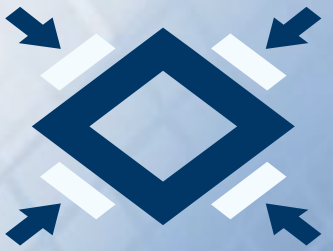


internet
security
auditors

PCI DSS, JUSTIFICACIÓN DEL CUMPLIMIENTO

DANIEL FERNÁNDEZ BLEDA, GLOBAL SALES MANAGER

CISM, CISA, CISSP, CHFI, OPST/A, ISO 27001 LEAD AUDITOR

C. Santander, 101. Edif. A. 2º
E-08030 Barcelona (Spain)
Tel.: +34 93 305 13 18
Fax: +34 93 278 22 48

C. Arequipa, 1
E-28043 Madrid (Spain)
Tel.: +34 91 763 40 47
Fax: +34 91 382 03 96

Calle 90 # 12-28
110221 Bogotá (Colombia)
Tel: +57 (1) 638 68 88
Fax: +57 (1) 638 68 88

info@isecauditors.com
www.isecauditors.com

AGENDA

1. PCI SSC y Auditores
2. Ecosistema del Normas PCI
3. PCI DSS: Antecedentes, Tipo de Información de Datos de Pago, Requerimientos v3.2, ¿Porqué cumplir?, ¿Y por qué una empresa de CC&BPO?, ¿Certificación, Cumplimiento, ROC, SAQ?
4. Requerimientos de Validación
5. Cuestionarios de Auto-Evaluación (SAQ): Tipos de SAQ, Errores comunes tratando con los SAQ
6. Metodología de Cumplimiento de PCI DSS
7. Puntos clave para tener éxito en un proceso de Cumplimiento
8. Conclusiones

PCI SSC y Auditores

- **PCI Security Standards Council (PCI SSC)** se crea el año 2006 y está formado por las principales compañías emisoras de tarjetas de crédito: **VISA, MASTERCARD, AMERICAN EXPRESS, JCB** y **DISCOVER**.
- Gestiona los diferentes estándares de la **familia PCI**, la homologación de Auditores de las diferentes normas, las aplicaciones certificadas PA-DSS…
- Implementa rigurosos procesos de validación y QA a las empresas para garantizar la solvencia y calidad de los auditores y sus entregables.

