
S21sec
Committed to cybersecurity
Visión holística de los requerimientos de seguridad lógica de una red de ATM’s
www.s21sec.com
Author: S21sec | Date: 11 june 2015 | v 4.0.0

ÍNDICE

- S21sec
- Contexto global
- Incidentes y respuesta
- Contramedidas de seguridad
- Cumplimiento normativo. PCI DSS

S21sec


S21sec

S21sec

We are a pure-play Cyber Security company

We believe in the pervasive, rapidly evolving and increasingly complex nature of cyber criminality …

… our mission is to optimise our clients´ cyber risk management capabilities

… to mitigate financial, reputational and customer losses

S21sec

Colaboraciones con LEA's e instituciones gubernamentales

S21sec

Miembro activo de multitud de forums internacionales de ciberseguridadcc

Contexto Global

Contexto global y tendencias

La ciberseguridad es un asunto candente y figura en la agenda de los CxO

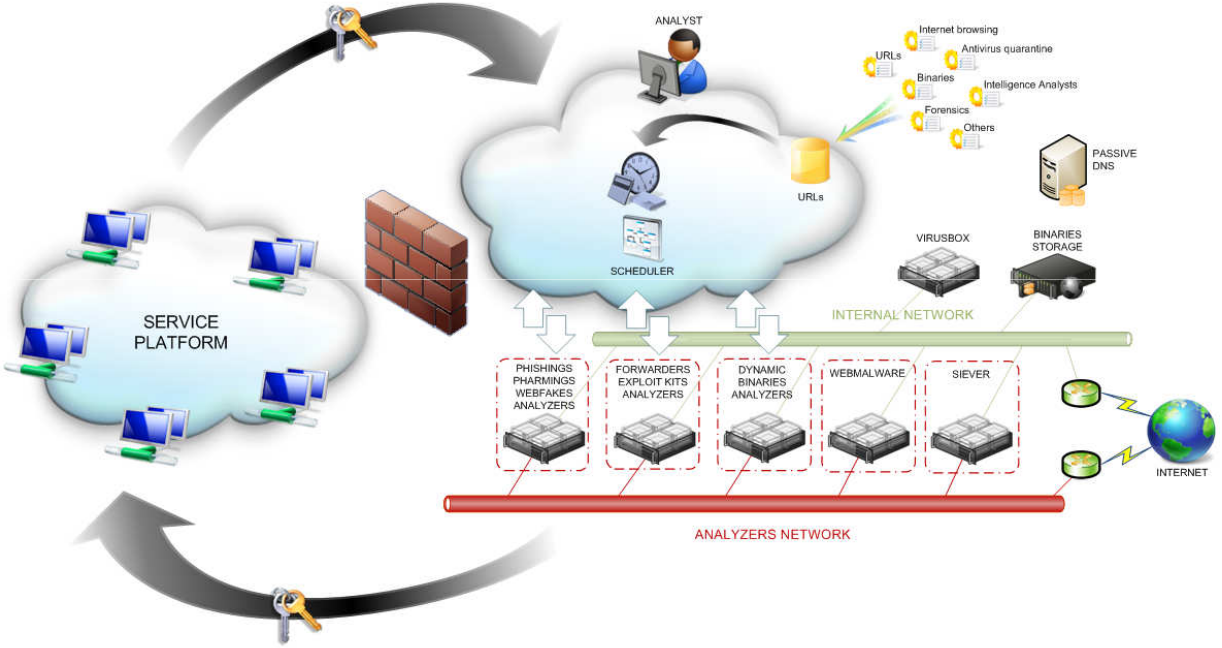
Global Study of Boardroom Issues and C-Suite Concerns

1. Regulatory changes and scrutiny may affect how our products/ services are produced or delivered
2. Economic conditions may significantly restrict growth opportunities
3. Our organisation may not be sufficiently prepared to manage cyber threats that have the potential to significantly disrupt core operations and/ or damage our brand
4. Our organisation´s succession challenges and ability to attract and retain top talent may limit our ability to achieve operational targets
5. Our organisation´s culture may not sufficiently encourage the timely identification and escalation of risk issues that have the potential to significantly affect our core operations and achievement of strategic objectives
6. Resistance to change may restrict our organisation from making necessary adjustments to the business
7. Ensuring privacy / identify management and information security / system protection may require significant resources
8. Our organisation may not be sufficiently prepared to manage an unexpected crisis significantly impacting our reputation

Protiviti, Executive Perspectives on Top Risks, 2015

El entorno

Observación del medio desde nuestras plataformas de servicio



Número de muestras detectadas por S21sec afectando a marcas relevantes

Año	Entidades	Paises	Sectores
2012	1898	95	18
2013	2066	100	20
2014	2284	105	21
2015	2535	110	22

