Norma de seguridad de datos de la Industria de tarjetas de pago (PCI)

Cuestionario de autoevaluación

Instrucciones y directrices

Versión 2.0

Octubre de 2010

Modificaciones realizadas a los documentos

Fecha	Versión	Descripción
1 de octubre de 2008	1.2	Alinear el contenido con la nueva versión 1.2 de PCI DSS e implementar cambios menores notados desde la versión 1.1 original.
28 de octubre de 2010	2.0	Alinear el contenido con la nueva versión v2.0 de PCI DSS y aclarar tipos de entornos de SAQ y criterios de elegibilidad. Adición de C-VT de SAQ para comerciantes con terminales virtuales basados en la web

Índice

Acerca de este documento

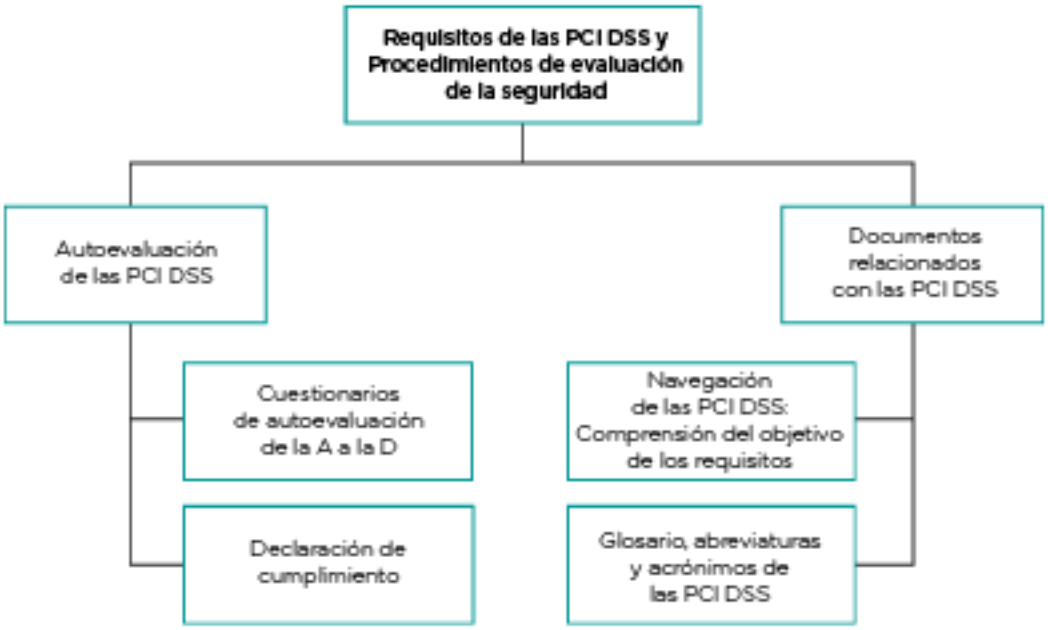
Este documento se desarrolló para ayudar a los comerciantes y proveedores de servicio a comprender el Cuestionario de autoevaluación (SAQ) de las Normas de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI DSS). Lea todo este documento de Instrucciones y directrices para comprender por qué las PCI DSS son importantes para su organización, qué estrategias puede utilizar su organización para facilitar la validación de cumplimiento, y si su organización es elegible para completar una de las versiones más cortas del SAQ. Las siguientes secciones señalan lo que necesita saber sobre el SAQ de las PCI DSS.

- Autoevaluación de las PCI DSS: Cómo encaja todo
- PCI DSS: Documentos relacionados
- Descripción general del SAQ
- ¿Por qué es importante el cumplimiento con las PCI DSS?
- Sugerencias generales y estrategias para prepararse para la validación de cumplimiento
- Selección del SAQ y la declaración que mejor se aplican a su organización
- Guía para la no aplicabilidad de ciertos requisitos específicos
- Instrucciones para completar el SAQ
- ¿Cuál SAQ se aplica mejor a mi entorno?