PCI Security Standards Council™
QUALIFIED SECURITY ASSESSOR

PCI Security Standards Council™
PAYMENT APPLICATION QUALIFIED SECURITY ASSESSOR

PCI Security Standards Council™
APPROVED SCANNING VENDOR

Ecosistema de Normas PCI

PCI DSS

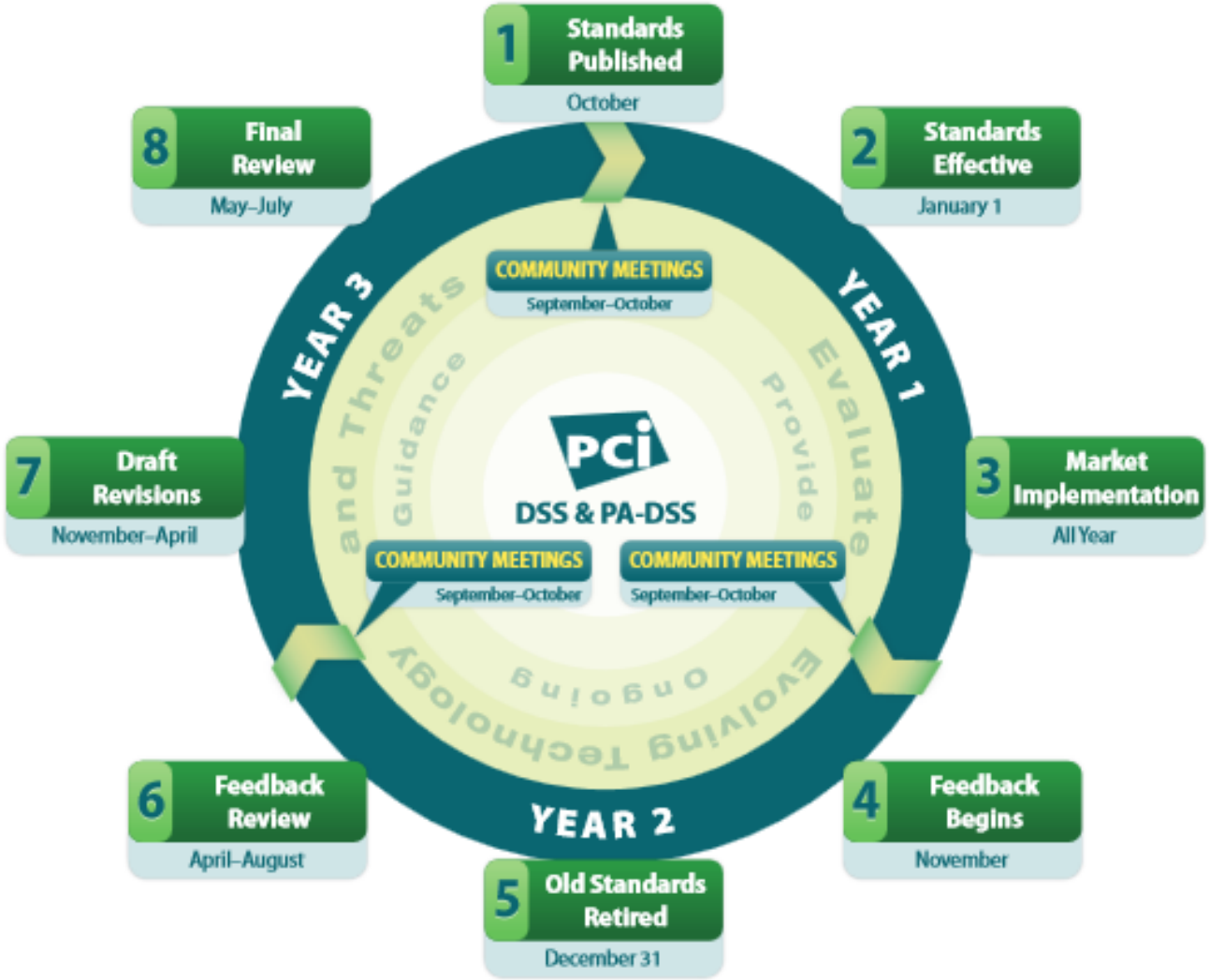
PA-DSS

P2PE

PCI PTS POI - HSM

PCI Card Production

PCI PTS PIN SECURITY



PCI DSS: Antecedentes

- Estándar de seguridad que abarca todas las tarjetas de crédito/débito que son emitidas sobre cualquier franquicia perteneciente al PCI SSC.
- Fruto del esfuerzo del **PCI Security Standards Council (PCI SSC)** y resultado de los programas de seguridad inicialmente creados por VISA y Mastercard.
- La primera versión común data del año 2004.
- La versión vigente desde octubre de 2017 es la 3.2.

PCI DSS: Tipo de Información Datos de Pago

La información de tarjetas de pago es la información que pertenece a las tarjetas de crédito/débito y a sus propietarios. Esta información está clasificada en 2 categorías:

- **Información de titulares de tarjeta:**
  - Número Primario de Cuenta (PAN)
  - Nombre Titular
  - Fecha de Vencimiento
- **Información Sensible de Autenticación:**
  - Información de la Banda Magnética
  - Código de Validación de Tarjeta (CVV o CVV2)

PCI DSS: Requerimientos v3.2

Principios	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

PCI DSS: ¿Por qué cumplir?

Reducimos el efecto de:

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

Consecuencias:

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

PCI DSS: ¿Y por qué una empresa de CC&BPO?

- Cualquier empresa que **TRATE**, **TRANSMITA** O **ALMACENE** datos de tarjetahabiente debe implementar y cumplir en el tiempo con los requerimientos de PCI DSS.
- Las empresas de CC&BPO pueden:
  - **Tratar**: obteniendo los datos de tarjeta del cliente final o del cliente al que le prestan servicios.
  - **Almacenar**: sea temporal o “permanentemente” los datos de pago para realizar operaciones en nombre del cliente.
  - **Transmitir**: sea de forma digital, telefónica o física de los datos de pago.
- Dependiendo del escenario de trabajo de prestación de servicios se puede ampliar o reducir los requerimientos a cumplir: tecnología del cliente, VDI, instalaciones donde se presta el servicio.

PCI DSS: ¿Certificación, Cumplimiento, ROC, SAQ?

