



Ecuador
SEGURINFO 2011

XIII Congreso y Feria Interamericana de Seguridad de la Información

**EL STANDARD PCI
DE MEDIOS DE
PAGO**



USUARIA

1



Ecuador
SEGURINFO 2011

XIII Congreso y Feria Interamericana de Seguridad de la Información

Presentada por:

Pablo Milano
(CISSP / QSA / PA-QSA)
Cybsec S.A.



CYBSEC[®]
Security Systems

Aclaración:

- © Todos los derechos reservados. No está permitida la reproducción parcial o total del material de esta sesión, ni su tratamiento informático, ni la transmisión de ninguna forma o por cualquier medio, ya sea electrónico, mecánico, por fotocopia, por registro u otros métodos, sin el permiso previo y por escrito de los titulares de los derechos. Si bien este Congreso ha sido concebido para difusión y promoción en el ámbito de la profesión a nivel internacional, previamente deberá solicitarse una autorización por escrito y mediar la debida aprobación para su uso.

Agenda

- ◇ Casos reales de robo de información de tarjetas de pago
- ◇ Payment Card Industry Security Standards Council (PCI-SSC)
- ◇ Requisitos de validación de cumplimiento
- ◇ Qualified Security Assessor (QSA / PA-QSA)
- ◇ PCI Data Security Standard (PCI-DSS)
- ◇ Payment Application Data Security Standard (PCI PA-DSS)
- ◇ Verificaciones técnicas periódicas de seguridad
- ◇ Preguntas y respuestas

Casos Reales



Junio de 2005: Un intruso, abusando una vulnerabilidad en el sistema logró acceder a la red de la empresa “Card Systems”, un procesador de transacciones de pago. De allí robó información de más de **40 millones de tarjetas de crédito y débito**, que luego fueron utilizadas en estafas. Este fue uno de los mayores robos de información de tarjetas de pago de la historia.

Agosto de 2007: La cadena de retail estadounidense “TJX” detectó que atacantes lograron robar más de **94 millones de registros** de tarjetas de crédito y débito.

La investigación posterior mostró que la fuga de información había comenzado 8 meses antes. **No cumplía con PCI-DSS**

La empresa enfrentó demandas de sus clientes y multas de las firmas de tarjetas de crédito



Casos Reales



enero de 2007: Se investigó un probable robo de información de tarjetas de pago de la cadena de indumentaria “Club Monaco” en Canada.

Los bancos emisores de las tarjetas involucradas estuvieron siguiendo de cerca los consumos de sus clientes, con el fin de detectar signos de estafas.

marzo de 2008: La cadena de retail estadounidense “Hannaford Brothers” detectó que atacantes lograron obtener **4, 2 millones de registros de tarjetas de crédito y débito** (PANs, PINs y fechas de expiración).

Parentemente el robo se realizó a través de un compromiso de las redes wireless de la compañía.

La compañía estaba **certificada PCI-DSS 1.1**

La empresa enfrentó demandas de sus clientes y multas de las firmas de tarjetas de crédito



Casos Reales

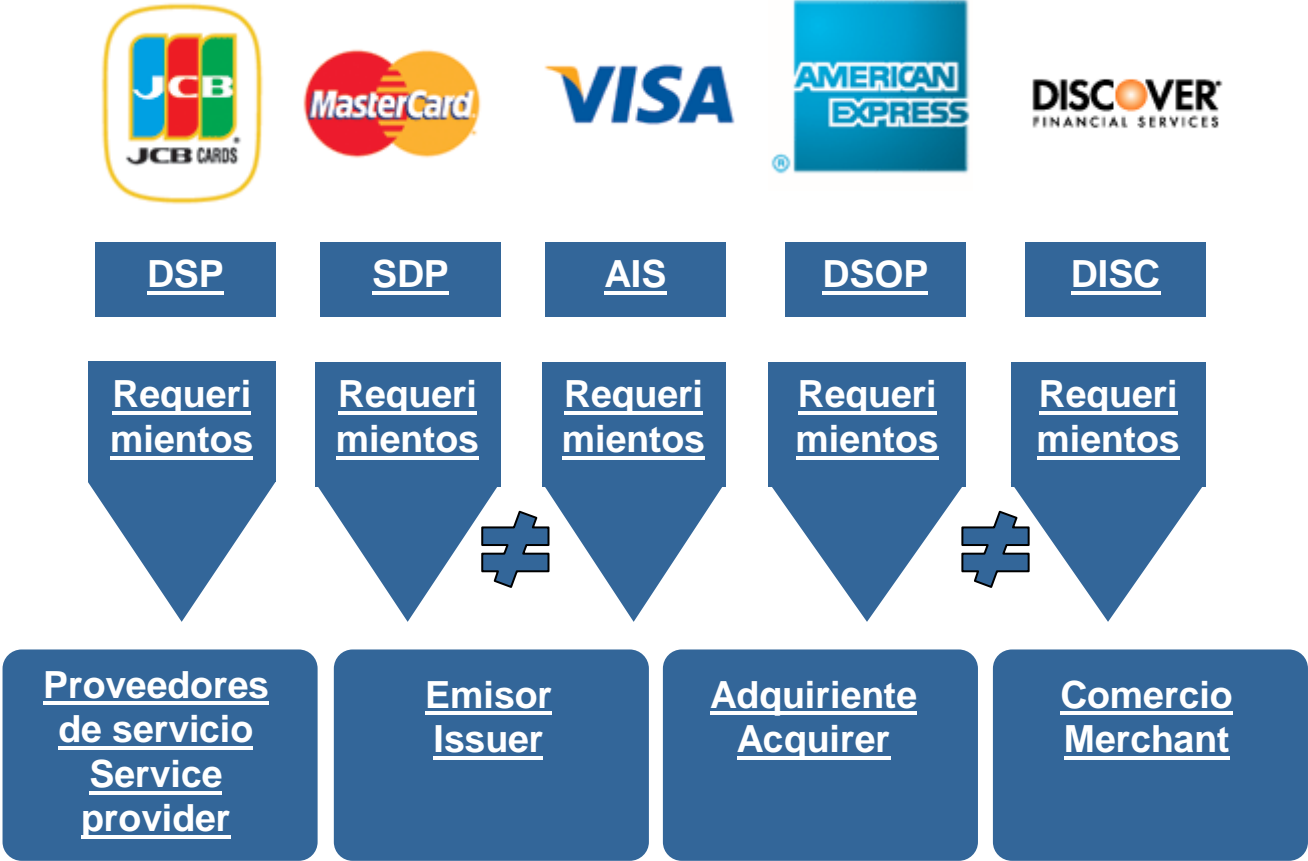
Enero de 2009: El procesador de tarjetas norteamericano “Heartland Payment Systems” sufrió un compromiso a sus sistemas informáticos, que dio lugar al robo de millones de datos de tarjetas de crédito y débito.