Autoevaluación de las PCI DSS: Cómo encaja todo

Las PCI DSS y los documentos de apoyo representan un conjunto de herramientas y medidas comunes que se utilizan en la industria a fin de ayudar a asegurar el manejo seguro de información confidencial. La norma proporciona un marco que se puede utilizar para desarrollar un proceso de seguridad de datos de la cuenta sólido, incluyendo la prevención y detección de incidentes de seguridad y la reacción a estos. Con el fin de reducir el riesgo de que ocurra un compromiso de la seguridad y mitigar su impacto si el mismo llegara a ocurrir, es importante que todas las entidades que almacenan, procesan o transmiten datos de los titulares de tarjetas cumplan con las normas. El diagrama que aparece a continuación delinea las herramientas ya establecidas para ayudar a las organizaciones a cumplir con las PCI DSS y la autoevaluación.

Puede consultar estos y otros documentos relacionados en www.pcisecuritystandards.org.



Norma de seguridad de datos de la PCI: Documentos relacionados

Los siguientes documentos fueron creados para ayudar a los comerciantes y proveedores de servicio a entender las PCI DSS y el SAQ de las PCI DSS.

Documento	Audiencia
Norma de seguridad de datos de la PCI: Requisitos y procedimientos de evaluación de seguridad	Todos los comerciantes y proveedores de servicio
Navegación de las PCI DSS: Comprensión del objetivo de los requisitos	Todos los comerciantes y proveedores de servicio
Norma de seguridad de datos de la PCI: Directrices e instrucciones para el cuestionario de autoevaluación	Todos los comerciantes y proveedores de servicio
Norma de seguridad de datos de la PCI: Cuestionario de autoevaluación A y Declaración	Comerciantes elegibles[1]
Norma de seguridad de datos de la PCI: Cuestionario de autoevaluación B y Declaración	Comerciantes elegibles[1]
Norma de seguridad de datos de la PCI: Cuestionario de autoevaluación C-VT y Declaración	Comerciantes elegibles[1]
Norma de seguridad de datos de la PCI: Cuestionario de autoevaluación y declaración C	Comerciantes elegibles[1]
Norma de seguridad de datos de la PCI: Cuestionario de autoevaluación D y Declaración	Los comerciantes y proveedores de servicio elegibles[1]
Norma de Seguridad de la PCI y Norma de Seguridad de Datos para las Aplicaciones de Pago Glosario de términos, abreviaturas y acrónimos	Todos los comerciantes y proveedores de servicio

[1] Para determinar el Cuestionario de autoevaluación apropiado, consulte “Selección de las SAQ y Declaración de que se aplica mejor a su organización”, en la página 12 de este documento.

Descripción general del SAQ

El *Cuestionario de autoevaluación (SAQ) de las PCI DSS* (SAQ) es una herramienta de validación cuya intención es asistir a los comerciantes y proveedores de servicio en el proceso de evaluar su cumplimiento con las Normas de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI DSS). Hay varias versiones del SAQ de las PCI DSS que corresponden a diversos escenarios y situaciones. Este documento se ha desarrollado para ayudar a las organizaciones a determinar cuál SAQ se aplica mejor a su caso.

El SAQ de las PCI DSS es una herramienta de validación para los comerciantes y proveedores de servicio a los cuales no se les requiere pasar Informe de cumplimiento (ROC) de evaluación de seguridad in situ según los *Procedimientos de Auditoría de Seguridad de las PCI DSS,* y puede ser requerido por su adquirente o marca de pago. Consulte con su adquirente o marca de pago para obtener información más detallada referente a los requisitos de validación de las PCI DSS.

El SAQ de las PCI DSS consiste en los siguientes componentes:

1. Preguntas que se correlacionan con los requisitos de las PCI DSS, apropiadas para los proveedores de servicio y comerciantes: consulte "Selección del SAQ y la declaración que mejor se aplican a su organización" en este documento.
2. Declaración de cumplimiento: La Declaración es su certificación de que es elegible para realizar una autoevaluación de las PCI DSS apropiada y ya la ha realizado.

¿Por qué es importante el cumplimiento con las PCI DSS?

Los miembros del PCI Security Standards Council (American Express, Discover, JCB, MasterCard y Visa) continuamente supervisan los casos en que se compromete la seguridad de los datos de las cuentas. Estos compromisos de la seguridad ocurren en todo tipo de organizaciones, desde las más pequeñas hasta las más grandes empresas y proveedores de servicio.

