Payment Card Industry
Estándar de Seguridad de Datos

Instrucciones y Directrices del Cuestionario de Autoevaluación

Versión 4.0.1

Revisión 1

Abril de 2025

Cambios en el Documento

Fecha	Versión	Descripción
1 de Octubre, 2008	1.2	Para alinear el contenido con el nuevo estándar PCI DSS v1.2 e implementar los cambios menores observados desde la v1.1 original.
28 de Octubre, 2010	2.0	Para linear el contenido con el nuevo estándar PCI DSS v2.0 y aclarar los tipos de entorno SAQ y los criterios de elegibilidad. Adición de SAQ C-VT para comerciantes de Terminales Virtuales Basados en la Web.
Junio de 2012	2.1	Adición de SAQ P2PE-HW para comerciantes que procesan datos de tarjetahabiente solo a través de terminales de pago de hardware incluidas en una solución de cifrado Punto a Punto PCI (P2PE) validada de la lista por PCI SSC. Este documento es para uso con PCI DSS versión 2.0.
Abril de 2015	3.1	Alinear el contenido con PCI DSS v3.1, incluida la adición de los SAQ A-EP y B-IP, y aclarar los criterios de elegibilidad para los SAQ existentes.
Mayo de 2016	3.2	Actualizado para alinearse con PCI DSS v3.2 y aclarar los criterios de elegibilidad para los SAQ existentes.
Junio de 2018	3.2.1	Actualizaciones menores para alinearse con PCI DSS v3.2.1.
Septiembre de 2023	4.0	Se actualizó para alinear el contenido con PCI DSS v4.0, aclarar los criterios de elegibilidad para los SAQ existentes, incorporar el contenido de *Comprensión de los SAQ para PCI DSS v3.0* e incluir la adición de SAQ SPoC.
Octubre de 2024	4.0.1	Actualizado para alinearse con PCI DSS v4.0.1. Para ver los detalles de cambios en PCI ver *PCI DSS –Resumen de Cambios de la Versión PCI DSS 4.0 a 4.0.1*. Para el SAQ C-VT, se actualizaron los Criterios de Elegibilidad que hacen referencia a la “segmentación de la red” para alinearlos con la redacción del SAQ C-VT restaurada del SAQ C-VT para PCI DSS v3.2.1, y se añadió guía adicional para aclarar.
Abril de 2025	4.0.1 r1	Corrección de la tabla (Métodos comunes de comercio electrónico y SAQs aplicables) para reflejar con precisión el número de requisitos aplicables de PCI DSS. Se eliminaron los Requisitos 6.4.3 y 11.6.1 de la sección "Importancia de los nuevos requisitos añadidos al SAQ A para PCI DSS v4.x." Se añadieron los nuevos Criterios de Elegibilidad del SAQ A para los comerciantes de comercio electrónico en los siguientes dos lugares: A la tabla de "¿Cómo se compara el SAQ A con el SAQ A-EP?" A la sección de Criterios de Elegibilidad del SAQ A.

DECLARACIONES: La versión en inglés del texto en este documento tal y como se encuentra en el sitio web de PCI SSC deberá considerarse, para todos los efectos, como la versión oficial de estos documentos y, si existe cualquier ambigüedad o inconsistencia entre este texto y el texto en inglés, el texto en inglés en dicha ubicación es el que prevalecerá.