Enero de 2010: Se detectó que atacantes accedieron a las bases de sistemas de pago de al menos 37 cadenas hoteleras de la empresa “Wyndham”. Al parecer, el robo de información comenzó en octubre de 2009, y recién fue descubierto 3 meses después.

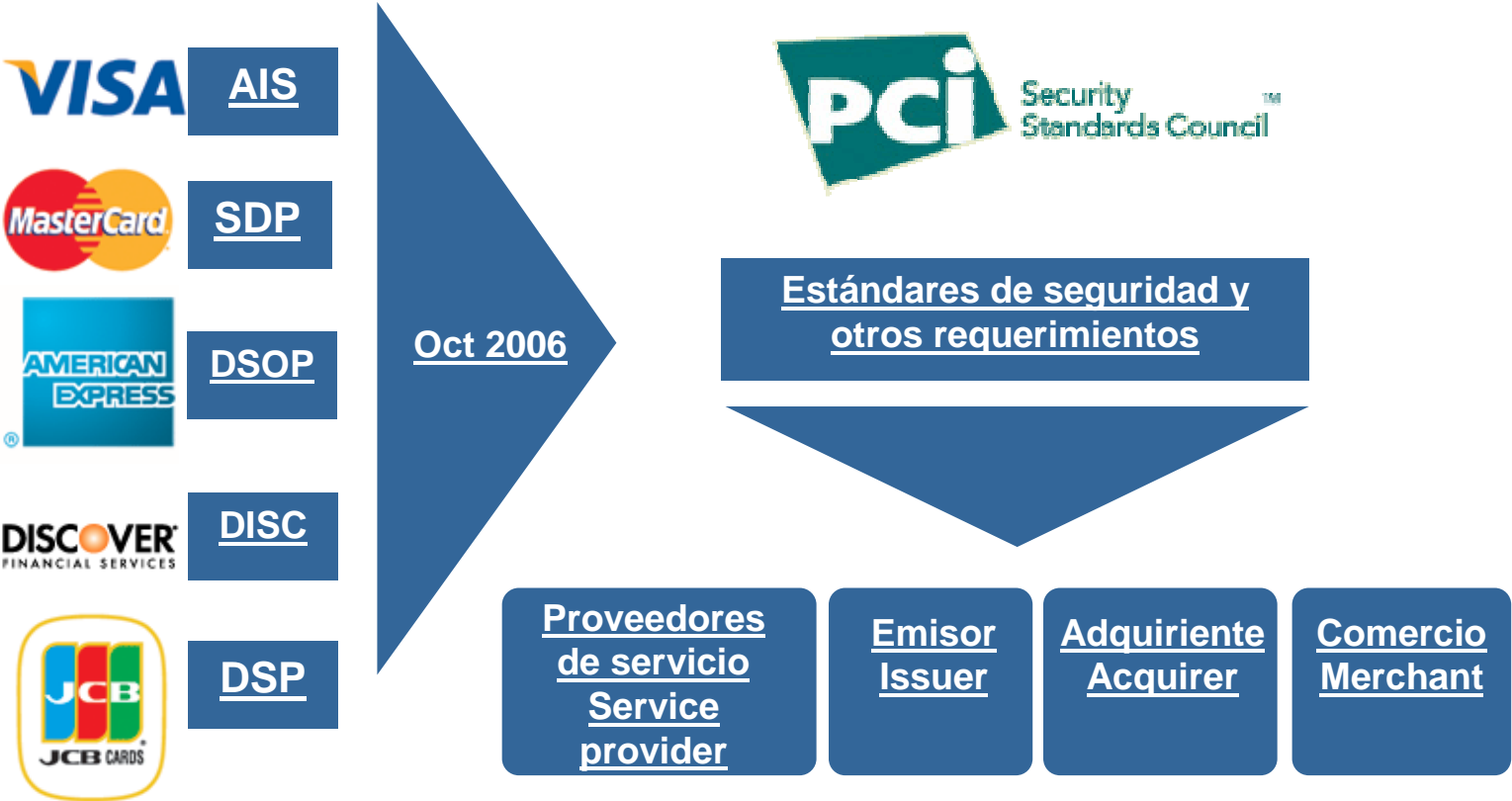
Payment Card Industry Security Standards Council (PCI SSC)

Antes de octubre de 2006: Cada marca de tarjetas tenía su propio programa de requerimientos de seguridad.
Actividad descoordinada.