Una violación de la seguridad y el compromiso de la seguridad de los datos de las tarjetas de pago que la misma conlleva tienen consecuencias de muy largo alcance para las organizaciones afectadas, incluyendo:

1. Requisitos de notificaciones reglamentarias,
2. Pérdida de la buena reputación,
3. Pérdida de clientes
4. Posibles obligaciones económicas (por ejemplo, cuotas reglamentarias, multas, etc.) y
5. Litigios

El análisis forense de diversos tipos de compromisos de Información han revelado debilidades comunes que las PCI DSS contemplan, pero que las organizaciones afectadas no habían implementado cuando ocurrieron los incidentes. Las PCI DSS fueron diseñadas precisamente por esta razón e incluyen requisitos detallados para minimizar las probabilidades de que ocurra un compromiso de la seguridad, así como el efecto del mismo, en caso de que ocurriera.

Las investigaciones realizadas después de ocurridos los incidentes de seguridad muestran en casi todos los casos violaciones comunes de las PCI DSS, incluyendo, sin limitación:

- Almacenamiento de datos de la banda magnética (Requisito 3.2). Es importante tener presente que muchas de las entidades que han visto comprometida la seguridad de sus datos no están conscientes de que sus sistemas están almacenando estos datos.
- Controles de acceso inadecuados debido a sistemas de POS instalados en forma inapropiada en los comercios, los cuales permiten a los individuos maliciosos penetrarlos a través de vías de conexión reservadas para los proveedores de los equipos (Requisitos 7.1, 7.2, 8.2 y 8.3).
- Configuraciones y contraseñas predeterminadas que no se cambiaron cuando se instaló el sistema (Requisito 2.1).
- Servicios innecesarios y vulnerables que no se eliminaron o aseguraron cuando se instaló el sistema (Requisito 2.2.2 y 2.2.4).
- Aplicaciones de web con códigos deficientes que han permitido la inyección SQL y otras vulnerabilidades que permiten el acceso a la base de datos donde se guardan los datos de los titulares de la tarjeta directamente desde el sitio web (Requisito 6.5).
- Parches de seguridad que no se han instalado o están obsoletos (Requisito 6.1).
- Falta de registros (Requisito 10).
- Falta de supervisión (por medio de revisiones de registros, detección/prevención de intrusión, escaneos trimestrales de vulnerabilidad y sistemas de supervisión de la integridad de los archivos (Requisitos 10.6, 11.2, 11.4 y 11.5).
- Falta de segmentación en una red que hace fácilmente accesibles los datos de los titulares de tarjetas debido a vulnerabilidades en otros lugares de la red (por ejemplo, desde puntos de acceso inalámbricos, correo electrónico de los empleados y exploradores de redes) (Requisitos 1.2, 1.3 y 1.4).

Sugerencias generales y estrategias para prepararse para la validación de cumplimiento

A continuación se ofrecen algunas sugerencias generales y estrategias para comenzar sus esfuerzos con vistas a la validación del cumplimiento con las PCI DSS. Estas sugerencias podrían ayudarle a eliminar los datos que no necesita, a aislar los datos que sí necesita en áreas centralizadas, definidas y controladas, así como a limitar el alcance de sus esfuerzos para validar el cumplimiento con las PCI DSS. Por ejemplo, al eliminar los datos que no necesita y/o aislar los datos que sí necesita en áreas centralizadas, definidas y controladas, puede eliminar los sistemas y redes que ya no almacenan, procesan o transmiten datos de los titulares de tarjetas de su proceso de autoevaluación.

