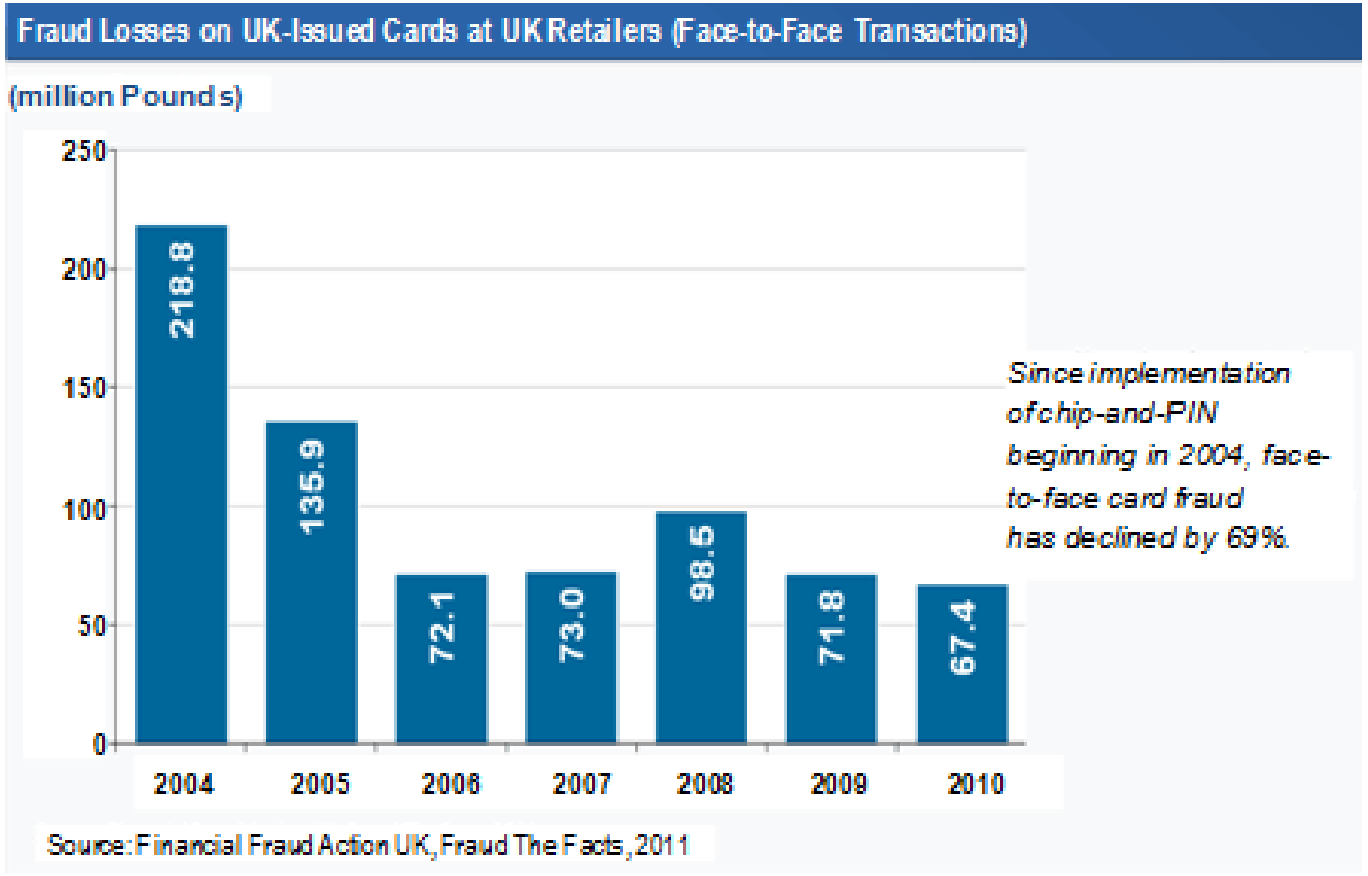
Tecnología EMV

Strategos
Consulting Services

- Microprocesador o chip en la tarjeta
- POS y ATM que soporten EMV (con contacto o sin contacto)