Payment Card Industry Security Standards Council (PCI SSC)

El 1º de octubre de 2006, se forma el PCI SSC para coordinar y administrar los esfuerzos conjuntamente para combatir el robo de datos de titulares de tarjetas.



Payment Card Industry Security Standards Council (PCI SSC)

Objetivos del PCI SSC



Proveer una única voz a nivel global sobre la industria

Entrenar, testear y certificar
*QSAs/ASVs/PA-QSAs/ISA y laboratorios PED

Crear conciencia y dirigir la adopción de los estándares.

Emitir estándares de seguridad y administrar su ciclo de vida.

Fortalecer la seguridad en el manejo de cuentas de tarjetas

Fomentar la participación de la comunidad.

Payment Card Industry Security Standards Council (PCI SSC)

Actores

Titular de tarjeta Cardholder	Toda aquella persona que posee una tarjeta de crédito y débito.
Marca de pago Payment Brand	Organización de procesamiento que licencia a los miembros y comercios la emisión y aceptación de tarjetas de crédito respectivamente. Ej.: Visa, Mastercard, AMEX, etc.
Emisor Issuer	Institución financiera (miembro licenciado de una marca de pago) que mantiene contratos y emisiones de tarjetas con los tarjetahabientes. Es la responsable de la administración de las cuentas de los tarjetahabientes, y aprobar las solicitudes de autorización.
Adquiriente Acquirer	Miembro de una marca de pago que mantiene relaciones y cuentas para los comercios que aceptan tarjetas de pago. Sirve como un intermediario entre los comercios y las marcas.
Comercio Merchant	Cualquier negocio que cumple con los estándares de calificación de una marca de pago, y que se encuentra aprobado por cualquier Adquiriente. El negocio acepta tarjetas de pago a cambio de algún bien o servicio.
Proveedores de servicio Service provider	Negocio que no es miembro de una marca de pago o comercio que se encuentre directamente relacionado al procesamiento, almacenamiento, transmisión e intercambio de información de la transacción o del tarjetahabiente. Incluyen a las organizaciones que proveen servicios a los comercios, organizaciones que controlan o pueden impactar en la seguridad de la información del tarjetahabiente. Ej.: Procesadores, Gateway de pago, proveedores de hosting.



Payment Card Industry Security Standards Council (PCI SSC)

Elementos para la alineación



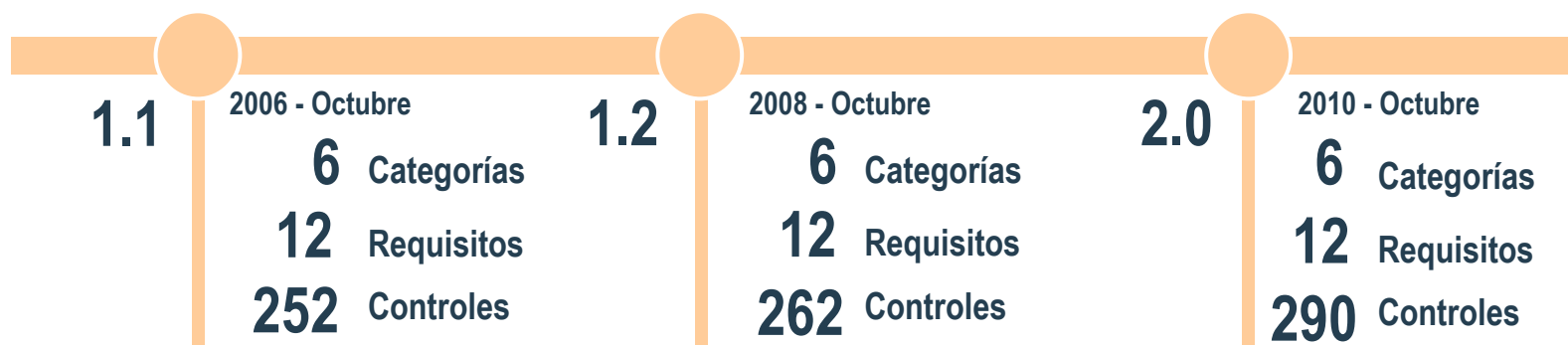
Gestión de los estándares	Entrenamiento de asesores	Otorgamiento de certificaciones	Declaraciones de cumplimiento
<p>DSS: Data Security Standards</p> <p>PA-DSS: Payment Application - Data Security Standards</p> <p>PTS: PIN Transaction Security</p>	<p>QSA: Qualified Security Assessor</p> <p>ASV: Approved Scanning Vendor</p> <p>PA-QSA: Payment Application – Qualified Security Assessor</p> <p>ISA: Internal Security Assessor</p>	<p>Lista de empresas QSA aprobadas</p> <p>Lista de asesores QSAs aprobados</p> <p>Lista de PA-QSAs aprobados</p> <p>Lista de aplicaciones aprobadas</p> <p>Lista de ASVs aprobados</p> <p>Lista de PTSD aprobados</p>	<p>Formularios de cumplimiento de DSS (SAQ, ROC y AOC)</p> <p>Formularios de cumplimiento de PA-DSS</p> <p>Laboratorios PTSD</p> <p>SAQ: Self assessment questionnaire</p> <p>ROC: Request of Compliance</p> <p>AOC: Attestation of Compliance</p>