1. **Datos Confidenciales de Autenticación (incluyen el contenido íntegro de la banda magnética, los códigos y valores de verificación de tarjeta, los PIN y los bloques de PIN):**
   a. Asegúrese de ***nunca almacenar estos datos***.
   b. Si no está seguro o no sabe, pregúntele al proveedor de su equipo de POS si la versión de software y el producto que usted usa guarda estos datos. Como alternativa, considere contratar a un Evaluador de Seguridad Calificado que le ayude a determinar si su sistema está guardando, registrando o capturando en algún lugar los datos confidenciales de autenticación.
2. **Si es un comerciante, pregúntele al proveedor de su equipo de POS sobre la seguridad de su sistema. Le sugerimos las siguientes preguntas:**
   a. ¿Mi software de POS está validado para las Normas de Seguridad de Datos para las Aplicaciones de Pago (PA-DSS)? (Consulte la lista de Aplicaciones de pago validadas del PCI SSC).
   b. ¿Guarda mi software de POS datos de la banda magnética (datos de la pista) o bloques de PIN? Si es así, está prohibido almacenar estos datos. ¿Cuán rápidamente me puede ayudar a eliminarlos?
   c. ¿Mi software de POS almacena números de cuentas principales (PAN)? Si es así, se deben proteger estos datos. ¿Cómo protege el POS estos datos?
   d. ¿Se documentará la lista de archivos escritos por la aplicación con un resumen del contenido de cada archivo, a fin de verificar que los datos mencionados anteriormente, cuyo almacenamiento está prohibido, no se guardan?
   e. ¿Requiere su sistema de POS que yo instale un firewall para proteger el sistema del acceso no autorizado?
   f. ¿Se requieren contraseñas complejas y únicas para obtener acceso a mi sistema? ¿Puede confirmar que no usa contraseñas comunes o por defecto para mi sistema y para otros sistemas de comercios a los cuales brinda soporte?
   g. ¿Se han cambiado la configuración y las contraseñas predeterminadas en los sistemas y bases de datos que forman parte del sistema de POS?
   h. ¿Se han eliminado todos los servicios innecesarios y no seguros de los sistemas y bases de datos que forman parte del sistema de POS?
   i. ¿Puede acceder a mi sistema de POS remotamente? Si es así, ¿ha implementado controles apropiados para evitar que otros accedan a mi sistema de POS, tales como el uso de métodos de acceso remoto seguros y no usar contraseñas comunes o predeterminadas? ¿Con cuánta frecuencia accede a mi dispositivo de POS remotamente y por qué? ¿Quién está autorizado para acceder remotamente a mi equipo de POS?

j. ¿Se han instalado los parches de seguridad aplicables en todos los sistemas y bases de datos que forman parte del sistema de POS?

k. ¿Está activada la capacidad de registro en los sistemas y bases de datos que forman parte del sistema de POS?

l. Si las versiones previas de mi software de POS almacenaban los datos de la pista, ¿se ha eliminado esta función en las actualizaciones al software de punto de venta? ¿Se usó una utilidad segura para destrucción de estos datos?

3. Datos de titulares de tarjetas—Si no los necesita, ¡no los guarde!

a. Los reglamentos de las marcas de pago permiten guardar el Número de Cuenta Personal o Primario (PAN), la fecha de vencimiento, el nombre del titular de la tarjeta y el código de servicio.

b. Haga una lista de las razones y un inventario de los lugares donde guarda estos datos. Si los datos no cumplen un propósito valioso para el negocio, considere eliminarlos.

c. Considere si el almacenamiento de estos datos y el proceso de negocio que los mismos apoyan amerita lo siguiente:

i. El riesgo de que la seguridad de los datos se vea comprometida.

ii. El esfuerzo adicional que requieren las PCI DSS y que usted debe implementar para proteger esos datos.

iii. Los continuos esfuerzos que se requieren para mantener el cumplimiento con dichas PCI DSS a través del tiempo.

4. Datos de titulares de tarjetas—Si no los necesita, consolídelos y aíslelos.

Usted puede limitar el alcance de la auditoría de las PCI DSS consolidando el almacenamiento de los datos en un ambiente definido y aislando los datos por medio de la segmentación apropiada de su red. Por ejemplo, si sus empleados navegan por Internet y reciben correo electrónico en la misma máquina o en el mismo segmento de la red donde se encuentran los datos de los titulares de tarjetas, considere segmentar (aislar) los datos de los titulares de tarjetas guardándolos en una máquina o segmento de red que esté dedicado únicamente a almacenar esos datos (por medio de routers o firewalls). Si puede aislar bien los datos de los titulares de tarjetas, podrá entonces concentrar sus esfuerzos para cumplir con las PCI DSS en la parte aislada, en lugar de incluir todos sus equipos.

5. Controles de compensación

Se podrían considerar controles de compensación para la mayoría de los requisitos de las PCI DSS cuando una organización no puede cumplir con la especificación técnica de un requisito, pero ha mitigado en forma suficiente el riesgo asociado con dicho requisito. Si su empresa no tiene el control exacto especificado en las PCI DSS, pero tiene establecidos otros controles que satisfacen la definición de controles compensatorios dada en dichas Normas (consulte “Controles de compensación” en el Anexo del SAQ correspondiente y el documento titulado *Glosario, Abreviaturas y Acrónimos de las PCI DSS y PA-DSS* en www.pcisecuritystandards.org), su empresa debe hacer lo siguiente:

a. Responda "SÍ" a la pregunta del SAQ y, en la columna "Especial" indique el uso de cada control de compensación que se utiliza para satisfacer un requisito.