EMV en Reino Unido

Strategos
Consulting Services



Transacción EMV

Strategos
Consulting Services

Fase 1

Autenticación de la tarjeta

- ***Static Data Authentication (SDA)***
- Dynamic Data Authentication (DDA)
- Combined DDA/generate Application Cryptogram (CDA)

Fase 2

Verificación del titular de tarjeta

- Signature
- ***Offline plaintext PIN***
- Offline enciphered PIN
- Offline plaintext PIN and signature
- Offline enciphered PIN and signature
- Online PIN
- No CVM required
- Fail CVM processing

Fase 3

Autorización de las transacciones

- Transaction certificate (TC) — Offline approval
- Authorization Request Cryptogram (ARQC) — Online authorization
- Application Authentication Cryptogram (AAC) — Offline decline

EMV y NFC

Strategos
Consulting Services

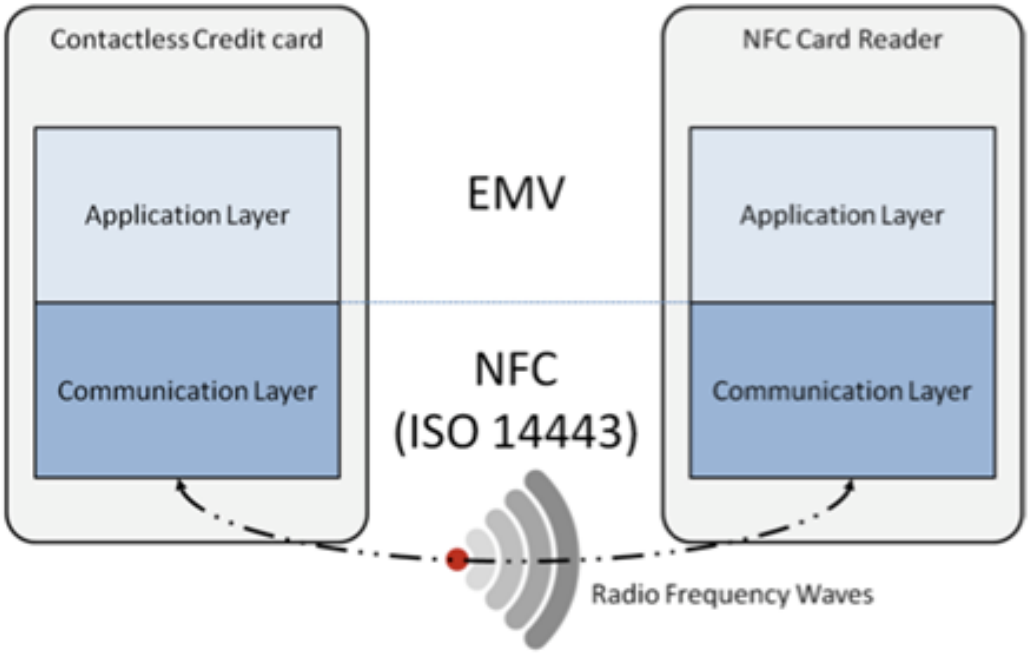
- *Near Field Communication (NFC)* es un protocolo derivado del RFID usado por los chips.
- Transmisión corta en centímetros.
- NFC esta siendo incluido en los dispositivos móviles.