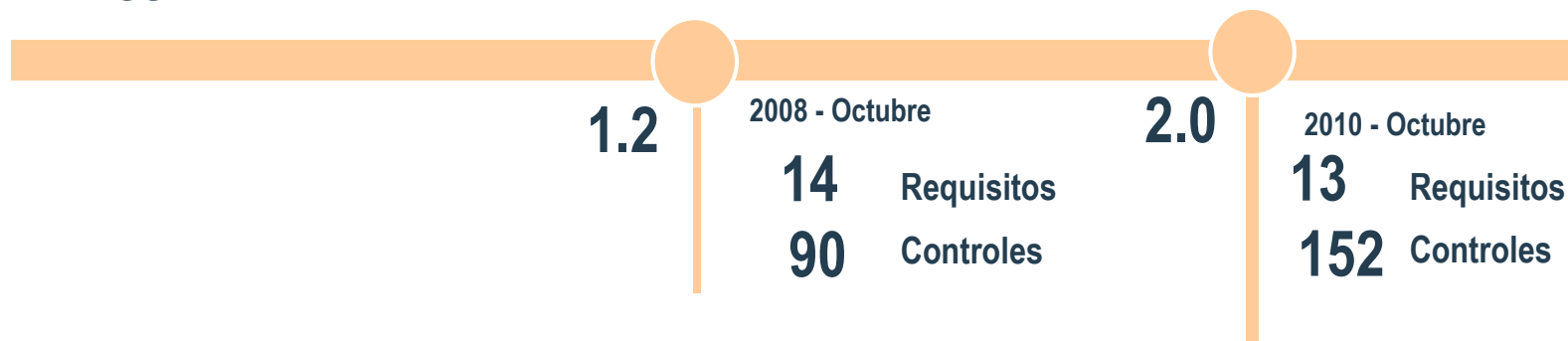
Payment Card Industry Security Estándards Council (PCI SSC)

Estándares y ciclo de vida

PCI-DSS

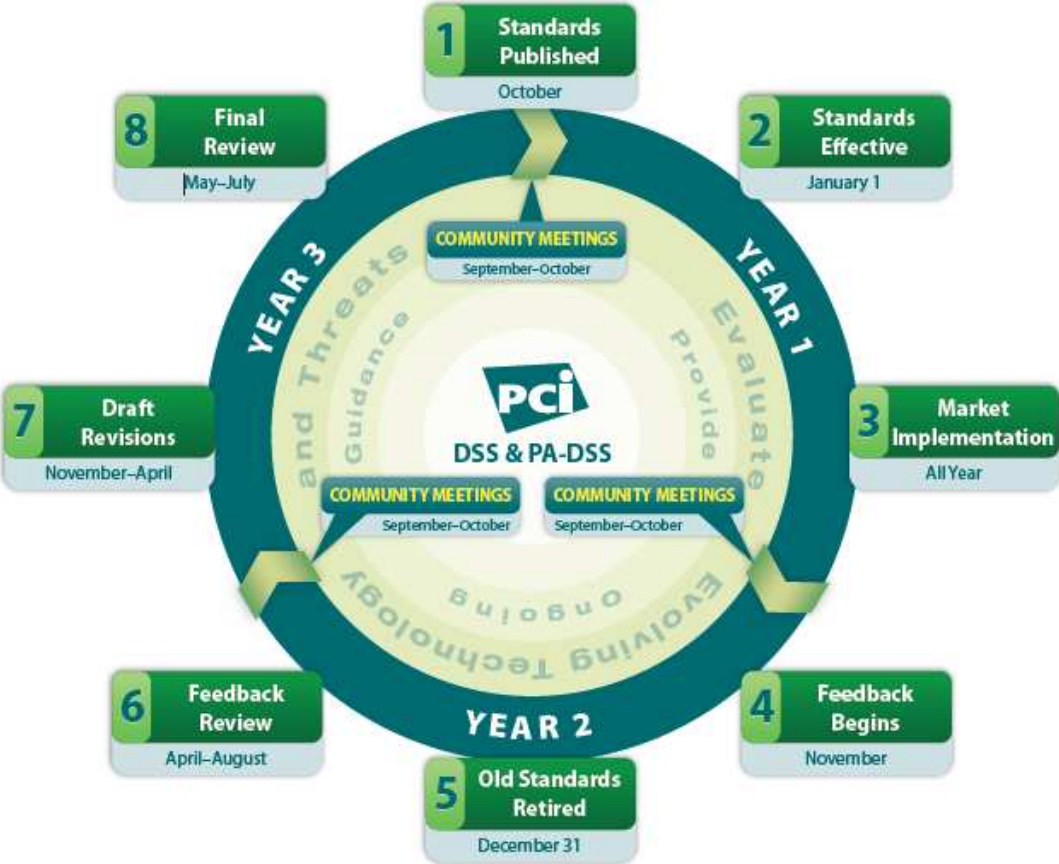


PA-DSS



Payment Card Industry Security Standards Council (PCI SSC)

Nuevo ciclo de vida para PCI DSS y PA-DSS (a partir de versión 2.0)



- Ciclo de 3 años
- Alineado a año calendario
- Incluye etapas de feedback

Ref:
www.pcisecuritystandards.org



Payment Card Industry Security Standards Council (PCI SSC)

¿Quiénes deben demostrar cumplimiento?