Contenido

Acerca de este Documento

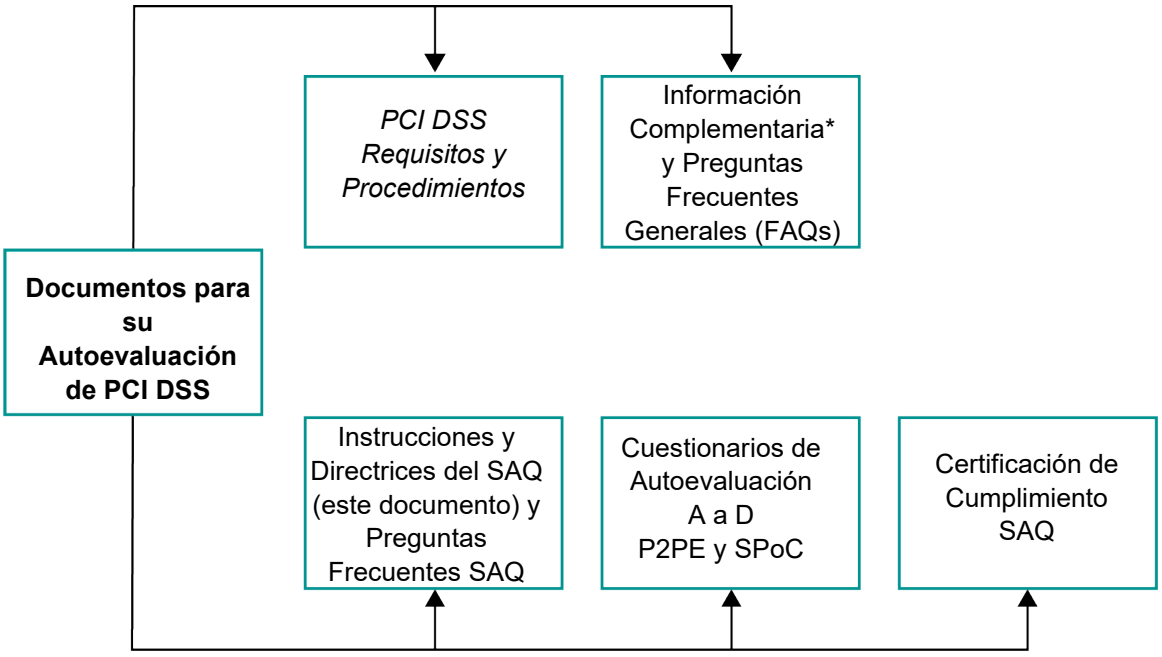
Este documento se ha elaborado para ayudar a comerciantes y proveedores de servicios a comprender los Cuestionarios de Autoevaluación (SAQ) del Estándar de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI DSS). Para entender los SAQ, qué estrategias puede utilizar su organización para llenar con facilidad un SAQ de PCI DSS y qué SAQ puede realizar su organización, le recomendamos que revise este documento de Instrucciones y Directrices en su totalidad.

Autoevaluación PCI DSS: Cómo Encaja Todo

PCI DSS y sus documentos de apoyo representan un conjunto común de herramientas de la industria para ayudar a garantizar el manejo seguro de los datos del titular de la tarjeta. El propio estándar ofrece un marco práctico para desarrollar un proceso de seguridad sólido, que incluye la prevención, detección y reacción ante incidentes de seguridad. Para reducir el riesgo de compromiso y mitigar el impacto en caso de que se produzca, es importante que todas las entidades que almacenan, procesan o transmiten datos del titular de la tarjeta protejan esos datos implementando los requisitos PCI DSS aplicables.

En el siguiente cuadro se describen las herramientas existentes para ayudar a las organizaciones a comprender a PCI DSS y el proceso de autoevaluación.

Estos y otros documentos relacionados pueden consultarse en www.pcisecuritystandards.org.



* ***Nota:*** *Los Suplementos Informativos sólo proporcionan información complementaria y orientación, y no sustituyen ni reemplazan ningún requisito PCI DSS.*

Descripción General de SAQ

Los *Cuestionarios de Autoevaluación* (SAQ) de PCI DSS son herramientas de validación para uso de comerciantes y proveedores de servicios elegibles para SAQ al realizar e informar los resultados de su autoevaluación PCI DSS. Existen múltiples versiones de los SAQ PCI DSS para responder a las distintas situaciones de los comerciantes. Este documento ha sido desarrollado para ayudar a las organizaciones elegibles para SAQ a determinar qué SAQ se aplica mejor a sus entornos.

Los PCI DSS SAQ son herramientas de validación alternativas para comerciantes y proveedores de servicios a los que un adquirente o una marca de pago no exige presentar un Informe de Conformidad (ROC) de PCI DSS. Ser “elegible para SAQ” significa que el comerciante o proveedor de servicios:

- Es elegible para realizar autoevaluaciones para validar su conformidad PCI DSS, de acuerdo con los programas de conformidad de marcas de pago,
- Cumple con los Criterios de Elegibilidad del SAQ especificados en el SAQ elegido.