Check out with PayPal

Google Wallet

EMV y NFC

Strategos
Consulting Services



Vulnerabilidades

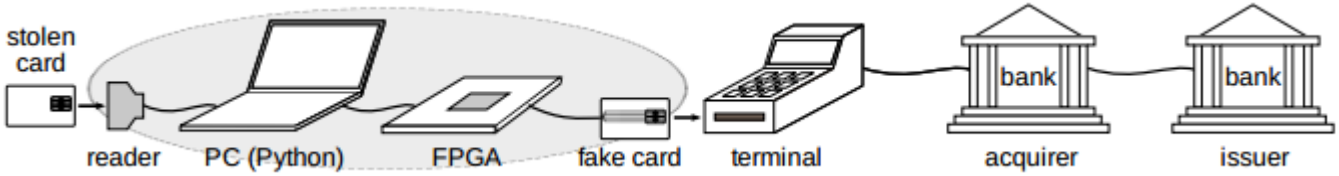
Strategos
Consulting Services

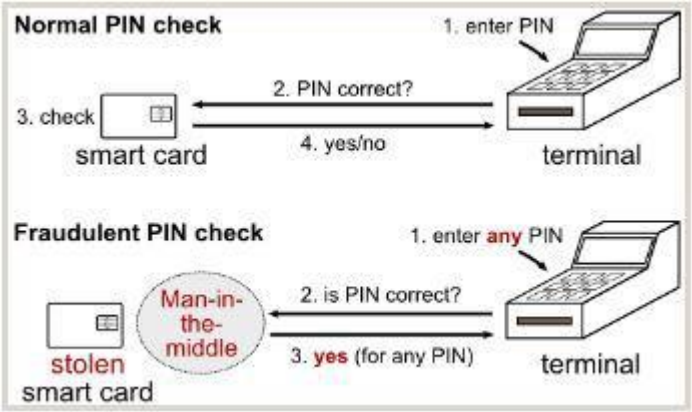
- Migración de banda magnética al Sistema EMV
- Ataque Yes-Card (Static Data Authentication, Dynamic Data Authentication)
- Mitm
- Chip Skimmers y extracción del PIN (Cardholder Verification Method)

Vulnerabilidades

Strategos
Consulting Services

- MITM

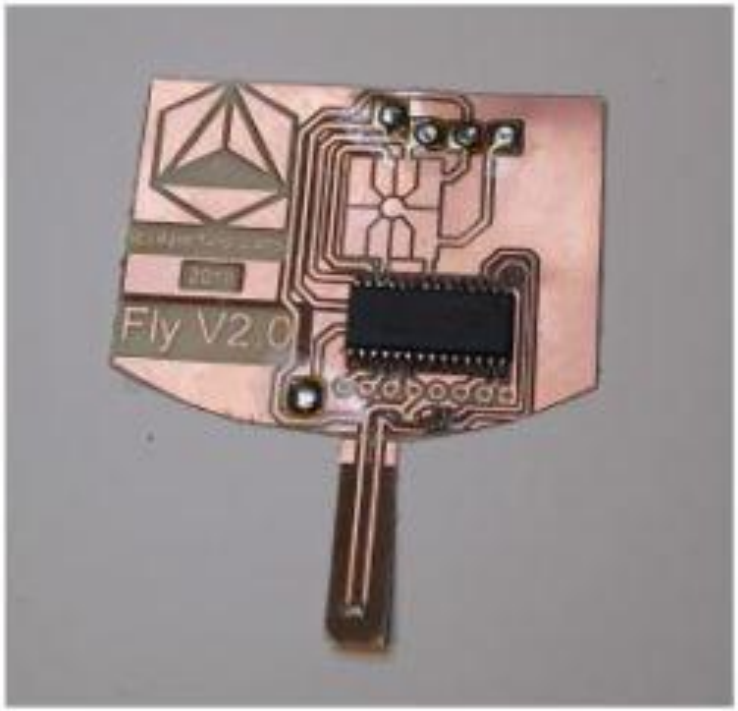




Chip Skimmer

Strategos
Consulting Services

- Plaintext Pin Verification



PCI DSS en el Perú

Empresas certificadas en el Perú

Strategos
Consulting Services

- Visanet
- Procesos MC (Mastercard)
- Alignet
- Unibanca

1st SECURE IT
When compliance is not enough

Certificate of PCI Compliance

Certificate of Compliance

This is to certify that ALIGNET S.A.C. has completed an onsite PCI DSS Report on Compliance (ROC) and has been found PCI compliant per the PCI Security Standards, as set forth by the Payment Card Industry Security Standards Council and endorsed by the major payment brands.

Based upon the information validated by the 1st Secure IT auditor and provided by the entity regarding their policies, procedures and technical systems that store, process and/or transmit cardholder data and the ASV scans of those systems, the Entity has satisfactorily met the requirements of PCI DSS and has been issued a passing Report on Compliance. No other guarantees are given.