41.248 handled incidents

5.792.938 Malicious URLs

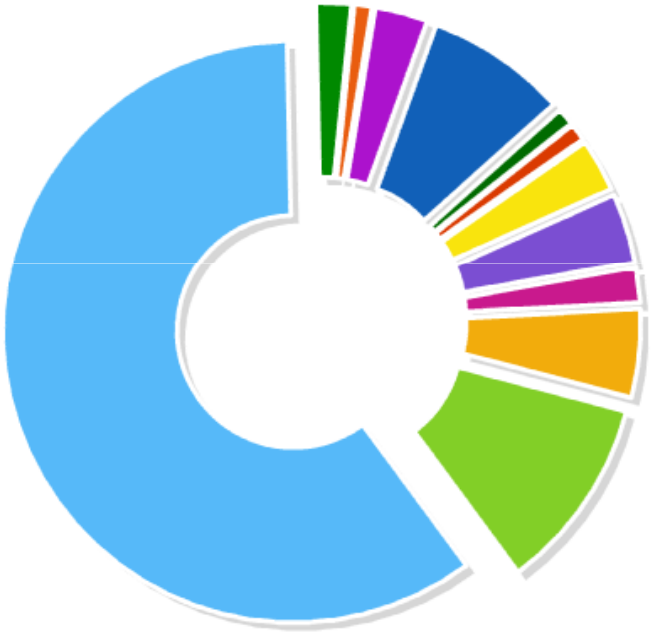
+

14 DGA (23.000 daily domains)

Distribución de Malware

Segmentación de tipos de malware

Mas de 250 familias distintas detectadas



Tipos de malware detectados en 2015

- Adware
- APT/RAT
- Banking trojan
- Clickfraud
- CoinMiner
- DDoS
- Downloader
- Fake AV
- Generic Keylogger
- POS Malware
- Ransomware
- SPAM

Incidentes y Respuesta

Observación

Evolución continua de las tendencias y adaptación al medio

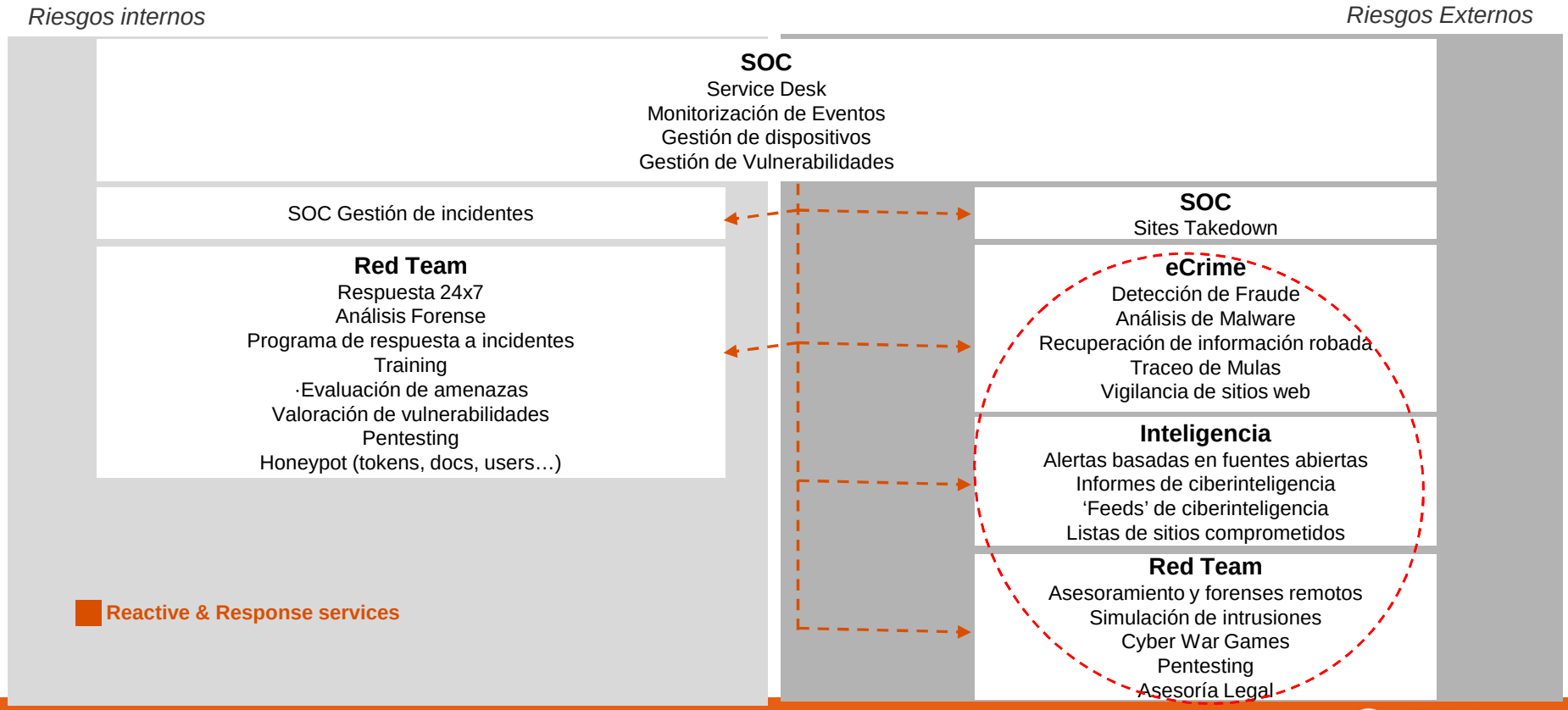
La fase de detección de amenazas es una de las mas importantes en el ciclo de detección de fraude online, principalmente porque una resolución efectiva depende de una detección temprana y una gestión adecuada del incidente. Detectados en su momento, la mayor parte de los incidentes de fraude tendrán un alcance limitado sin suponer un impacto financiero. El proceso de detección debe ser PROACTIVO, es decir, es un proceso de búsqueda activa de nuevas amenazas. **No puede limitarse a la actualización de contramedidas convencionales.**

Sigan nuestro blog. Mas novedades en breve!