Las organizaciones son responsables de confirmar que cumplen todos los criterios de elegibilidad para un SAQ particular antes de comenzar su autoevaluación.

Nota: *Se recomienda a todas las entidades que llenen los SAQ que se pongan en contacto con las organizaciones que gestionan los programas de conformidad y a las que se presentará el SAQ—por ejemplo, un adquirente (banco comerciante) o las marcas de pago— para confirmar que son elegibles para llenar un SAQ, para validar la conformidad con PCI DSS y para entender cualquier requisito o instrucción específicos.*

Cada SAQ PCI DSS consta de las siguientes secciones:

1. Llenando el Cuestionario de Autoevaluación: Esta sección incluye los criterios de elegibilidad para ese SAQ específico, junto con las instrucciones para llenarlo y una guía para ayudarle en el proceso de autoevaluación. Consulte "Seleccionar el SAQ y el Certificado que Mejor se Apliquen a Su Organización" en este documento para conocer los criterios de elegibilidad de cada SAQ.

   Además, cada SAQ incluye Pasos para Llenar la Autoevaluación, actividades de Prueba Previstas, opciones de Respuestas a los Requisitos, Guía para Requisitos No Aplicables, uso de Restricciones Legales y Recursos Adicionales PCI SSC.

2. Certificación de Conformidad: La Certificación es la declaración de elegibilidad de la entidad para completar el SAQ aplicable y su certificación de los resultados de una autoevaluación PCI DSS. La Certificación de Conformidad en cada SAQ consta de la Sección 1: Información sobre la Evaluación y Sección 3: Certificación y Detalles de Validación.
3. Requisitos PCI DSS: La Sección 2 de cada SAQ consta de los requisitos PCI DSS aplicables para el entorno identificados en los criterios de elegibilidad del SAQ, junto con un lugar para que la entidad registre las respuestas para cada requisito. Esta sección también incluye los anexos aplicables para ese SAQ (por ejemplo, documentar el uso de controles compensatorios y describir cualquier respuesta No aplicable).

Controles de Compensación

Los controles compensatorios pueden considerarse cuando una organización no puede cumplir un requisito PCI DSS tal y como está establecido debido a limitaciones técnicas o empresariales legítimas y documentadas, pero ha mitigado suficientemente el riesgo asociado implementando controles alternativos. Para implementar un control compensatorio para uno o más requisitos PCI DSS, su organización debe hacer lo siguiente:

1. Siga los procedimientos para definir y documentar los controles compensatorios tal y como se indica en el Anexo B de PCI DSS, "Controles Compensatorios", incluido el llenado de una Ficha de Control Compensatorio (CCW) para cada requisito que se cumpla con un control compensatorio.
2. Documente cada control compensatorio completando el Anexo B: Ficha de Control Compensatorio en el SAQ.

   Se debe completar una Ficha de Control Compensatorio (CCW) para cada requisito que se cumpla con un control de compensación.

   Se pueden encontrar Fichas de Control de Compensatorio adicionales en el sitio web PCI SSC.

3. Para cada requisito que se cumplió con un control compensatorio, responda a ese requisito en el SAQ marcando la columna "Implementado con CCW".

Asistencia Profesional y Entrenamiento

Si desea contratar a un profesional de seguridad para que lo ayude con su autoevaluación, le recomendamos que considere comunicarse con un Asesor de Seguridad Calificado (QSA). Los QSA han sido capacitadas por PCI SSC para llevar a cabo evaluaciones PCI DSS y figuran en la lista del sitio web PCI SSC.

- El sitio web PCI SSC es una fuente primaria de recursos adicionales, entre los que se incluyen:
  - *Glosario de Términos, Abreviaturas y Acrónimos de PCI DSS*
  - Preguntas Frecuentes (FAQ)
  - Seminarios Web
  - Directrices e Información Complementaria
  - Formularios SAQ y Certificaciones de Conformidad
  - Pequeños recursos comerciales.
- PCI SSC también ofrece varios programas de entrenamiento para ayudar a crear conciencia entre el personal de una organización. Algunos ejemplos incluyen la Concienciación sobre la PCI, el programa de Profesionales PCI (PCIP) y el programa de Asesores Internos de Seguridad (ISA).
- Consulte www.pcisecuritystandards.org para obtener más información.
- Los programas y recursos de capacitación relacionados con los pagos también pueden estar disponibles a través de las marcas de pagos y/o su adquirente comercial.