In the event the entity is required to show validation of PCI DSS compliance, the entity should show this certificate along with their Attestation of PCI Compliance. PCI Compliance is a point in time Certification and it is the entity's responsibility to maintain current and on-going PCI DSS compliance. Additionally, current ASV scan reports should be kept with this certificate of compliance.

1st Secure IT LLC makes no representation or warranty to any third party as to whether entity's systems are secure or protected from attack and/or breaches, or whether cardholder data is at risk of being compromised. 1st Secure IT LLC accepts no liability to any third party in the event of loss or damage of any description, caused by any failure in or breach of entity's security. This certificate is for the sole purpose of identifying compliance and can not be used for any other purpose.

Abelardo Rodrigues, CISSP, PCI QSA

Awarded To:

ALIGNET S.A.C.

Address & Data Center:
Casimiro Ulloa 333, Miraflores
Lima - Perú

Business:
Payment Solutions for e-Commerce

Date of Onsite Audit:
November 2013

Date of Next Audit:
September 2014

Scanning Tool:
McAfee Secure

Contact:
Vicente Huayllla
Vicente.huayllla@alignet.com

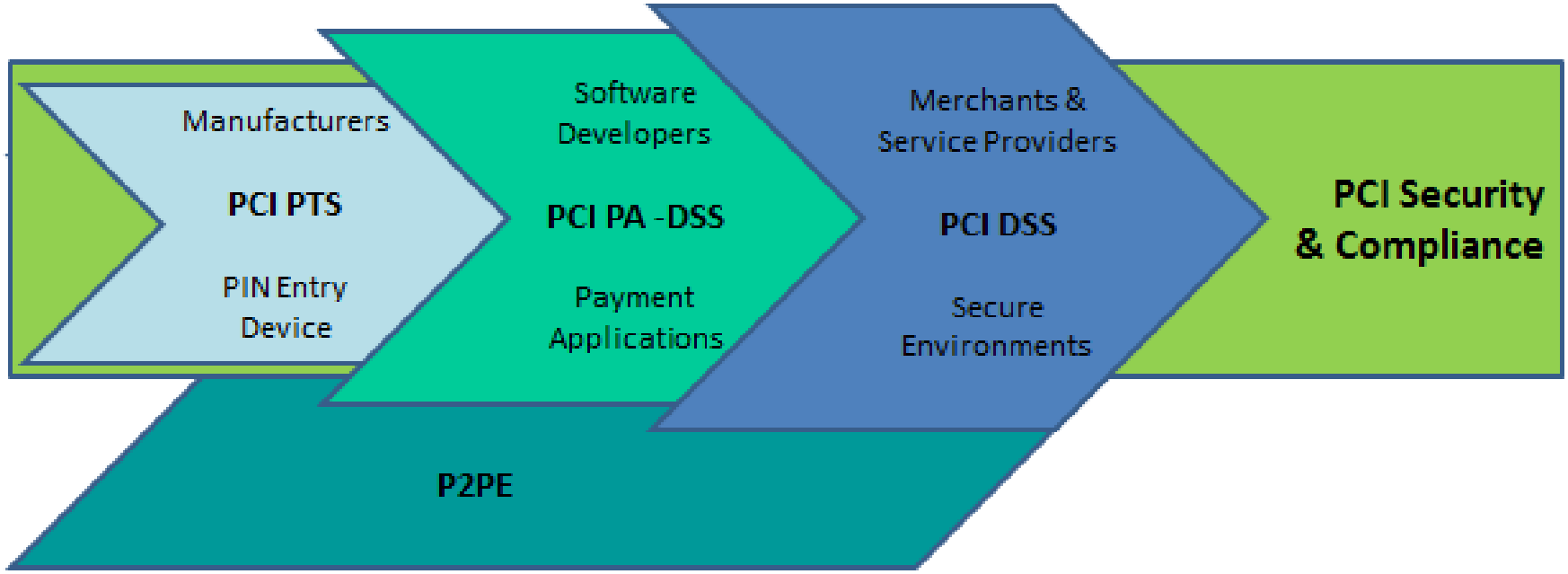
Certificate Number:
131121B

- Empresas QSA:
  - ***1st Secure***
  - Trustwave
  - IQ Information Quality

https://www.pcisecuritystandards.org/

Documentos PCI SSC

Strategos
Consulting Services



Alcance PCI DSS

Strategos
Consulting Services

- PCI DSS se aplica donde sea que se almacenen, procesen o transmitan **"datos de cuentas"**