- La norma no tiene niveles de cumplimiento.
- NO se “elige” el nivel de cumplimiento.
- La cantidad de transacciones anuales en comercios o proveedores de servicio determina el nivel de la empresa y este nivel ÚNICAMENTE determina la forma en la que demostrar que estamos cumplimiento con la norma: Auditoría o SAQ.
- La Certificación de PCI DSS suele asociarse a la Auditoría pero no ésta es la única forma de validar el cumplimiento.
- Certificar el Cumplimiento en la norma se consigue también mediante el Cuestionario de Auto-Evaluación (SAQ).
- Tanto la Auditoría, **que únicamente puede llevar a cabo una compañía QSA**, como el SAQ, **que puede ser firmado por el QSA**, validan o “certifican” el cumplimiento.

Requerimientos de Validación: Comercios (I)

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: Comercios (II)

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: Proveedores de Servicio

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.**

Cuestionarios de Auto-Evaluación (SAQ)

- ¿Por qué existen diferentes tipos de SAQ?
  - No todos los Comercios o Proveedores son iguales en sus procesos de pago:
    - Diferentes arquitecturas Tecnológicas: propias, del cliente o de terceros
    - E-commerce o venta presencial: IPSP, captura de datos, POS en LANs, etc.
    - Desarrollo de software o uso de productos de pago (PA-DSS)
- Cada Tipo SAQ incluye un **subconjunto de controles de PCI DSS aplicados a un escenario específico** de procesos de pago.
- Firmado por un QSA tiene **la misma validez** que un Informe de Auditoría (ROC).

Tipos de SAQ

Descripción	SAQ	Preguntas
• Transacciones no presenciales (e-commerce, telefónicas) • Nunca para compras presenciales	A	22
• E-commerce con re-dirección a terceras partes para el pago • No se almacenan datos de tarjeta	A-EP	193
• Sólo se imprimen los datos de tarjeta, pero no se almacenan • Comercios con terminales independientes, por líneas telefónicas • No se almacenan los datos de tarjeta	B	41
• Comercios con terminales independientes, a través de IP • Sin e-commerce • No se almacenan datos de tarjeta	B-IP	88

Tipos de SAQ

Descripción	SAQ	Preguntas
• Los sistemas que procesan las transacciones están conectados a Internet • No se almacenan datos de tarjeta	C	162
• Terminales virtuales basados en web sin almacenamiento electrónico de datos de los titulares de tarjeta	C–VT	85
• Cualquier comercio que no encaje en las opciones anteriores	D-MER	348
• Proveedores de Servicios que la marca establezca	D-SP	369
• Terminales de pago (h/w) en una solución PCI P2PE • Sin e-commerce • No se almacenan datos de tarjeta	P2PE	33

Errores Comunes tratando con los SAQ

- Tratarlo como un simple tramite
- Considerar que un SAQ evita una multa
- Diligenciar el SAQ sin realizar validaciones
- SAQ diligenciado por alguien sin conocimientos pertinentes:
  - Escoger el SAQ incorrecto
  - Dar respuestas incorrectas (por omisión o desconocimiento)

Puntos clave para el éxito de un proyecto de PCI DSS

El éxito de un proyecto de PCI DSS se basa en:

- Seguir una **metodología robusta**
- Contar con el **asesoramiento adecuado** en todo el proyecto: los QSA existen por alguna razón, somos los únicos **expertos con garantías**.
- Gap Análisis **preciso** es clave en la toma de decisiones posterior
- Tener clara una **estrategia de cumplimiento**: Plan de Acción
- Definir **proyectos** de cumplimiento con **objetivos y responsables**
- No esperar a la ejecución de los proyectos para que estos sean validados por un QSA: **el QSA es un aliado, no sólo el auditor** al final del proceso.

Metodología de Implementación de PCI DSS

FASE I: Análisis del Estado de Cumplimiento	• Identificación del entorno y diagnóstico de cumplimiento • Familiarización con PCI DSS • Informe de Estado de Cumplimiento
FASE II: Valoración de Riesgos y Priorización de Acciones	• Identificación de riesgos asociados al robo de datos de tarjeta • Valoración de riesgos
FASE III: Programa de Cumplimiento	• Selección de Controles y Medidas de Seguridad • Creación del Plan de Acción para la Adecuación

Metodología de Implementación de PCI DSS

FASE IV: Implantación de Requerimientos para la Adecuación

- Adecuación y/o Creación de Políticas, Normas y Procedimientos de Seguridad
- Definición de Métricas e Indicadores
- Diseño de soluciones para eliminación de datos de tarjetas e información sensible de autenticación
- Diseño de arquitecturas de red segura
- Definición o adecuación de metodologías de desarrollo que integren la seguridad en su ciclo de vida
- Definición y aplicación de estándares de configuración segura de sistemas y dispositivos de red
- Despliegue de Firewall de Aplicación
- Despliegue de IDS/IPS
- Despliegue de Firewalls y Routers
- Integración de herramientas SIEM
- Adecuación de aplicaciones
- Despliegue de sistemas VDI