b. Revise la sección sobre “Controles de compensación” en el Anexo B del SAQ aplicable y documente el uso de los controles de compensación llenando la Hoja de trabajo de controles de compensación en el Anexo C del SAQ.

c. Complete una Hoja de trabajo de controles de compensación para cada requisito que se llene mediante un control de compensación.

d. Presente todas las Hojas de trabajo de controles de compensación, debidamente llenadas, junto con su SAQ y/o Declaración, debidamente completados, de acuerdo con las instrucciones que reciba de su adquirente o marca de pago.

6. Asistencia y capacitación profesional

a. Si desea contar con orientación profesional para poder cumplir con las normas y completar el SAQ, le recomendamos que la obtenga. Reconozca que, si bien es libre de contratar a cualquier profesional de seguridad de su elección, solamente los que están incluidos en la lista de Evaluadores de Seguridad Calificados (QSA) están reconocidos como tales y capacitados por el PCI SSC. Esta lista está a su disposición en https://www.pcisecuritystandards.org.

b. El PCI Security Standards Council (SSC) proporciona diversos recursos de educación para profundizar los conocimientos de seguridad dentro de la industria de tarjetas de pago. Estos recursos incluyen capacitación sobre las PCI DSS para Asesores de Seguridad Internos (ISA) y capacitación sobre normas. Asimismo, el sitio web de las PCI SSC es una de las fuentes principales de recursos adicionales, incluyendo:

- La guía *Navegación de las PCI DSS*
- El *Glosario de términos, abreviaturas y acrónimos de las PCI DSS y PA-DSS*
- Preguntas frecuentes (FAQ)
- Webinars
- Suplementos informativos y directrices
- Declaración de cumplimiento

Consulte www.pcisecuritystandards.org para obtener más información.

Nota: *Los suplementos informativos complementan las PCI DSS e identifican las consideraciones y recomendaciones adicionales para cumplir con los requisitos de las PCI DSS, las cuales no modifican ni eliminan ni sustituyen las PCI DSS ni ninguno de sus requisitos*.

Selección del SAQ y la declaración que mejor se aplican a su organización

De conformidad con los reglamentos de la marca de pago, se requiere a todos los comerciantes y proveedores de servicio cumplir con las PCI DSS en su totalidad. Existen cinco categorías de SAQ, las cuales se describen brevemente en la tabla que aparece a continuación y en mayor detalle en los párrafos que siguen. Utilice la tabla para determinar cuál SAQ se aplica a su organización y revise después las descripciones detalladas para asegurar que cumple todos los requisitos para llenar dicho SAQ.

SAQ	Descripción
A	Comerciantes con tarjetas ausentes (comercio electrónico, pedido por correo o pedido por teléfono); todas las funciones que impliquen el manejo de datos del titular de la tarjeta, tercerizadas. *Esto nunca se aplicaría a comerciantes cara a cara.*
B	Comerciantes que usan solamente máquinas impresoras, sin almacenamiento electrónico de datos de titulares de tarjetas, o comerciantes que tienen terminales independientes con discado externo y no almacenan electrónicamente datos de los titulares de tarjetas.
C-VT	Comerciantes que tienen terminales independientes con discado externo y no almacenan electrónicamente datos de los titulares de tarjetas.
C	Comerciantes con sistemas de aplicaciones de pago conectados a Internet, sin almacenamiento electrónico de datos de los titulares de tarjetas.
D	Todos los demás comerciantes, no incluidos en las descripciones correspondientes a las versiones de A a C del SAQ según se expone anteriormente, y **todos** los **proveedores de servicio** definidos por una marca de pago como elegibles para completar un SAQ.

SAQ A – Comerciantes con tarjetas ausentes; todas las funciones que impliquen el manejo de datos del titular de la tarjeta, tercerizadas.

El SAQ A se ha desarrollado para contemplar los requisitos aplicables a los comerciantes que retienen solamente informes o recibos en papel con datos de los titulares de tarjetas, no guardan los datos de los titulares de tarjetas en formato electrónico y no procesan ni transmiten ningún tipo de información de los titulares de tarjetas en sus locales.