- Los datos de titulares de tarjetas incluyen: **Número de cuenta principal (PAN),** Nombre del titular de la tarjeta, Fecha de vencimiento y Código de servicio
- Los datos confidenciales de autenticación incluyen: **Todos los datos de la banda magnética o datos equivalentes que están en un chip, CAV2 / CVC2 / CVV2 /CID y PIN / PIN Block**
- El **Número de cuenta principal** es el factor que define la aplicabilidad de los requisitos de las PCI DSS

Datos de cuentas	
Los datos de titulares de tarjetas incluyen:	**Los datos confidenciales de autenticación incluyen:**
▪ Número de cuenta principal (PAN) ▪ Nombre del titular de la tarjeta ▪ Fecha de vencimiento ▪ Código de servicio	▪ Contenido completo de la pista (datos de la banda magnética o datos equivalentes que están en un chip) ▪ CAV2/CVC2/CVV2/CID ▪ PIN/Bloqueos de PIN

Aplicación PCI DSS Comercios

Strategos
Consulting Services

NIVEL	CRITERIO (Visa, MC)	REQUERIMIENTO
1	Comercios de alto riesgo que procesan más de *6 millones de transacciones anualmente**	• Evaluación anual en-sitio • Escaneo de red trimestral (ASV)
2	Comercios de alto riesgo que procesan entre *1 millón a 6 millones de transacciones anualmente* *	• Cuestionario de auto-evaluación anual (SAQ) o Evaluación en-sitio • Escaneo de red trimestral (ASV)
3	Comercios que procesan entre *20,000 a 1 millón de transacciones anualmente*	• Cuestionario de auto-evaluación anual (SAQ) • Escaneo de red trimestral (ASV)
4	Todos los comercios restantes	• Validación establecida por el Adquirente. Recomendado: • Cuestionario de auto-evaluación anual (SAQ) y Escaneo Trimestral ASV

* Comercios de alto riesgo: cualquier comercio con capacidad de almacenar información, usualmente mediante algún tipo de aplicación de software.