- 26 SEP 2010 — Zeus Mitmo: Man-in-the-mobile
- 25 FEB 2011 — Tatanga: a new banking trojan with MitB functions
- 20 APR 2014 — NeoPocket: A new ATM malware
- 25 JUL 2014 — New Feodo variant follows Geodo steps
- 04 AUG 2014 — Kronos is here...
- 20 OCT 2014 — New malware targeted attacks on ATMs hit the banking industry
- 28 NOV 2014 — Dridex Learns New Trick: P2P over HTTP
- 25 MAR 2015 — New banking trojan 'Slave' hitting Polish Banks

Equipos y servicios de respuesta

Perfiles de servicio a valorar en un esquema de respuesta ante incidentes



Contramedidas de seguridad lógica en el ATM

ATMs: Objetivo de los ciberdelincuentes

Los ATM son muy atractivos para los atacantes:

- Contienen CASH y se rellenan periodicamente
- Gestionan información sensible: **Credit/Debit Cards & PINs**
- En ocasiones con poca vigilancia (factor emplazamiento)
- Seguridad lógica inmadura (comparada con la física)

Multiples vectores de ataque:

- **Ataques físicos**
- **Ataques lógicos**
  (Malware)
- **Lógico-Físicos**
  (Malware + Acceso físico al cajero)

Componente regional en los ataques

Ejemplos

ATM Cash-Out (Tyupkin / Ploutus)

Destino	Finalidad	MODUS OPERANDI
Instituciones financieras Latam, Europa y Asia Pérdidas acumuladas de Millones de dólares	**Goal:** Extraer el cash directamente del dispensador del cajero **Vectores:** Manipulación del disco duro Infección Malware	▪ Acceso físico al Top-Box del cajero ▪ Arranque desde dispositivo externo ▪ Desabilitación de las contramedidas de seguridad e infección por malware ▪ Reboot del ATM que carga el malware ▪ El cajero queda a la espera de comandos en el Pin-Pad para ganar control ilegítimo del dispensador y extraer el cash

References: http://securityblog.s21sec.com/2014/10/new-malware-targeted-attacks-on-atms.html

Advanced Persistent Threat (Carbanak)

Destino	Finalidad	MODUS OPERANDI
+ 100 Instituciones Financieras + 30 paises Pérdidas acumuladas de Millones de dólares	Goal: Extraer el cash de los dispensadores del cajero Vectores: Alteración del software del cajero Infección por Malware	▪ Infectar sistemas corporativos: spear phishing y drive-by web attack ▪ Escalado de privilegios y movimientos laterales ▪ Espionaje y aprendizaje de las heramientas y procedimientos internos ▪ Ganar acceso a la infraestructura de gestión de los ATM para controlarlos ▪ Infección por malware de determinados ATM el malware cambia la denominación de los billetes ▪ También hay muestras de extracción directa del cash

Black Box Attack

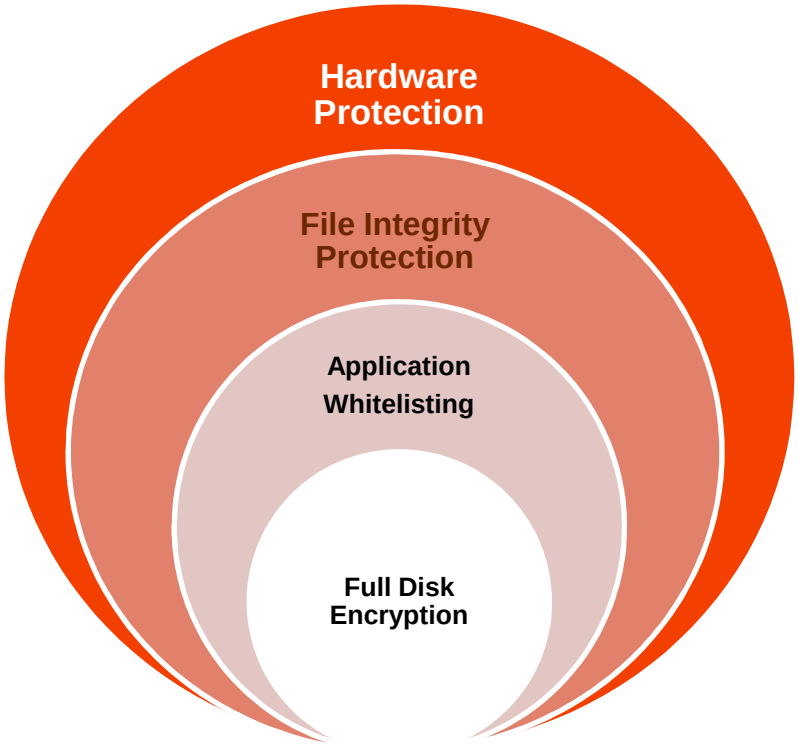
Destino	Finalidad	MODUS OPERANDI
Instituciones financieras **Pérdidas no evaluadas globalmente**	**Goal:** **Extraer directamente el cash de dispensador del cajero** **Vectores:** **Conexión de hardware manipulado**	▪ **Técnicos de mantenimiento corruptos o no autorizados** ▪ **Ganan acceso físico al Top-Box del cajero** ▪ **Desconectan el dispensador del cajero del sistema core** ▪ **Conectan al core un simulador del dispensador para evitar alarmas** ▪ **Conectan al dispensador un smart phone que emula el funcionamiento del core system y extraen el cash**