Para consultar una guía gráfica que lo ayude a determinar su tipo de SAQ, consulte "¿Cuál SAQ se aplica mejor a mi entorno?" en la página 17.

Los comerciantes correspondientes al SAQ no almacenan datos de los titulares de tarjetas en formato electrónico y no procesan ni transmiten datos de los titulares de tarjetas en sus sistemas y locales. Dichos comerciantes deben validar el cumplimiento completando el SAQ A y la Declaración de cumplimiento relacionadacon dicho cuestionario, a fin de confirmar que:

- Su empresa maneja solamente transacciones con tarjeta ausente (comercio electrónico y órdenes por correo/teléfono);
- Su empresa no almacena, procesa ni transmite datos de los titulares de tarjetas en sus sistemas o locales, sino que depende completamente de un uno o varios terceros que realizan estas funciones.

- Su empresa ha confirmado que el tercero o los terceros que manejan el almacenamiento, procesamiento y/o transmisión de los datos de los titulares de tarjetas cumplen con las PCI DSS.
- Su empresa retiene solamente reportes o recibos en papel con datos de los titulares de tarjetas, y estos documentos no se reciben por medios electrónicos; **y**
- Su empresa no almacena datos del titular de la tarjeta en formato electrónico.

Esta opción nunca se aplicaría a comerciantes con un entorno de POS cara a cara.

SAQ B – Comerciantes que usan solamente máquinas impresoras o que tienen terminales independientes con discado externo. Sin almacenamiento electrónico de datos de titulares de tarjetas.

El SAQ B se ha desarrollado para contemplar los requisitos aplicables a los comerciantes que procesan datos de los titulares de tarjetas solamente por medio de máquinas impresoras o terminales independientes con discado externo.

Para consultar una guía gráfica que lo ayude a determinar su tipo de SAQ, consulte "¿Cuál SAQ se aplica mejor a mi entorno?" en la página 17.

Los comerciantes que se corresponden con el SAQ B procesan datos de los titulares de tarjetas solamente por medio de máquinas impresoras o terminales independientes con discado externo y pueden ser comerciantes con instalaciones físicas (con tarjeta presente) o comercio electrónico o pedido por correo electrónico/teléfono (tarjeta no presente). Esos comerciantes deben validar el cumplimiento completando el SAQ B y la Declaración de cumplimiento relacionada con dicho cuestionario, a fin de confirmar que:

- Su empresa usa solamente máquinas impresoras y/o terminales independientes con discado externo (conectados a través la línea telefónica a su procesador) para registrar la información de la tarjeta de pago de sus clientes;
- Los terminales independientes con discado externo no están conectados a ningún otro sistema en su entorno;
- Los terminales independientes con discado externo no están conectados a Internet;
- Su empresa no transmite datos de los titulares de tarjetas por la red (ni a través de una red interna ni de Internet.
- Su empresa retiene solamente reportes o recibos en papel con datos de los titulares de tarjetas, y estos documentos no se reciben por medios electrónicos; **y**
- Su empresa no almacena datos del titular de la tarjeta en formato electrónico.

SAQ C-VT – Comerciantes con terminales independientes con discado externo sin almacenamiento electrónico de datos de los titulares de tarjetas

El SAQ C-VT se ha desarrollado para contemplar los requisitos aplicables a los comerciantes que procesan datos de los titulares de tarjetas solamente por medio de terminales virtuales aislados en computadoras personales conectadas a Internet.

Para consultar una guía gráfica que lo ayude a determinar su tipo de SAQ, consulte "¿Cuál SAQ se aplica mejor a mi entorno?" en la página 17.

Un terminal virtual es un acceso basado en explorador web para un adquiriente, procesador o sitio web de proveedor de servicios externos que permite autorizar transacciones de tarjetas de pago, donde el comerciante ingresa manualmente datos de tarjetas de pago mediante un explorador web conectado de forma segura. A diferencia de los terminales físicos, los terminales virtuales no leen datos directamente de una tarjeta de pago. Debido a que las transacciones de tarjetas de pago se ingresan manualmente, comúnmente se utilizan terminales virtuales en lugar de

terminales físicos en entornos de comerciantes con bajo volumen de transacciones.