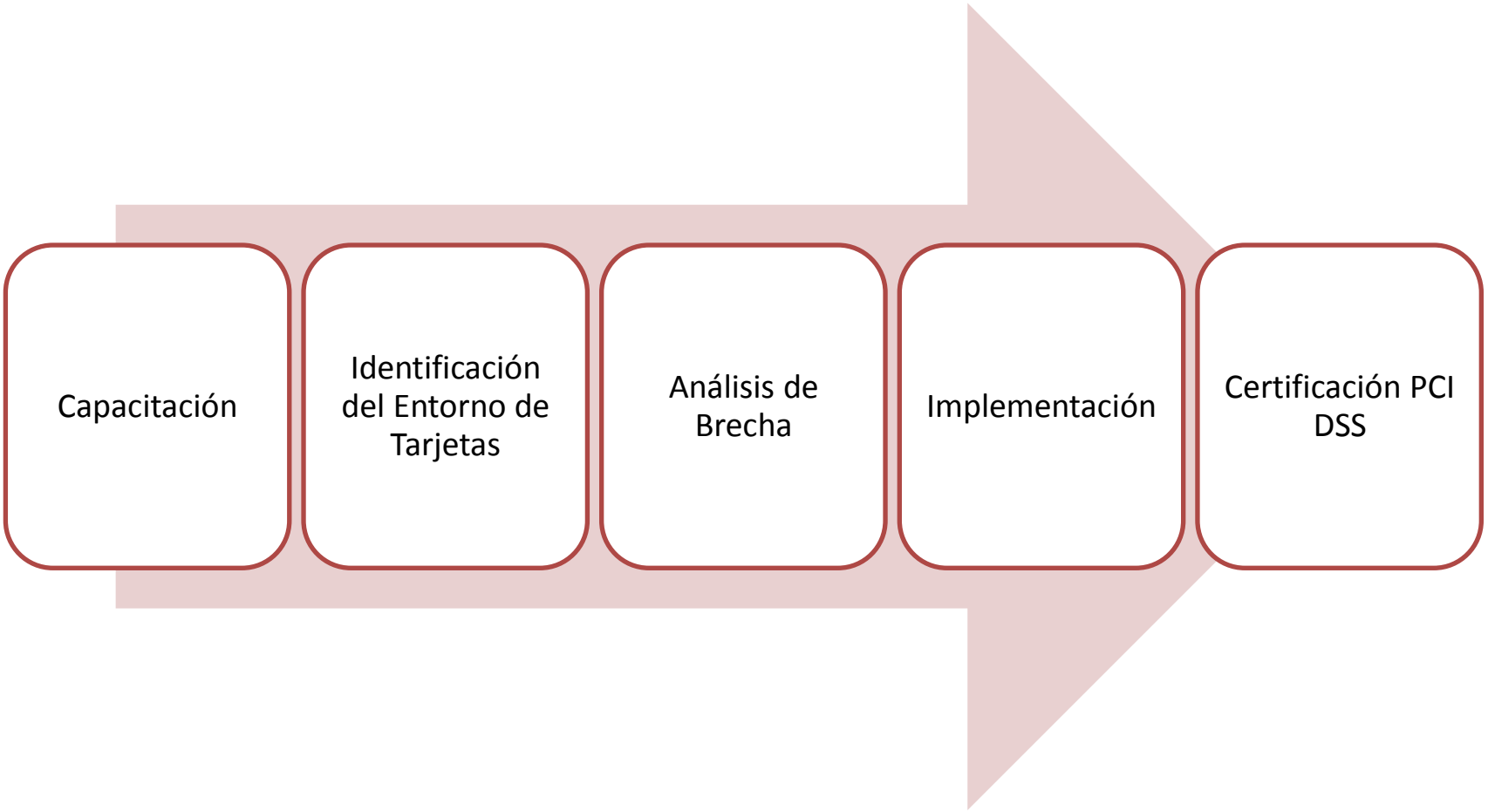
Requerimientos

Strategos
Consulting Services

Construir Y Mantener Redes Seguras	1. **Instalar y mantener configuraciones de firewall para proteger la información** 2. **No usar contraseñas o parámetros de seguridad provistos por suplidores**
Proteger La Información Del Tarjetahabiente	3. **Proteger información almacenada** 4. **Cifrar datos de tarjetahabientes e información sensitiva al enviarla por redes públicas**
Establecer Programas De Pruebas De Vulnerabilidades	5. **Usar y actualizar regularmente programas de antivirus** 6. **Desarrollar y mantener sistemas y aplicativos seguros**
Implementar Medidas Fuertes De Control De Acceso	7. **Restringir acceso a información de acuerdo a reglas del negocio** 8. **Asignar IDs únicos para cada persona con acceso a sistemas** 9. **Restringir acceso a la información de tarjetahabiente**
Regularmente Monitorear Y Probar Acceso A La Red	10. **Rastrear y monitorear todos los accesos a la red e información del tarjetahabiente** 11. **Regularmente probar sistemas y procedimientos de seguridad**
Mantener Políticas De Seguridad De La Información	12. **Establecer políticas dirigidas a la seguridad de la información**

Metodología

Strategos
Consulting Services



Cardholder Data Environment Matrix (Buena Práctica)

Strategos
Consulting Services

Listado de todos los activos que procesan, almacenan y transportan datos de tarjeta.