References: http://krebsonsecurity.com/2015/01/thieves-jackpot-atms-with-black-box-attack

Contramedidas necesarias

Modelo de protección en capas

Requerimiento de seguridad	¿Por qué?
Hardware Protection	*Evita la conexión de HW no confiable o manipulado*
File Integrity Protection	*Bloquea los intentos de reemplazar ficheros legítimos por otros manipulados o añadir nuevos ficheros (malware)*
Application Whitelisting	*Evita la ejecución de software no autorizado, manipulado o fraudulento*
Full Disk Encryption	*Evita el acceso a la información almacenada en el disco duro del cajero cuando el cajero está off-line, eliminando así la posibilidad de espionaje, robo de información o manipulación del sistema de protección*



Aplicabilidad de las distintas medidas en casos prácticos

ATAQUE	CONTRAMEDIDA
Tyupkin/Ploutus Manipulación del disco duro	Full Disk Encryption: para evitar el acceso al disco duro offline y la manipulación de sus datos
Carbanak I Malware que cambia la denominación de los billetes	Application Whitelisting: para evitar la ejecución de SW no autorizado
Carbanak II Manipulación de aplicaciones corporativas	File Integrity Protection: Para evitar la manipulación del SW legítimo
Black Box Conexión de hardware manipulado	Hardware Protection: para evitar la conexión de HW no autorizado o manipulado

Aplicabilidad de contramedidas por vector de ataque

Vector de ataque	CONTRAMEDIDA
Infección por malware	Application Whitelisting: Evita la ejecución de software no autorizado File Integrity Protection: Evita la manipulación del software legítimo Hardware Protection: Evita la infección desde dispositivos externos Full Disk Encryption: Evita la inyección de malware en discos offline
Conexión de HW manipulado	Hardware Protection: Evita la conexión de hardware no autorizado
Alteración de las aplicaciones corporativas	File Integrity Protection: Evita la manipulación del SW legítimo del cajero

Aplicabilidad de contramedidas por vector de ataque

Vector de ataque	Contramedida
Manipulación o robo del disco duro	Full Disk Encryption: Evita el acceso a la información que almacena el disco
Acceso no autorizado con privilegios administrativos	Application Whitelisting: Evita la carga de software no autorizado a los administradores del sistema (*) User Control: Monitorización de cambios en los usuarios locales del cajero
Fuga de datos	Hardware Protection: Evita la conexión de dispositivos de almacenamiento
Espionaje y monitorización fraudulenta de la actividad del cajero	Application Whitelisting: Evita la ejecución de SW espia File Integrity Protection: Evita la inyección de software espia

Contramedidas necesarias (y algunas exquisiteces más)

Multi-Vendor Solution

Full Disk Encryption

Application Whitelisting

Centralized GUI

Hardware Protection

Remote Actions
Forensics

Monitoring of ANY control & SIEM Integration

File Integrity Protection

Limited Resource Consumption

// El ejemplo de PCI DSS

PCI DSS

- PCI DSS es un estándar que establece un conjunto de medidas, prácticas y herramientas de seguridad que pretenden garantizar la seguridad en el tratamiento de la información asociada a pagos con tarjeta.

- Este estándar alinea las principales iniciativas de seguridad para la infraestructura de medios de pago, con el fin de garantizar la existencia de un marco global consistente para la protección de los datos de cuentas bancarias, tarjetas, transacciones y datos de autenticación.

- El estándar ha sido creado por las principales empresas de tarjetas: Visa Internacional, MasterCard Worlwide, American Express, JCB y Discover Financial Services.

- En la actualidad, PCI DSS es gestionado, revisado y actualizado por el **PCI Security Standards Council**.

Objetivos de PCI DSS

- El principal objetivo de PCI DSS es mejorar el nivel de seguridad de los pagos realizados mediante tarjetas, promoviendo la existencia de un entorno de pago seguro para la información de tarjetas.
- PCI DSS ha sido específicamente desarrollado para:
  - ✓ Garantizar la protección de la información de titulares de tarjetas.
  - ✓ Minimizar el riesgo de posibles intrusiones no autorizadas o compromiso de la información de cuentas y tarjetas.
  - ✓ Incrementar la confianza de los titulares de tarjetas en las transacciones realizadas con tarjetas.
  - ✓ Luchar contra la suplantación y otros fraudes que se producen en Internet u otros canales.

Diapositiva 29

RRC8 Existen webs donde las tarjetas pueden comprarse por centimos de euro. Muxhas webs enseñan sobre tecnicas de hacking, herraminetas de libre acceso, etc.

Raul Rodriguez Celaya; 16/03/2015

Beneficios de PCI DSS

- Las organizaciones deben buscar el cumplimiento de PCI DSS con objeto de mitigar los riesgos asociados a un posible compromiso de la información de cuentas o titulares de tarjetas:
  - Impacto financiero.
  - Impacto negativo en la imagen pública o frente a clientes que podría sufrir su marca.
  - Costes de investigación y costes legales asociados a un posible compromiso de información.