Estos comerciantes procesan datos de titulares de tarjetas sólo a través de un terminal virtual y no almacenan los datos de titulares de tarjetas en cualquier sistema de computadoras. Estos terminales virtuales están conectados a Internet para acceder a un tercero que que sea proveedor de hosting de la función de procesamiento de pagos en terminales virtuales. Este tercero puede ser un procesador, adquiriente u otro proveedor de servicios externo que almacena, procesa y/o transmite los datos de los titulares de tarjetas para autorizar y/o liquidar las transacciones de pago en terminal virtual de los comerciantes.

Esta opción de SAQ está dirigida sólo a comerciantes que ingresan manualmente una sola transacción a la vez utilizando un teclado en una solución de terminal virtual basado en Internet.

Los comerciantes que se corresponden al SAQ C-VT procesan datos de titulares de tarjetas a través de terminales virtuales en computadoras personales conectadas a Internet, no almacenan datos de titulares de tarjetas en ningún otro sistema de computadora, y pueden ser comerciantes con instalaciones físicas (con la tarjeta presente) o comercio electrónico o pedido por correo electrónico/teléfono (tarjeta no presente). Tales comerciantes validan el cumplimiento llenando el SAQ C-VT y la Declaración de cumplimiento, con los cuales confirman que:

- El único procesamiento de pagos de su empresa se realiza a través de un terminal virtual al que se accede mediante un explorador web conectado a Internet;
- La solución de terminal virtual de su empresa está proporcionada y sujeta al hosting de un proveedor de servicios externo validado por las PCI DSS;
- Su empresa accede a la solución de terminal virtual compatible con las PCI DSS a través de una computadora que está aislada en una ubicación individual, y no está conectada a otras ubicaciones o sistemas dentro de su entorno (esto se puede alcanzar mediante un firewall o una segmentación de red para aislar la computadora de los demás sistemas);
- La computadora de su empresa no tiene software instalado que ocasione que los datos de titulares de tarjetas se almacenen (por ejemplo, no hay software para procesamiento por lotes o almacenamiento y transmisión);
- La computadora de su empresa no tiene dispositivos de hardware conectados que se utilizan para capturar o almacenar datos de titulares de tarjetas (por ejemplo, no hay lectores de tarjetas conectados);
- Su empresa no recibe de otro modo datos de titulares de tarjetas electrónicamente a través de canales (por ejemplo, mediante una red interna o Internet);
- Su empresa conserva solamente informes en papel o copias en papel de recibos; **y**
- Su empresa no almacena datos del titular de la tarjeta en formato electrónico.

Esta opción nunca se aplicaría a comerciantes de comercio electrónico.

SAQ C – Comerciantes con sistemas de aplicaciones de pago conectados a Internet, sin almacenamiento electrónico de datos de titulares de tarjetas

SAQ C ha sido desarrollado para abordar los requisitos aplicables a los comerciantes cuyos sistemas de aplicación de pago (por ejemplo, sistemas de punto de venta) están conectados a Internet (por ejemplo, a través de DSL, módem de cable, etc.). porque:

1. *El sistema de aplicación de pago reside en una computadora personal conectada a Internet (por ejemplo, para fines de correo electrónico o para navegar la red), o*
2. *El sistema de aplicación de pago está conectada a la Internet para transmitir datos de los titulares de tarjeta.*

Para consultar una guía gráfica que lo ayude a determinar su tipo de SAQ, consulte "¿Cuál SAQ se aplica mejor a mi entorno?" en la página 17.

Los comerciantes correspondientes al SAQ C procesan los datos de los titulares de tarjeta a través de máquinas de POS u otros sistemas de aplicaciones de pago conectados a Internet, no almacenan datos de los titulares de tarjeta en ningún sistema informático, y pueden ser comerciantes con instalaciones físicas (con la tarjeta presente) o comercio electrónico o pedido por correo electrónico/teléfono (tarjeta no presente). Los comerciantes de SAQ C validan el cumplimiento llenando el SAQ C y la Declaración de cumplimiento, con los cuales confirman que:

- Su empresa tiene un sistema de aplicaciones de pago y conexión a Internet en el mismo dispositivo y/o la misma red de área local (LAN);
- El sistema de aplicación de pago o dispositivo de Internet no está conectado a otros sistemas dentro de su entorno (esto se puede lograr a través de la segmentación de la red para aislar el sistema de aplicaciones de pago/dispositivo de Internet de todos los otros sistemas);
- La tienda de su empresa no está conectada a otras ubicaciones de las tiendas, y ninguna LAN es para una sola tienda;
- Su empresa conserva solamente informes en papel o copias en papel de recibos;
- Su compañía no almacena datos de titulares de tarjeta en formato electrónico; **y**
- El proveedor del software de la aplicación de pagos de su empresa utiliza técnicas seguras para proporcionar soporte remoto a su sistema de aplicación de pago.