- Personal relacionado con el CDE
- Servidores y estaciones de trabajo
- Equipos activos de red y de seguridad perimetral
- Bases de datos
- Aplicaciones
- Medios de almacenamiento y otros soportes
- Canales de comunicación
- Proveedores
- Instalaciones
- Documentación

CDEM

Strategos
Consulting Services

CardHolder Data Matrix PCI DSS

Listado de aplicaciones en el entorno PCI DSS

ID	Tipo	Aplicación	Información	Instalada en
APP001	*Base de datos, sistema operativo..*			

Cambios de la versión 2 a la 3

Sumary of Changes

Strategos
Consulting Services

- 1.1.3 Se aclaró lo que debe incluir el diagrama de red y se agregó un nuevo requisito en 1.1.3 para **un diagrama actual** que muestre los flujos de datos del titular de la tarjeta.
- 2.4 Se creó un nuevo requisito para **mantener un inventario de los componentes del sistema** que se encuentran dentro del alcance de las PCI DSS a fin de respaldar el desarrollo de las normas de configuración.
- 5.1.2 Se creó un nuevo requisito para **evaluar las amenazas futuras de malware** para cualquier sistema que no se considere frecuentemente afectado por software malicioso.
- 6.5.10 Se creó un nuevo requisito para **prácticas de codificación para proteger** ante una autenticación y administración de sesión interrumpidas. En vigor a partir del 1 de julio de 2015.
- 8.5.1 Se creó un nuevo requisito para los **proveedores de servicios con acceso remoto** a las instalaciones del cliente para usar credenciales de autenticación exclusivas para cada cliente. En vigor a partir del 1 de julio de 2015

Sumary of Changes

Strategos
Consulting Services

- 9.3 Se creó un nuevo requisito para controlar el **acceso físico a áreas confidenciales para el personal del sitio**, lo que incluye un proceso para autorizar el acceso y revocar el acceso inmediatamente después de la finalización.
- 9.9.x Se incorporaron nuevos requisitos para **proteger contra alteración y sustitución a los dispositivos que capturan datos de la tarjeta de pago** a través de interacción física directa con la tarjeta. En vigor a partir del 1 de julio de 2015.
- 11.3 Se creó un nuevo requisito para implementar una **metodología para las pruebas de penetración**. En vigor a partir del 1 de julio de 2015. Hasta la implementación de la versión 3.0, se deben seguir los requisitos de la versión 2.0 de las PCI DSS para las pruebas de penetración.
- 12.8.5 Se creó un nuevo requisito para mantener información sobre qué requisitos de las **PCI DSS administra cada proveedor de servicios**, y cuáles están a cargo de la entidad.
- 12.9 Se creó un nuevo requisito para que los **proveedores de servicios proporcionen el reconocimiento/acuerdo** escrito a sus clientes, tal como se especifica en el requisito 12.8. En vigor a partir del 1 de julio de 2015.

https://es.pcisecuritystandards.org/_onelink_/pcisecurity/en2es/minisite/en/docs/PCI_DSS_v3_Summary_of_Changes.pdf

Nuestros Servicios

Nuestros Servicios

Strategos
Consulting Services

- Análisis de Brecha (incluye plan de acción)
- Diseño de Arquitectura de Seguridad Informática.
- Gestión de Proyecto de Implementación.
- Outsourcing de especialistas PCI DSS.
- Diseño de documentación obligatoria.
- Pruebas de Penetración y Análisis de Vulnerabilidades.

Nuestros Entregables

Entregables

Strategos
Consulting Services

- Informe de capacitación PCI DSS y materiales complementarios.
- Informe de identificación del entorno PCI DSS.
- Informe de diagnostico y análisis de Brecha.
- Informe de plan de implementación de requisitos.
- Informe de seguimiento de implementación PCI DSS.
- Informe de resultados de la preparación orientado al cumplimiento de la norma PCI DSS.
- Informe final de servicios de consultoría.

Strategos
Consulting Services

Contacto

Raúl Díaz, Socio IT & Information Security Services
CISM, CISA, CEH, CHFI, ECSA,
ECSP, ITIL(F), ISF ISO/IEC 27002
raul.diaz@strategoscs.com
Cel: +51-994521461
@rauldiazp
www.rauldiazparra.com