Alcance de PCI DSS

- El alcance de PCI DSS comprende todos aquellos **componentes de sistemas** que almacenan, procesan o transmiten información de tarjetas de crédito o débito así como los **sistemas conectados** a estos.
- Los componentes del sistema incluyen, a modo de ejemplo:
  - Sistemas que ofrecen servicios de seguridad (por ejemplo, servidores de autenticación), que facilitan la segmentación (por ejemplo, firewalls internos) o que pueden afectar la seguridad del CDE (por ejemplo, servidores de resolución de nombres o de redireccionamiento web).
  - Componentes de virtualización, como máquinas virtuales, interruptores/routers virtuales, dispositivos virtuales, aplicaciones/escritorios virtuales e hipervisores.
  - Los componentes de red incluyen, a modo de ejemplo, firewalls, interruptores, routers, puntos de acceso inalámbricos, aplicaciones de red y otras aplicaciones de seguridad.
  - Los tipos de servidores incluyen, a modo de ejemplo: web, aplicación, bases de datos, autenticación, correo electrónico, proxy, NTP (protocolo de tiempo de red) y DNS (servidor de nombre de dominio).
  - Aplicaciones, que abarcan todas las aplicaciones compradas y personalizadas, incluso las aplicaciones internas y externas (por ejemplo, Internet).
  - Cualquier otro componente o dispositivo ubicado en el CDE o conectado a este.

Alcance de PCI DSS

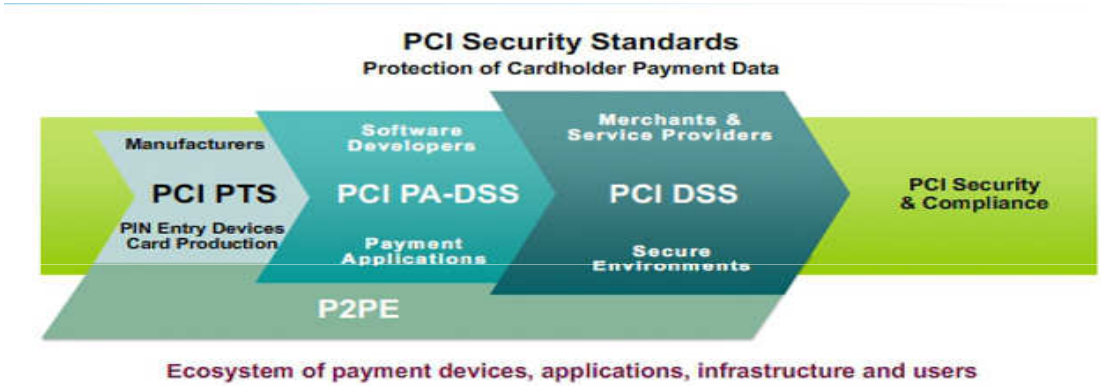
- Los requerimientos de PCI DSS aplican siempre que el PAN (Primary Account Number) de la tarjeta se almacena, procesa o transmite.

- PCI DSS aplica a los diferentes **canales** a través de los que se transmiten datos de tarjetas (TPV Físico, TPV Virtual, compensación, …)

// Introducción

PCI Security Standars

- El PCI council ha publicado los siguientes estándares.



- Todos ellos se complementan unos con otros cubriendo diferentes áreas.
- Incluyen seguridad desde el punto de producción y transmision de datos de tarjetas (P2P), entrada de datos de tarjetas en dispositivos seguros (PTS) , seguridad de aplicaciones (PA DSS) y seguridad en entornos (PCI DSS) de datos de tarjetas
- PCI DSS es el estándar mas importante para muchas organizaciones ya que provee el marco estratégico de seguridad para el entorno de IT

PCI Security Standars

https://es.pcisecuritystandards.org/security_standards/documents.php

- **PCI DSS** incluye la seguridad de los entornos que procesan, transmiten o almacenan datos de tarjetas
  - Estos entornos pueden recibir datos de tarjetas de aplicaciones de pago u otras fuentes (ej. Banco adquirente)
- **PCI PA-DSS** incluye la seguridad de aplicaciones de pago que permiten el cumplimiento de PCI DSS
  - Las aplicaciones de pago reciben los datos de tarjetas desde los PEDS (PIN-entry devices) u otros dispositivos e inician la transacción del pago
- **PCI P2PE** cubre la encriptación, desencriptación y gestión de claves para las soluciones de encriptación punto a punto (Ej. SNCP)
- **PCI-PTS POI** cubre la protección de datos de autenticación sensibles en los dispositivos de entrada de datos (Point of interaction devices –POI) y sus componentes de seguridad, incluyendo PIN y Datos de tarjetas, y claves criptográficas usadas para la protección de esos datos.
- **PCI PTS-PIN** cubre la gestión, procesamiento y transmisión seguros de los PIN (Personal identification number) durante los pagos online y offline
- **PCI PTS-HSM** cubre los requerimientos de seguridad física, lógica y de dispositivos para la securización de los HSM (Hardware Security Models)
- **PCI Card Production** cubre los requisitos de seguridad física y lógica y los procesos de negocio asociados a la personalización de tarjetas (estampación), Generación de PIN, envió y distribución de PIN y transportistas de tarjetas