Requisitos de cumplimiento



Payment Card Industry Security Standards Council (PCI SSC)

¿Quiénes deben demostrar cumplimiento?

PCI DSS - COMERCIOS

<p>1</p> <p>6.000.000</p>	<p>Más de 6 millones de transacciones anuales de VISA o comercios globales identificados como Nivel 1 por VISA fuera de USA.</p> <ul style="list-style-type: none"> * Auditoría on site anual realizada por un QSA * Escaneos trimestrales realizados por un ASV * Formulario de Testimonio de Cumplimiento 	<p>Más de 6 millones de transacciones MasterCard anualmente, aquellos que sean identificados como Nivel 1 por otra marca, o comercios que hayan experimentado algún compromiso de datos de tarjetas</p> <ul style="list-style-type: none"> * Auditoría on site anual realizada por un QSA * Escaneos trimestrales realizados por un ASV
<p>2</p> <p>1.000.000</p>	<p>Comercios que procesen de 1 a 6 millones de transacciones VISA anualmente</p> <ul style="list-style-type: none"> * Escaneos trimestrales realizados por un ASV * Formulario de Testimonio de Cumplimiento * Cuestionario de Autoevaluación anual 	<p>Comercios que procesen de 1 a 6 millones de transacciones MasterCard anualmente o comercios que sean calificados como Nivel 2 en otras marcas</p> <ul style="list-style-type: none"> * Auditoría on site anual realizada por un QSA * Escaneos trimestrales realizados por un ASV
<p>3</p> <p>20.000</p>	<p>Comercios que procesen 20.000 a 1 millón de transacciones VISA e-commerce anualmente</p> <ul style="list-style-type: none"> * Cuestionario de Autoevaluación anual * Escaneos trimestrales realizados por un ASV 	<p>Comercios que procesen 20.000 a 1 millón de transacciones MasterCard e-commerce anualmente o comercios que sean identificados como Nivel 3 por otras marcas</p> <ul style="list-style-type: none"> * Cuestionario de Autoevaluación anual * Escaneos trimestrales realizados por un ASV
<p>4</p>	<p>Comercios que procesen menos de 20.000 transacciones VISA e-commerce anualmente, u otros comercios que procesen hasta 1 millón de transacciones VISA anualmente</p> <ul style="list-style-type: none"> * Cumplimiento a discreción del Adquiriente * Cuestionario de Autoevaluación recomendado * Escaneos trimestrales realizados por un ASV recomendado 	<p>Los demás comercios que procesen MasterCard</p> <ul style="list-style-type: none"> * Cumplimiento a discreción del Adquiriente



Payment Card Industry Security Standards Council (PCI SSC)

¿Quiénes deben demostrar cumplimiento?

PCI DSS – Procesadores y Proveedores de servicio

1

300.000

Procesadores de VisaNet o cualquier proveedor de servicio que almacene, procese o transmita más de 300.000 transacciones anualmente

- * Auditoría on site anual realizada por un QSA
- * Escaneos trimestrales realizados por un ASV
- * Formulario de Testimonio de Cumplimiento



Todos los TPP (Third Party Processor)
Todos los DSE (Data Storage Entities) que almacenen, procesen o transmitan más de 300.000 transacciones anualmente combinadas entre MasterCard y Maestro

- * Auditoría on site anual realizada por un QSA
- * Escaneos trimestrales realizados por un ASV



2

Cualquier proveedor de servicio que almacene, procese o transmita menos de 300.000 transacciones anualmente

- * Escaneos trimestrales realizados por un ASV
- * Formulario de Testimonio de Cumplimiento
- * Cuestionario de Autoevaluación anual

Todos los DSE (Data Storage Entities) que almacenen, procesen o transmitan menos de 300.000 transacciones anualmente combinadas entre MasterCard y Maestro

- * Escaneos trimestrales realizados por un ASV
- * Cuestionario de Autoevaluación anual



Payment Card Industry Security Standards Council (PCI SSC)

¿Quiénes deben demostrar cumplimiento?

PCI PA-DSS - Desarrolladores de aplicaciones de pago

Todas las empresas que comercialicen soluciones de software para pagos con tarjetas.

Se certifica una versión específica de software
Las marcas de tarjetas definen el requisito a los clientes de utilizar aplicaciones certificadas.

