CÁMARA
COLOMBIANA DE
COMERCIO
ELECTRÓNICO
www.ccce.org.co

CÁMARA COLOMBIANA DE COMERCIO ELECTRÓNICO
www.ccce.org.co

Cambios de las versiones 3.2, Cuestionarios y Ecosistema de Normas PCI

David A. González Lewis
PCI QSA, PA-QSA, CISM, PCIP
dagonzalez@isecauditors.com

internet security auditors

Nota Legal

CÁMARA COLOMBIANA DE COMERCIO ELECTRÓNICO
www.ccce.org.co

La CCCE asume el compromiso de regir sus actuaciones y decisiones empresariales de conformidad con la ley colombiana y normas nacionales de competencia, y estatutos & reglamentos internos; en todo momento la libre participación de las empresas en el mercado, el bienestar de los consumidores y la eficiencia económica.

Las conclusiones y recomendaciones realizadas en los espacios de formación, capacitación y talleres por los conferencistas, así como en los contenidos expuestos por la CCCE, directa o indirectamente, (nuestros portales, redes sociales y en general medios digitales o tradicionales) son de carácter informativo sin comprometer a ninguno de los afiliados o en general al público con su aplicación.

Agenda

CÁMARA COLOMBIANA DE COMERCIO ELECTRÓNICO
www.ccce.org.co

1. Retos a medios de pago y sus Amenazas.
2. **Ecosistema del PCI SSC**
3. Principales Cambios en las nuevas versiones.
    - Cambios en PCI DSS.
    - Cambios en PA-DSS.
4. Requerimientos de validación y reporte del cumplimiento.
5. Autoformularios SAQ.
6. Recursos de Interés PCI SSC.

Nuevos Retos Métodos de Pago

CÁMARA COLOMBIANA DE COMERCIO ELECTRÓNICO
www.ccce.org.co

- Gateway
- Payment Back Office
- Payment Gateway/Switch
- Payment Middleware
- Payment Switching
- POS Admin
- POS Face to Face
- POS General
- POS Kiosk
- POS Specialized
- POS SUite
- Shopping Cart & Store
- Front






- Existen miles de aplicaciones en diferentes lenguajes conviviendo.
- Los datos necesitan protección y está depende de la seguridad de cada una de esas aplicaciones.
- Las plataformas avanzan rápidamente.

Amenazas

- Fraudes.
- Malware.
- Seguridad en sus aplicaciones (OWASP TOP 10).
- Robo de Información.
- Errores humanos:
  - Malas configuraciones.
  - Empleados mal entrenados o descontentos.

Consecuencias:

- Pérdida de confianza de los clientes.
- Notificación de brechas (regulaciones en algunos países lo exigen).
- Multas, sanciones.
- Impacto en la reputación corporativa.