PCI Security Standars

- **PCI DSS** aplica a todas las entidades involucradas en el procesamiento de pagos de tarjeta y cualquier entidad que almacena, procesa o transmite datos de tarjetas (PAN)
  - Incluye seguridad para cualquier componente de sistema incluido o conectado al entorno de tarjetas de pago (cardholder data enviroment _CDE) del comercio o proveedor
- **PA DSS y PCI DSS**
  - Las aplicaciones de pago PA DSS deben facilitar el cumplimiento de PCI DSS pero no lo garantizan ni lo suplen
  - Muchos de los requerimientos de aplicaciones de PA DSS coinciden con los que PCI DSS exige para las aplicaciones (Dominio 6)
- **P2PE y PCI DSS**
  - P2Pe incorpora requerimientos de PTS, PCI DSS, PA DSS y PCI PIN para proteger los datos de tarjetas desde el punto de captura de los datos hasta que llegan al procesador del pago.
  - Cuando una solución P2PE listada por el council esta correctamente implementada y mantenida, esta ayuda a reducir el alcance de las auditorias PCI de comercios

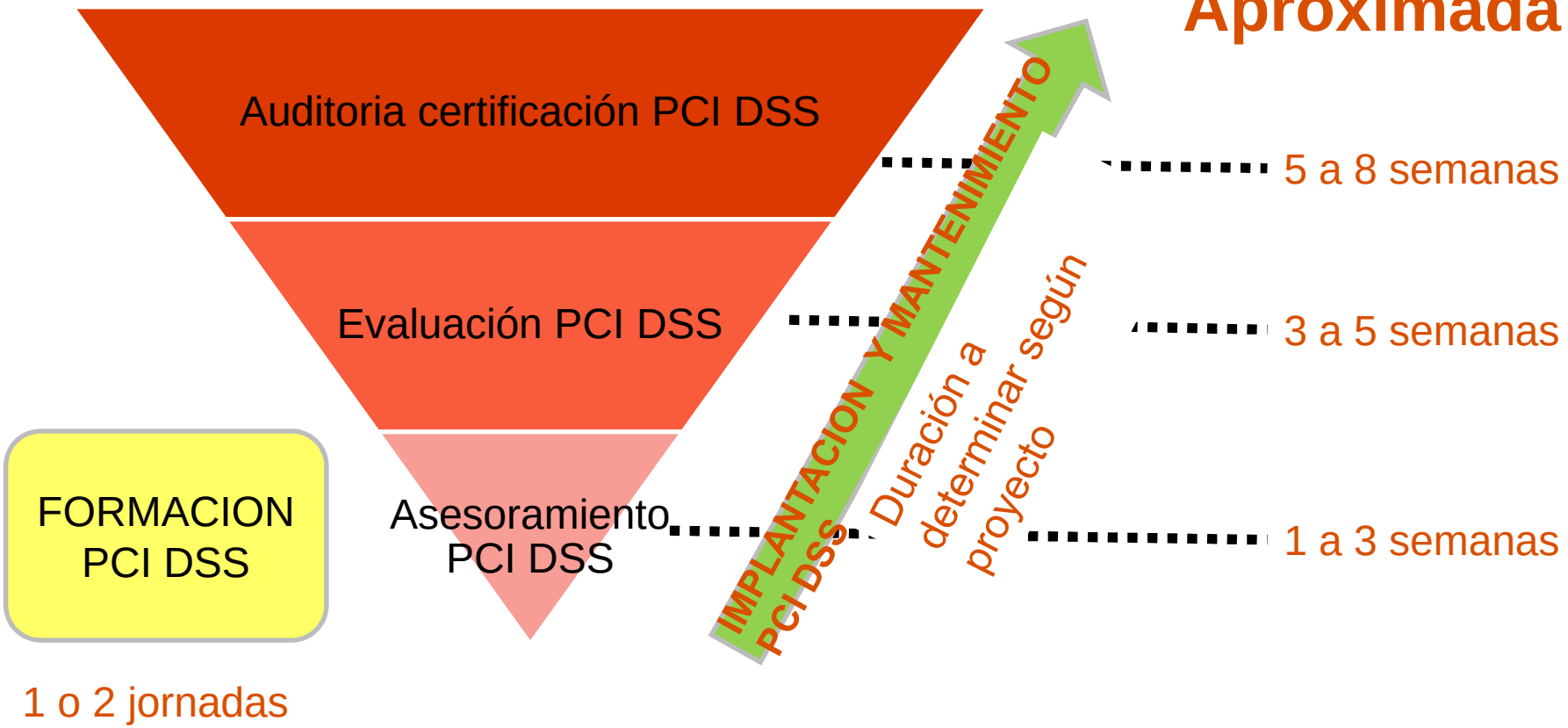
PCI Security Standars

- **PCI PTS-POI y PCI DSS**
  - PCI DSS requiere que los datos trasmitidos sean protegidos en su almacenamiento y transmisión a través de redes publicas
  - PCI PTS-POI establece como los POIs protegen el PIN, los datos de tarjetas y la gestión de claves criptográficas.
  - Los dispositivos certificados PCI PTS-POI podrían formar parte del entorno de certificación PCI DSS
- **PCI PTS- PIN Security Standar y PCI DSS**
  - PCI DSS prohíbe el almacenamiento de datos de PIN
  - No hay solapamiento entre estas normas ya que su alcance es diferente.
- **PCI PTS-HSM y PCI DSS**
  - PCI DSS exige que los datos de tarjetas almacenados deben ser protegidos y las claves de encriptación gestionadas de manera segura
  - El uso de un HSM no es necesario para cumplir PCI DSS pero puede ayudar con la gestión y manejo de las claves usadas para proteger los datos de tarjetas.
- **PCI Card Production y PCI DSS**
  - No hay solapamiento
  - Los procesos para evaluar los sistemas de producción de tarjetas son definidos por las marcas de pago directamente. El council únicamente ha publicado dos normativas para alinear las prácticas de la industria