Listado oficial de aplicaciones certificadas:

- https://www.pcisecuritystandards.org/security_standards/vpa/vpa_approval_list.html

2 posibles estados:

- *Acceptable for new deployments*
- *Acceptable only for pre-existing deployments*

Payment Card Industry Security Standards Council (PCI SSC) Qualified Security Assessor

QSA

- Realiza las auditorias “On Site” de PCI DSS
 - (Comercios / Procesadores, etc)
- Envía el Reporte de Cumplimiento a las marcas de tarjetas

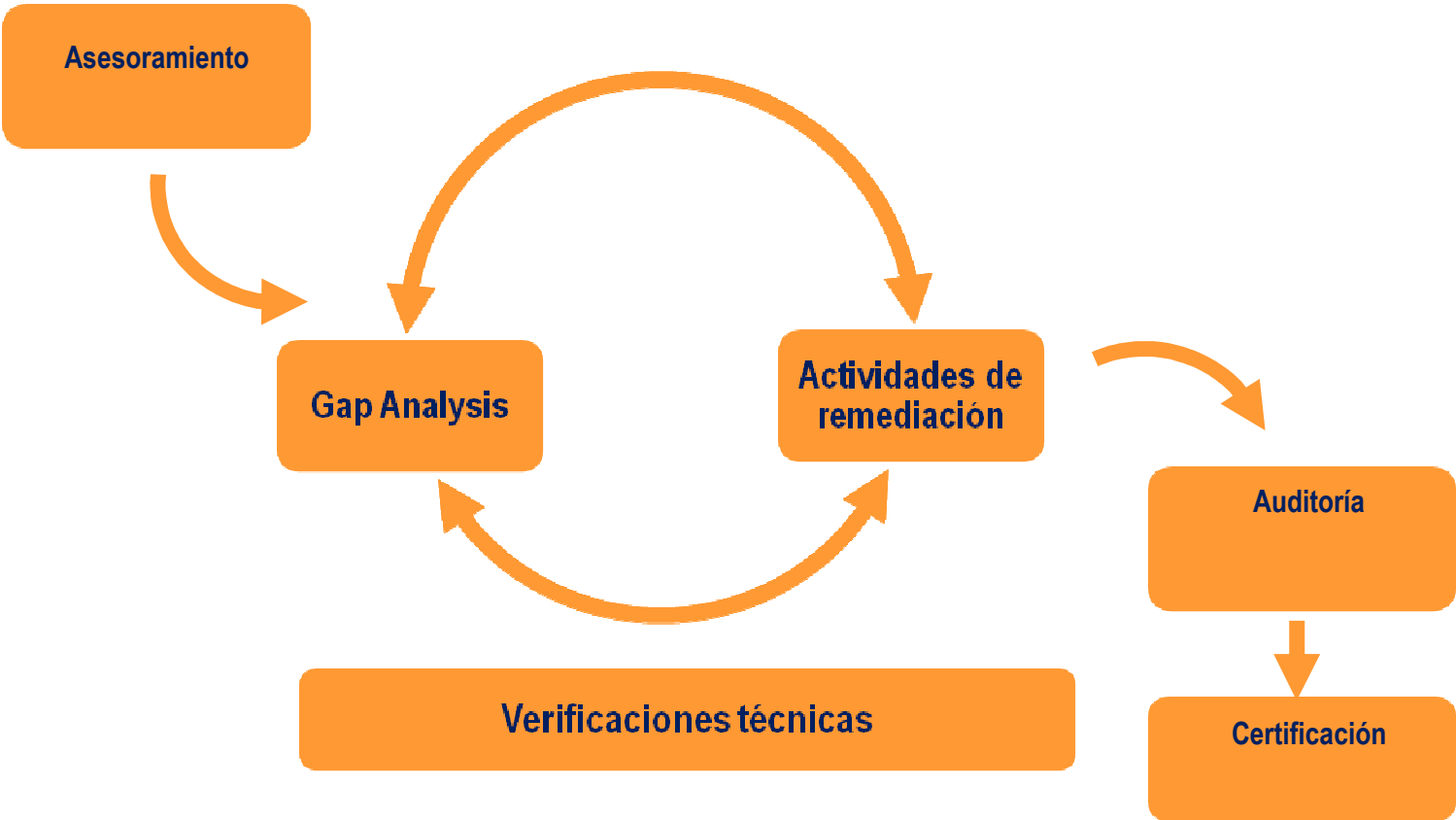
PA- QSA

- Realiza las auditorías de aplicaciones de pago
 - (Software , documentación y procesos)
- Envía los reportes de cumplimiento al PCI SSC.
- Tiene que ser primero QSA para poder luego ser PA-QSA

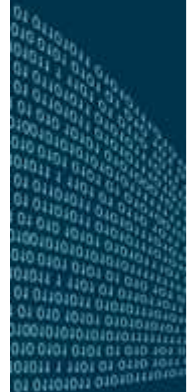
Listado oficial de QSAs y PA-QSAs:
https://www.pcisecuritystandards.org/qsa_asv/find_one.shtml

Payment Card Industry Security Standards Council (PCI SSC) Qualified Security Assessor

Proceso recomendado de cumplimiento



PCI DSS 2.0



Payment Card Industry Security Standards Council (PCI SSC) PCI DSS 2.0

1

Desarrollar y mantener una red segura

Requisito 1: Instale y mantenga una configuración de firewalls para proteger los datos de los titulares de las tarjetas

Requisito 2: No use contraseñas de sistemas y otros parámetros de seguridad provistos por los proveedores

Riesgos a mitigar

- Fuga de información a través de la red.
- Robo de información a través de la red
- Intentos o Incidentes a nivel de red
- Compromisos de dispositivos de comunicaciones.