Metodología de Implementación de PCI DSS

FASE IV: Implantación de Requerimientos para la Adecuación

- Despliegue de sistemas de acceso remoto basados en doble factor de autenticación
- SOC de Respuesta a Incidentes
- Despliegue de WIPS (Wireless IPS)
- Despliegue de HSM
- Servicios de hosting, colocation, housing y/o cloud
- Despliegue de soluciones antivirus
- Despliegue, configuración y mantenimiento de sistemas de gestión de identidades
- Despliegue, configuración y mantenimiento de servidores web, aplicaciones, servidores de salto, LDAP, NTP, etc.
- Formación a empleados (desarrollo de software, backoffice, sistemas, seguridad, etc.)
- Soporte y/o adecuación de bases de datos
- Despliegue de sistemas de tokenización

Metodología de Implementación de PCI DSS

FASE V: Certificación del Cumplimiento

- Auditoría de Certificación del Cumplimiento:
  - Preparación y Ejecución del Plan de Auditoría
  - Elaboración del Informe de Cumplimiento (ROC) y documentación para las franquicias de tarjetas
- Preparación de SAQ para reporte de Cumplimiento:
  - Toma de Evidencias del cumplimiento
  - Diligenciamiento del SAQ adecuado

Metodología de Implementación de PCI DSS

Mantenimiento del Cumplimiento: Oficina Técnica de PCI DSS (OTP)

Procesos de Seguridad

Business-as-usual

- Actividades de Seguimiento, Gestión de la OTP y Reporting
- Revisiones Técnicas de Seguridad (Análisis de Vulnerabilidad ASV e Internos, Test de Intrusión Externos e Internos, Escaneos WiFi y Revisión de reglas de Firewall)
- Actualización del AA.RR.
- Asesoramiento ante cambios en los procesos del Entono
- Formación y Concientización (personal de backoffice, SAU, técnico, sistemas,desarrollo, etc.)
- Revisión del Cumplimiento de Proveedores de Servicios
- Cuadro de Mandos del Cumplimiento
- Revisiones Técnicas y Pruebas tras Cambios
- Servicios de Respuesta y Gestión de Incidentes 24x7
- Respuesta a terceros sobre Cumplimiento
- Adecuación del Marco Normativo Documental ante cambios

Conclusiones

- Se debe tener bien definida la clasificación de nuestra compañía como comercio o proveedor de servicio: escoger adecuadamente SAQ o tener que realizar la Auditoría.
- El diligenciamiento de el SAQ debe ser una tarea a conciencia y soportada con evidencias, no es un mero trámite administrativo.
- Un incorrecto proceso de Adecuación y Certificación del Cumplimiento con PCI DSS genera riesgos en el caso de un compromiso o la identificación de un cumplimiento inadecuado.
- Los únicos asesores con la garantía del PCI SSC como profesionales expertos en PCI DSS somos los QSA: cualquiera puede descargar la norma, pero no cualquiera puede ser un asesor homologado y asume las responsabilidades legales en la firma de SAQ o del ROC.

internet
security
auditors

C. Santander, 101. Edif. A. 2º
E-08030 Barcelona (Spain)
Tel.: +34 93 305 13 18
Fax: +34 93 278 22 48

C. Arequipa, 1
E-28043 Madrid (Spain)
Tel.: +34 91 763 40 47
Fax: +34 91 382 03 96

Calle 90 # 12-28
110221 Bogotá (Colombia)
Tel: +57 (1) 638 68 88
Fax: +57 (1) 638 68 88

info@isecauditors.com
www.isecauditors.com

internet
security
auditors

C. Santander, 101. Edif. A. 2º
E-08030 Barcelona (Spain)
Tel.: +34 93 305 13 18
Fax: +34 93 278 22 48

C. Arequipa, 1
E-28043 Madrid (Spain)
Tel.: +34 91 763 40 47
Fax: +34 91 382 03 96

Calle 90 # 12-28
110221 Bogotá (Colombia)
Tel: +57 (1) 638 68 88
Fax: +57 (1) 638 68 88

info@isecauditors.com
www.isecauditors.com