PCI Security Standars

- **Resumen:**
  - **PCI DSS no es un proyecto trivial, requiere un esfuerzo importante, máxime si se trata de la primera certificación**

Datos típicos de esfuerzo del proyecto



Requisitos de Revalidación

American Express	Discover	JCB	MasterCard
• Compliance validation documents are due yearly	• Annual revalidation is due 12 months from the date full compliance was achieved as indicated by the Attestation of Compliance (AOC)	• Please contact JCB directly	• Annual revalidation is due 12 months from the Attestation of Compliance (AOC) date • QSAs must provide the PCI SSC Attestation of Compliance for Onsite Assessments – Service Providers form to MasterCard - ROCs are not accepted • A compliant AOC must be provided prior to the due date. AOCs will be considered delinquent thereafter and may result in delisting from the listing of compliant service providers on the MasterCard Web site and also may result in non-compliance assessments to the appropriate acquirers.

Requisitos de Revalidación

Visa Inc.	Visa Europe
• Annual revalidation is due 12 months from date of ROC acceptance • Validation documentation must be accepted prior to due date • Validation documentation is delinquent thereafter, with the list entry color-coded to indicate: - Up to 60 days late (yellow) - Greater than 60 days late (red) • Once 90 days late, Service Provider will be removed until validation documentation received and accepted	**Member Agent** • Annual revalidation is due 12 months from date of ROC acceptance • Validation documentation is delinquent thereafter, with the list entry color-coded to indicate: - Up to 60 days late (yellow) - Greater than 61 days late (red) • Once 90 days late, Service Provider will be removed until validation documentation received and accepted **Member Agent** • Sixty days from expiry of ROC/SAQ

Requisitos de Reporte de Proveedores de Servicio

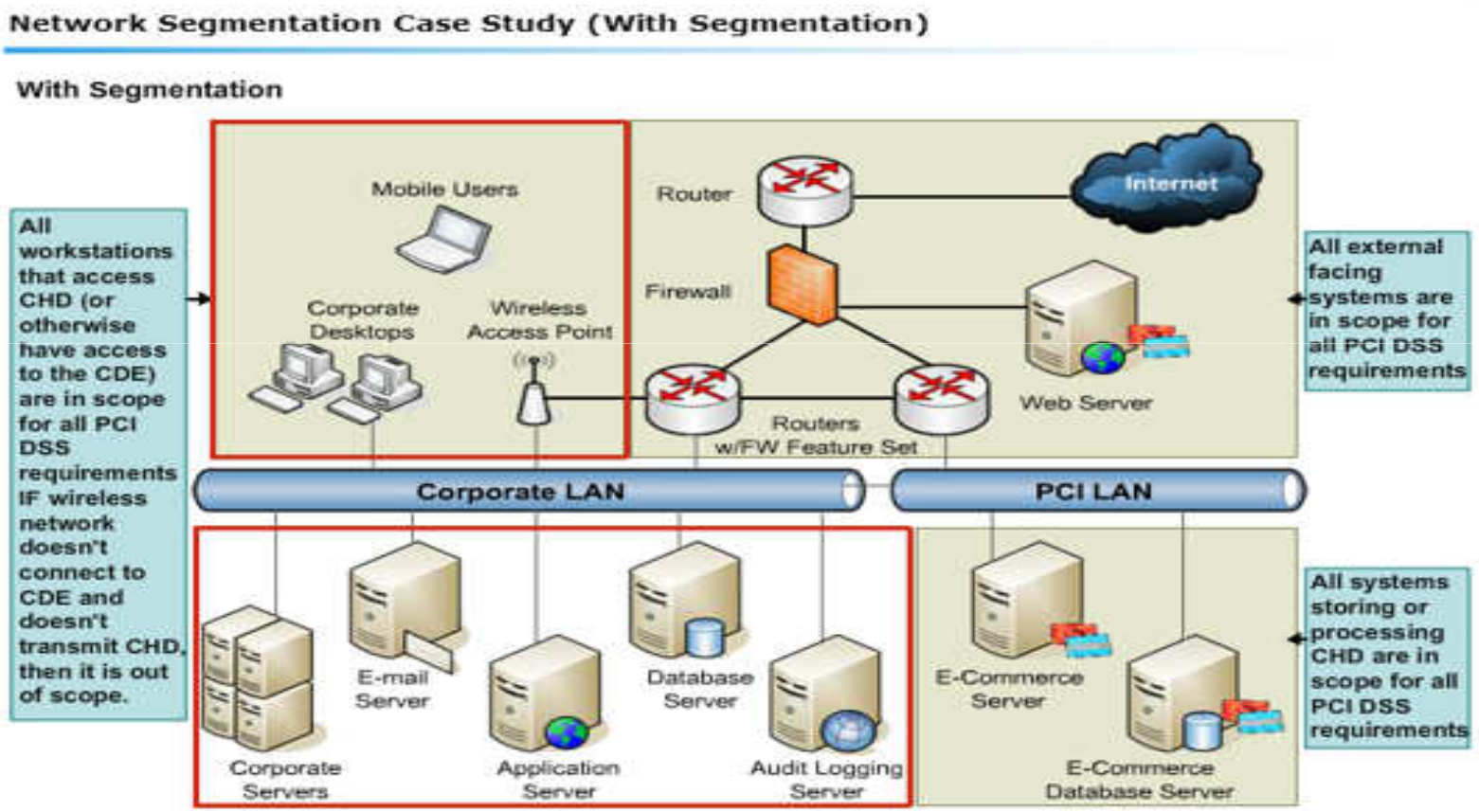
Discover	JCB	MasterCard
• Attestation of Compliance – Service Providers from Report on Compliance for Level 1 Service Providers -OR- • Attestation of Compliance – Service Providers from SAQ D for Level 2 Service Providers • If not fully compliant, must also complete the Action Plan for Non-Compliant Status section of the Attestation of Compliance • Send reports to: DISCCompliance@discover.com	• No reporting requirement at this time	• Attestation of Compliance (AOC) for Onsite Assessments – Service Providers -OR- • Attestation of Compliance (AOC) for Self-Assessment Questionnaire D – Service Providers • Send AOC to PCIReports@MasterCard.com • MasterCard will not accept or review a ROC (Report on Compliance) • For noncompliant service providers, a PCI Action Plan is required (only for new registrations) • Service Providers will not be listed on the MasterCard website of compliant service providers until AOC is received For further information: • http://www.mastercard.com/us/company/en/whatwedo/service_provider_level.html