2

Proteja los datos del titular de la tarjeta

Requisito 3: Proteja los datos del titular de la tarjeta que fueron almacenados

Requisito 4: Codifique la transmisión de los datos de los titulares de tarjetas a través de redes públicas abiertas.

Riesgos a mitigar

- Robo de información sensible
- Utilización de la información de titulares de tarjeta en fraudes.

Payment Card Industry Security Standards Council (PCI SSC)

PCI DSS 2.0

3

Desarrolle un programa de administración de vulnerabilidad

Requisito 5: Utilice y actualice regularmente el software o los programas antivirus

Requisito 6: Desarrolle y mantenga sistemas y aplicaciones seguras

Riesgos a mitigar

- Utilización de software malicioso como medio de compromiso de los equipos.
- Utilización de brechas de seguridad propias de los sistemas para el compromiso de los equipos.
- Plantación de código malicioso en sistemas, con distintos fines, por medio de actualizaciones o parches de seguridad no oficiales.

4

Implemente medidas sólidas de control de acceso

Requisito 7: Restrinja el acceso a los datos de los titulares de las tarjetas conforme a la necesidad de conocer de la empresa

Requisito 8: Asigne una ID única a cada persona que tenga acceso a equipos.

Requisito 9: Restrinja el acceso físico a datos de titulares de tarjetas.

Riesgos a mitigar

- Fuga de información a través de la aplicación, base de datos, etc.
- Robo de información a través de la aplicación, base de datos, etc.
- Suplantación de usuarios.
- Ataques contra cuentas de usuario.
- Impersonalización de usuarios.



Payment Card Industry Security Standards Council (PCI SSC) PCI DSS 2.0

5

Supervise y pruebe las redes con regularidad

Requisito 10: Rastree y supervise todo acceso a los recursos de red y datos de titulares de tarjetas.

Requisito 11: Pruebe con regularidad los sistemas y procesos de seguridad.

Riesgos a mitigar

- Presencia de troyanos, puertas traseras, etc.
- Fallas en las medidas de seguridad implementadas.
- Actividades no estipuladas en los sistemas
- Vulnerabilidades no identificadas.

6

Mantenga una política de seguridad de la información

Requisito 12: Mantenga una política de seguridad de la información

Riesgos a mitigar

- Detrimiento del nivel de seguridad.
- Errores intencionales o no en las actividades

PCI PA- DSS 2.0



Payment Card Industry Security Standards Council (PCI SSC) PCI PA-DSS 2.0

1

Proteger la información de tarjetas almacenada y en tránsito

Requisito 1: No retenga toda la banda magnética, el código de validación de la tarjeta ni el valor (CAV2, CID, CVC2, CVV2), ni los datos de bloqueo del PIN.

Requisito 2: Proteja los datos del titular de la tarjeta que fueron almacenados

Riesgos a mitigar

- Robo de datos sensibles de tarjetas almacenados en los sistemas de pago

2

Administrar el control de acceso a la aplicación y los datos

Requisito 3: Provea las funciones de autenticación segura

Requisito 4: Registre la actividad de la aplicación de pago

Riesgos a mitigar

- Accesos no autorizados a la aplicación de pagos
- “Repudio” de acciones realizadas en el sistema (por falta de auditoría)



USUARIA

Payment Card Industry Security Standards Council (PCI SSC) PCI PA-DSS 2.0

3

Ayudar al cliente a mantener una infraestructura segura

Requisito 6: Proteja las transmisiones inalámbricas

Requisito 8: Facilite la implementación de una red segura

Requisito 9: Los datos de tarjetas nunca se deben almacenar en un servidor conectado a Internet

Requisito 10: Facilite un acceso remoto seguro a la aplicación de pago

Requisito 11: Cifre el tráfico sensible de las redes públicas

Requisito 12: Cifre el acceso administrativo que no sea de consola

Riesgos a mitigar

- Implementaciones inseguras de la aplicación de pago por parte de los clientes
- Implementaciones inseguras de topología de red por parte de los clientes
- Captura de datos de tarjeta en redes inalámbricas o públicas
- Abusos del sistema de acceso remoto



Payment Card Industry Security Standards Council (PCI SSC) PCI PA-DSS 2.0

4

Mantener un proceso de desarrollo de software seguro

Requisito 5: Desarrolle aplicaciones de pago seguras

Requisito 7: Pruebe las aplicaciones de pago para tratar las vulnerabilidades

Riesgos a mitigar

- Vulnerabilidades en las aplicaciones de pago
- Vulnerabilidades en la plataforma que soporta la aplicación de pago.