Ecosistema PCI SSC

CÁMARA COLOMBIANA DE COMERCIO ELECTRÓNICO
www.ccce.org.co

PCI DSS

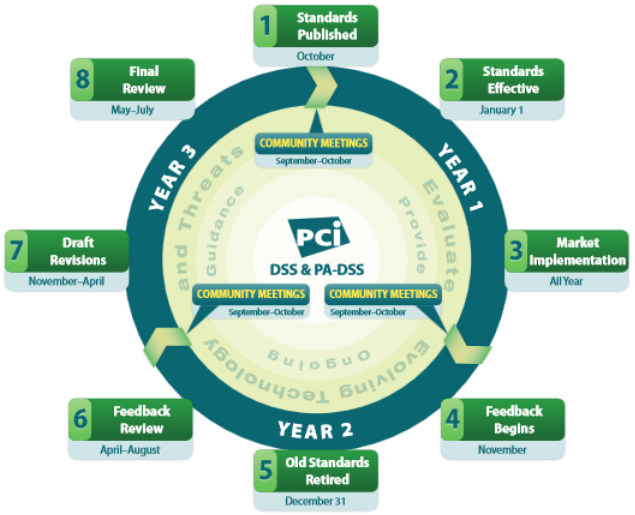
PA-DSS

P2PE

PCI PTS
POI - HSM

PCI Card
Production

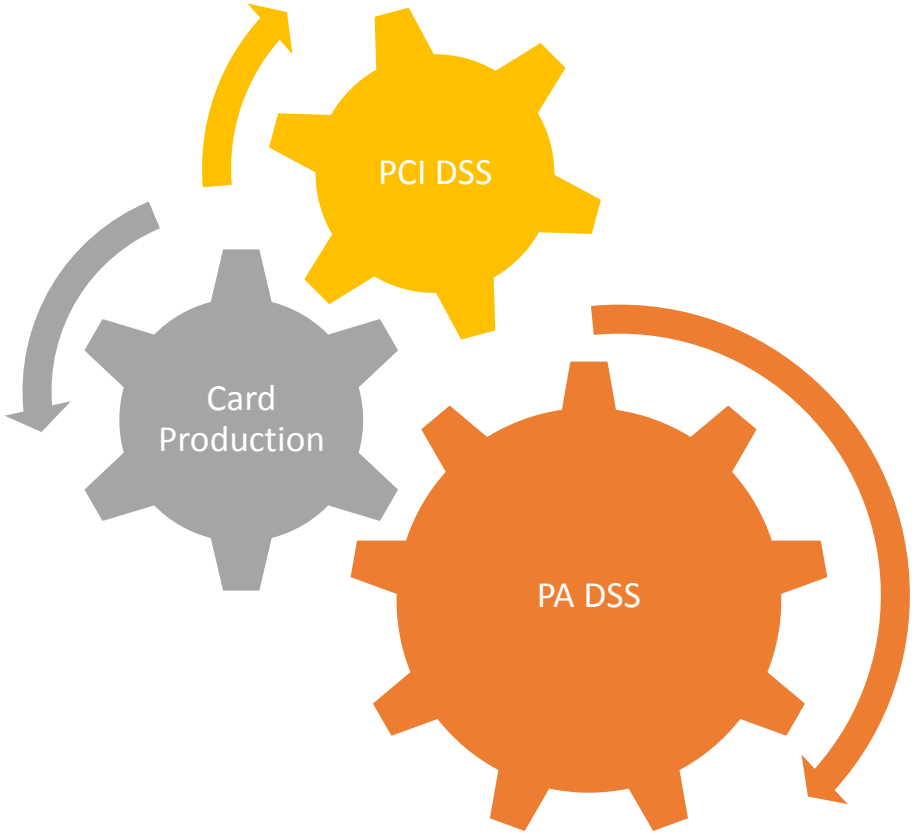
PCI PTS PIN
SECURITY



Principales Cambios en las Normas

CÁMARA COLOMBIANA DE COMERCIO ELECTRÓNICO
www.ccce.org.co

- **Aclaraciones:** Explicaciones de la intención de los requerimientos.
- **Guías Adicionales:** Explicaciones, definiciones o instrucciones que aumentan el entendimiento de la norma.
- **Requerimientos que evolucionan:** Cambios a la norma que aseguran que el estar está actualizado a las nuevas amenazas y cambios en el mercado.



Cambios PCI DSS

CÁMARA COLOMBIANA DE COMERCIO ELECTRÓNICO
www.ccce.org.co

Requerimiento	Descripción
2.2.3	Se remueve la nota y procedimientos de prueba sobre implementaciones de SSL e implementaciones tempranas de TLS.
3.3	Cualquier muestra del PAN con más de 6 primeros y 4 últimos debe llevar legitima necesidad de conocer.
3.5.1	Se debe tener documentada la descripción de la arquitectura de cifrado.
6.4.6	En un cambio se debe validar que no se está impactando el cumplimiento PCI DSS.
8.3	Se requiere multo-factor de autenticación para accesos administrativos que no sean por consola.
10.8	Se debe tener monitoreo y alerta de fallas en componentes que proveen seguridad.
11.3.4.1	Realizar pruebas de penetración cada 6 meses de la segmentación.
12.4	Establecer procedimiento y asignar responsabilidades sobre el cumplimiento de PCI DSS.
12.11	Trimestralmente se debe asegurar que el personal sigue las políticas de seguridad y los procedimientos operacionales.
Apéndice A2	Consideraciones sobre Implementaciones de SSL y TLS.

Cambios PCI DSS – Anexo A2

CÁMARA COLOMBIANA DE COMERCIO ELECTRÓNICO
www.ccce.org.co

- Cubre los requerimientos 2.2.3, 2.3, 4.1.
- Nuevas implementaciones solo se acepta TLS 1.2
- Después de Junio 30 de 2018 no se aceptan implementaciones inseguras.
- Implementaciones anteriores a Junio 30 de 2018 deben contar con un plan de mitigación.
- En POS POI (y terminaciones a las que se conectan) que se confirme que no son susceptibles a ser vulnerados, pueden no migrar.