*Discover reserves the right to request a full ROC or SAQ

Requisitos de Reporte de Proveedores de Servicio

Visa Inc.	Visa Europe
• Attestation of Compliance (Third Party Agents) and Full ROC and Attestation of Compliance (VisaNet Processors) must be submitted to Visa – send to pcirocs@visa.com and AP-CEMEA region send to VPSSAIS@visa.com • Service providers MUST BE registered with Visa before being added to list. For additional information send an email to: Americas - AgentRegistration@visa.com AP-CEMEA - agents@visa.com • For Visa AP, visit http://www.visa-asia.com/ap/sea/merchants/riskmgmt/vrsp_index.shtml for information about the Direct Registration Program • Global Registry of Service Providers is published here: http://www.visa.com/splisting	• Service Providers (Member Agents) - ROC, QSA confirmation form Attestation of Compliance form etc. must be submitted to Visa – send to pcidsseurope@visa.com • Merchants Agents – Online submission via https://www.visamerchantagents.com/ • Service providers MUST BE registered with Visa by a Visa Europe Member before being added to list – email agentcompliance@visa.com for information • Visa Europe's List of Compliant Service Providers is published on the AIS website: http://www.visaeurope.com/en/businesses__retailers/payment_security.aspx

Consejo uno. Limitar el alcance a los sistemas incumbentes.



Consejo dos. Contar con herramientas de monitorización adecuadas.

- **Recogida de datos universal**
  - Acceso a logs de sistemas
  - BBDD
  - Aplicaciones
  - Contramedidas
  - etc . . .
- **Automatización del muestreo de controles**
- **Automatización de los informes de cumplimiento**
- **Acceso forense al estado de determinados controles**
- **Incorporación de la información sobre vulnerabilidades**
- **Idealmente, gestión de activos**
  - **Operación basada en riesgo VS tecnología.**


//
Gracias
*


//
¿Preguntas?
*

linkedin.com/company/s21sec

facebook.com/pages/S21sec

twitter.com/@S21sec

SPAIN

MADRID
C/ Valgrande, 6
C.P. 28108
Alcobendas
T: +34 902 222 521
F: +34 91 6616679

BARCELONA
Passeig de Gracia,
56 - 4.D
C.P. 08007
T.: +34 902 222 521
F: +34 91 6616679

SAN SEBASTIÁN
P.E. Zuatzu.
Ed. Urgull, 2º
C.P. 20018
T.: +34 902 222 521
F: +34 91 6616679

PAMPLONA
PE. La Muga, 11-1
C.P. 31160
Orcoyen
T.: +34 902 222 521
F: +34 91 6616679

LEÓN
Avda. José Aguado, 41
Ed. INTECO
C.P. 24005
T: +34 902 222 521
F: +34 91 6616679

PORTUGAL

LISBOA
Rua do Viriato, 13B,
4º andar
1050-233 Lisboa
Portugal
T: +351 220 107 120
F: +351 220 107 121

PORTO
Lugar do Espido
-Via Norte
4470-177 Maia
Portugal
T: +351 220 107 120
F: +351 220 107 121

MEXICO

MÉXICO DF
Mariano Escobedo 510, planta alta
Colonia anzures
Delegación Miguel Hidalgo
11590 México D.F.
T: +52 55 33 00 52 00

UK

READING
Davidson House
Forbury Square
Reading
RG1 3EU
United Kingdom
T: +44 1189 001 062
F: +44 1189 001 063

www.s21sec.com

THANKS

S21sec

Committed to cybersecurity