5

Implementación de documentación formal sobre el producto

Requisito 13: Mantenga la documentación instructiva y los programas de capacitación para clientes, revendedores e integradores

Riesgos a mitigar

- Mala implementación de la aplicación de pago por falta de conocimiento o de instrucciones adecuada

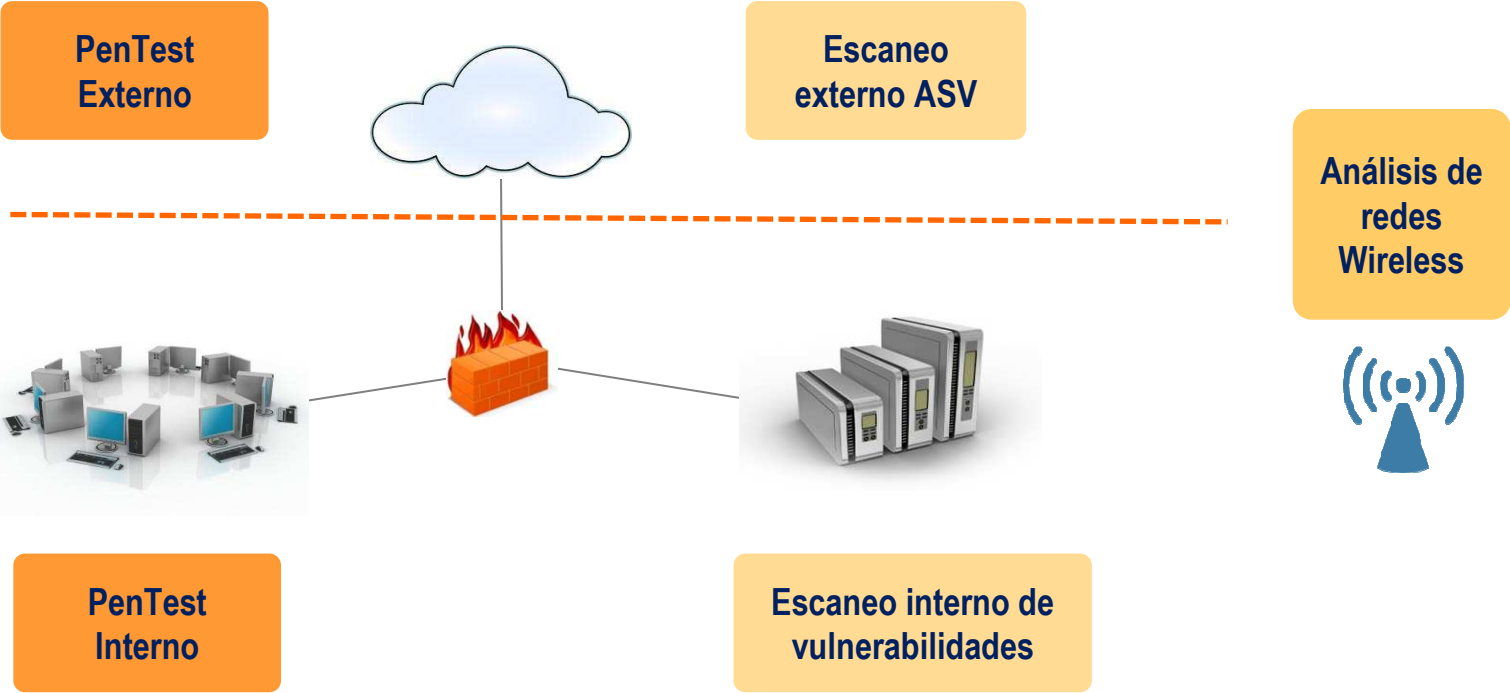


USUARIA

Payment Card Industry Security Standards Council (PCI SSC)

Verificaciones Técnicas de Seguridad

PCI DSS requiere la realización de 5 tipos de verificaciones técnicas de seguridad periódicas a la infraestructura de datos de tarjetas



Payment Card Industry Security Standards Council (PCI SSC)

Verificaciones Técnicas de Seguridad

Escaneo Vulns Externo (trimestral)	<ul style="list-style-type: none">• Escaneo automático (herramienta de software)• Debe ser realizado por un proveedor homologado como “Approved Scanning Vendor” (ASV)
PenTest Externo (anual)	<ul style="list-style-type: none">• Más profundo que el Escaneo de Vulns (incluye “intrusión”)• Emula las acciones que podría realizar un atacante Externo• Debe ser realizado por una empresa especializada en Seguridad Informática
Escaneo Vulns Interno (trimestral)	<ul style="list-style-type: none">• Escaneo automático (análogo al externo)• Puede ser realizado por personal de la empresa afectada a PCI
PenTest Interno (anual)	<ul style="list-style-type: none">• Análogo al PenTest Externo• Emula las acciones que podría realizar un atacante interno• Debe ser realizado por una empresa especializada en Seguridad Informática
Análisis redes Wireless (trimestral)	<ul style="list-style-type: none">• Búsqueda de redes inalámbricas “furtivas”.• Puede ser realizado por personal de la empresa afectada a PCI.• Puede reemplazarse por un IDS/IPS inalámbrico.



Payment Card Industry Security Standards Council (PCI SSC)

Escaneos Trimestrales ASV

PCI Status	
Number of IPs scanned: 23	Failed

Generally, to be considered compliant, a finding must not contain any vulnerability that has been assigned a CVSS base score equal to or higher than 4.0. Vulnerabilities or mis-configurations that may lead to DoS are not taken into consideration when determining compliance.



Gracias por asistir a esta sesión...



**Preguntas y
Respuestas...**

Para mayor información:

Pablo Milano

pmilano@cybsec.com



**Para descargar esta presentación visite
www.segurinfo.org**

Los invitamos a sumarse al grupo "Segurinfo" en **LinkedIn**®