Cambios en PA-DSS

CÁMARA COLOMBIANA DE COMERCIO ELECTRÓNICO
www.ccce.org.co

Requerimiento	Descripción
2.2	Cualquier muestra del PAN con más de 6 primeros y 4 últimos debe llevar legitima necesidad de conocer.
2.2.3	Logs de depuración que contengan PAN deben ser protegidos y borrados de forma segura.
5.1.7	La capacitación de desarrollo seguro debe estar actualizada y realizarse anualmente.
7.2.3	Instrucciones de como instalar los parches y actualizaciones de forma segura.
8.3 y 10.1	Se requiere multi-factor de autenticación para accesos administrativos que no sean por consola.

Requerimientos de Validación y Cumplimiento Comercios

CÁMARA COLOMBIANA DE COMERCIO ELECTRÓNICO
www.ccce.org.co

Nivel / Marca	Visa	MasterCard	American Express	Discover
1	Mas de 6 Millones de transacciones. Comprometidos en alguna brecha. Asignados a ser Nivel 1. **Auditoria Anual por QSA.** **Escaneos Trimestrales por ASV, AOC, Remitir el ROC.**	Mas de 6 Millones de transacciones. Comprometidos en alguna brecha. Asignados a ser Nivel 1. **Auditoria Anual por QSA.** **Escaneos Trimestrales por ASV, AOC, Remitir el ROC.**	Mas de 2.5 millones de transacciones. **Auditoria Anual por QSA.** **Escaneos Trimestrales por ASV.**	Mas de 6 Millones de transacciones. Asignados a ser Nivel 1. **Auditoria Anual por QSA.** **Escaneos Trimestrales por ASV.**
2	De 1 a 6 Millones **Llenado SAQ.** **Escaneos trimestrales ASV, AOC.**	De 1 a 6 millones de transacciones. **Llenado SAQ.** **Escaneos trimestrales ASV.**	De 50 mil a 2.5 millones de transacciones. **Llenado SAQ.** **Escaneos trimestrales ASV.**	De 1 a 6 millones de transacciones. **Llenado SAQ.** **Escaneos trimestrales ASV.**

Requerimientos de Validación y Cumplimiento Comercios

CÁMARA COLOMBIANA DE COMERCIO ELECTRÓNICO
www.ccce.org.co

Nivel / Marca	Visa	MasterCard	American Express	Discover
3	De 20 mil a 1 Millón. **Llenado SAQ.** **Escaneos trimestrales ASV.**	De 20 mil a 1 Millón. **Llenado SAQ.** **Escaneos trimestrales ASV.**	Menos de 50 mil. **Llenado SAQ.** **Escaneos trimestrales ASV.**	De 20 mil a 1 millón. **Llenado SAQ.** **Escaneos trimestrales ASV.**
4	Menos de 20 Mil. **Llenado SAQ.** **Escaneos trimestrales ASV.**	Los demás comercios. **Llenado SAQ.** **Escaneos trimestrales ASV.**	N/A.	Los demás comercios. **Llenado SAQ.**

Requerimientos de Validación y Cumplimiento Proveedores de Servicio

CÁMARA COLOMBIANA DE COMERCIO ELECTRÓNICO
www.ccce.org.co

Nivel / Marca	Visa	MasterCard	American Express	Discover
1	Mas de 300 mil transacciones. **Auditoria Anual por QSA.** **Escaneos Trimestrales por ASV, AOC, Remitir el ROC.**	Mas de 300 mil de transacciones. Comprometidos en alguna brecha. Cualquier TPP. **Auditoria Anual por QSA.** **Escaneos Trimestrales por ASV, AOC, Remitir el ROC.**	Mas de 2.5 millones de transacciones. **Auditoria Anual por QSA.** **Escaneos Trimestrales por ASV.**	Mas de 300 mil transacciones. Asignados a ser Nivel 1. **Auditoria Anual por QSA.** **Escaneos Trimestrales por ASV.**
2	Menos de 300 mil transacciones **Llenado SAQ.** **Escaneos trimestrales ASV, AOC.**	Menos de 300 mil transacciones **Llenado SAQ.** **Escaneos trimestrales ASV. Los PS en incumplimiento deben enviar plan de remediación.**	De 50 mil a 2.5 millones de transacciones. **Llenado SAQ.** **Escaneos trimestrales ASV.**	Menos de 300 mil transacciones. **Llenado SAQ.** **Escaneos trimestrales ASV. Los PS en incumplimiento deben enviar plan de remediación.**