SAQ D – Todos los demás comerciantes y todos los proveedores de servicio definidos por una marca de tarjeta de pago como elegible para completar un SAQ

El SAQ D se ha desarrollado para todos los proveedores de servicio elegibles para completar un SAQ según lo definido por la marca de pago, así como para los comerciantes que son elegibles para SAQ que no caen dentro de los SAQ A a C según lo descrito anteriormente.

Los proveedores de servicio y comerciantes elegibles para SAQ D validan su cumplimiento al completar el SAQ D y la Declaración de cumplimiento asociada.

Si bien muchas de las organizaciones que completan el SAQ D deberán validar su cumplimiento con todos los requisitos de las PCI DSS, es posible que algunas de las organizaciones con modelos de negocio muy específicos encuentren que algunos requisitos no son aplicables. Por ejemplo, no se esperaría de una compañía que no utiliza tecnología inalámbrica en modo alguno que valide el cumplimiento con las secciones de las PCI DSS relacionadas con el manejo de tecnología inalámbrica. Consulte la directriz de abajo para obtener información sobre la exclusión de tecnología inalámbrica y otros requisitos específicos.

Guía para la no aplicabilidad de ciertos requisitos específicos

Exclusión: Si se requiere que responda el SAQ C o D a fin de validar su cumplimiento con las PCI DSS, se deben considerar las siguientes excepciones. Consulte "No aplicabilidad" debajo para la la correspondiente respuesta de SAQ.

- Requisitos 1.2.3, 2.1.1 y 4.1.1 (SAQ C y D): Las preguntas específicas a la tecnología inalámbrica sólo deben ser contestadas si la tecnología inalámbrica está presente en cualquier parte de la red. Tenga en cuenta que el Requisito 11.1 (uso de un proceso para identificar los puntos de acceso inalámbricos no autorizados) de cualquier modo deben ser respondido incluso si en su red no hay tecnología inalámbrica, debido a que el proceso detecta cualesquiera accesos fraudulentos o dispositivos no autorizados que se hayan añadido sin su conocimiento.
- Requisitos 6.3 y 6.5 (SAQ D): Las preguntas son específicas de las aplicaciones personalizadas y el código y sólo se deben responder si su organización desarrolla sus propias aplicaciones personalizadas.
- Requisitos 9.1 a 9.4 (SAQ D): Estas preguntas sólo se deben responder si las instalaciones poseen “áreas confidenciales”, tal como se define aquí. “Áreas confidenciales” hace referencia a cualquier centro de datos, sala de servidores o cualquier área que aloje sistemas que almacenan procesos o transmitan datos de titulares de tarjetas. Esto excluye las áreas donde sólo hay terminales de punto de venta, tales como el área de cajas de un comercio; no obstante, sí incluye las salas de servidores trastienda que almacenan datos de titulares de tarjetas y las áreas de almacenamiento de grandes cantidades de datos de titulares de tarjetas.

No Aplicabilidad: Para todos los SAQ, estos y otros requisitos que pudieran no ser aplicables a su entorno se deben indicar con “N/A” en la columna “Especial” del SAQ. En consecuencia, llene la hoja de trabajo “Explicación de no aplicabilidad” en el Anexo del SAQ para cada entrada "N/A".

Instrucciones para completar el SAQ

1. Utilice las directrices que le damos en este documento para determinar cuál SAQ es el apropiado para su empresa.
2. Utilice le documento *Navegación de las PCI DSS: Comprensión del objetivo de los requisitos* para entender cómo y por qué los requisitos son relevantes para su organización.
3. Evalúe su entorno de cumplimiento de las PCI DSS.
4. Utilice el Cuestionario de Autoevaluación apropiado como herramienta para validar su cumplimiento con las PCI DSS.
5. Siga las instrucciones dadas en la sección “Cumplimiento con las PCI DSS – Pasos para Completar el Proceso” del Cuestionario de Autoevaluación apropiado y proporcione toda la documentación requerida a su adquirente o marca de pago, según sea apropiado.

¿Cuál SAQ se aplica mejor a mi entorno?