Autoformularios SAQ

CÁMARA COLOMBIANA DE COMERCIO ELECTRÓNICO
www.ccce.org.co

- No todos los Comercios o Proveedores son iguales
  - Diferentes arquitecturas
  - Servicios que se proveen
  - Complejidad en estructura
  - Relaciones con terceros
- Un SAQ es un **subconjunto de controles de PCI DSS aplicados a un escenario específico** en el cual el propio comercio o proveedor de servicios puede demostrar su cumplimiento mediante una auto-evaluación de los mismos y una confirmación que dicho trabajo se ha realizado siguiendo las indicaciones del PCI SSC.

Autoformularios - SAQ

CÁMARA COLOMBIANA DE COMERCIO ELECTRÓNICO
www.ccce.org.co

Errores Comunes en su diligenciado:

- Tratarlo como un simple tramite.
- Considerar que un SAQ evita una multa.
- Rellenar el SAQ como sin realizar las validaciones.
- SAQ rellenado por alguien sin conocimientos pertinentes.

Tipos de SAQ´s

CÁMARA COLOMBIANA DE COMERCIO ELECTRÓNICO
www.ccce.org.co

Autoformulario	Descripción
SAQ A	Comercios que aceptan transacciones con tarjeta no presente (ecommerce) y que han tercerizado las funciones de tarjetas
SAQ A – EP	Comercios electrónicos que en su portal no reciben datos de tarjeta pero pueden afectar la seguridad.
SAQ B	Comercios que solo reciben transacciones por medio de “imprinter” o terminales independientes.
SAQ B – IP	Comercios que reciben pagos con POI aprobados por PCI PTS y conexión IP a un procesador de pagos.
SAQ C	Comercios que sus aplicaciones de pago se conectan a internet pero no almacenan datos de tarjetas.
SAQ C – VT	Comercios quienes procesan datos de tarjetas de pago únicamente a través de una terminal de pago virtual aislada en un ordenador personal conectado a Internet.
SAQ D	Comercios: Todos los comercios que no encajan en los anteriores SAQs. Proveedores de Servicio: Todos los proveedores de servicio que por clasificación deban llenar SAQ.
SAQ P2PE – HW	Comercios que están empleando terminales de pago de hardware incluidas y gestionadas por un proveedor certificado P2PE, sin almacenamiento electrónico de datos de tarjetas de pago.

Autoformularios SAQ

- Ayuda a demostrar el cumplimiento a terceros. (No son Nivel 1).

- Al firmar se declara cumplimiento, se es responsable en caso de incidencia.
  - Si es firmado y Validado por QSA tiene la misma validez de un ROC.
- La nueva versión de los SAQ es obligatoria a partir del 1 de Octubre de 2017.

Payment Card Industry (PCI)
Data Security Standard

Attestation of Compliance for
Self-Assessment Questionnaire D – Merchants
Version 3.0

Recursos de Interés PCI SSC

CÁMARA COLOMBIANA DE COMERCIO ELECTRÓNICO
www.ccce.org.co

- Guía para definir el alcance – Diciembre 2016
- Migrar de SSL a TLS – Mayo 2016
- Guía para pruebas de Penetración – Marzo 2015
- Guía de Tokenización - Agosto 2011
- Guía sobre Ransomwere – Enero 2017
- Guía de Autenticación Multi – Factor – Febrero 2017
- Mejores prácticas para asegurar e-Commerce – Enero 2017

Conclusiones

CÁMARA COLOMBIANA DE COMERCIO ELECTRÓNICO
www.ccce.org.co

- Se debe tener bien definido la clasificación de el comercio/proveedor de servicio.
- El diligenciamiento de el autoformulario debe ser una tarea a conciencia y soportada con evidencias.
- Los cambios en la norma (aunque pocos) requieren de un profundo análisis y dedicación.
- Un incorrecto proceso de Adecuación y Certificación al cumplir con PCI DSS genera riesgos en el caso de un compromiso o la identificación de un cumplimiento inadecuado.

Gracias

CÁMARA COLOMBIANA DE COMERCIO ELECTRÓNICO
www.ccce.org.co

internet security auditors

www.isecauditors.com


CÁMARA
COLOMBIANA DE
COMERCIO
ELECTRÓNICO
www.ccce.org.co