Nota: *Los Suplementos de Información complementan PCI DSS e identifican consideraciones y recomendaciones adicionales para cumplir con los requisitos PCI DSS; no cambian, eliminan ni reemplazan a PCI DSS ni a ninguno de sus requisitos.*

Comprensión de los SAQ para PCI DSS v4.x

Hay varios tipos de SAQ que se resumen en la siguiente tabla y se describen con más detalle en las páginas siguientes. Utilice la tabla para ayudar a determinar qué SAQ se aplica a su organización y luego revise las descripciones detalladas que siguen para asegurarse de cumplir con todos los criterios de elegibilidad para ese SAQ.

Nota: *Se recomienda a todas las entidades que llenen el SAQ que se comuniquen con las organizaciones que administran programas de conformidad y a las que se enviará el SAQ,—por ejemplo, un adquirente (banco comercial) o las marcas de pago—para confirmar que son elegibles para llenar el SAQ, para validar la conformidad de PCI DSS y comprender cualquier requisito o instrucción específica.*

Para los proveedores de servicios elegibles para realizar una autoevaluación, el único SAQ aplicable es el SAQ D para Proveedores de Servicios.

SAQ	Descripción
A	Comerciantes sin tarjeta presencial (comercio electrónico o pedidos por correo/teléfono) que subcontratan completamente todas las funciones de los datos del titular de la tarjeta a terceros validados en conformidad con PCI DSS. No hay almacenamiento electrónico, procesamiento o transmisión de datos del titular de la tarjeta en sus sistemas o instalaciones. *Este SAQ no es aplicable a los canales de cara al público. No aplicable a los proveedores de servicios.*
A-EP	Comerciantes de comercio electrónicos que subcontratan parcialmente el procesamiento de pagos a terceros validados en conformidad con PCI DSS, y con una o varias páginas web que no reciben por sí mismas datos del titular de la tarjeta, pero que sí afectan la seguridad de la transacción de pago y/o a la integridad de la página que acepta los datos del titular de la tarjeta del cliente. Ningún almacenamiento, procesamiento o transmisión electrónica de datos del titular de la tarjeta en los sistemas o instalaciones del comerciante. *Aplicable únicamente a los canales de comercio electrónico. No aplicable a los proveedores de servicios.*
B	Sólo para comerciantes: ▪ Máquinas de impresión sin almacenamiento electrónico de datos del titular de la tarjeta, y/o ▪ Terminales autónomos de marcación de salida sin almacenamiento electrónico de datos del titular de la tarjeta. *No aplicable a los canales de comercio electrónico. No aplicable a los proveedores de servicios.*
B-IP	Comerciantes que utilizan únicamente dispositivos de Punto de Interacción (POI) de Seguridad de Transacciones con PIN (PTS) autónomos y aprobados por PCI con una conexión IP al procesador de pagos. No hay almacenamiento electrónico de datos del titular de la tarjeta. *No aplicable a los canales de comercio electrónico. No aplicable a los proveedores de servicios.*

SAQ	Descripción
C-VT	Comerciantes que introducen manualmente los datos del titular de la tarjeta de una transacción a la vez a través de un teclado en una solución de terminal de pago virtual de terceros validada y en conformidad con PCI DSS, con un dispositivo informático aislado y un navegador web conectado de forma segura. No hay almacenamiento electrónico de datos del titular de la tarjeta. *No aplicable a los canales de comercio electrónico. No aplicable a los proveedores de servicios.*
C	Comerciantes con sistemas de aplicación de pagos conectados a Internet, sin almacenamiento electrónico de datos del titular de la tarjeta. *No aplicable a los canales de comercio electrónico. No aplicable a los proveedores de servicios.*
P2PE	Comerciantes que utilizan únicamente una solución de Cifrado Punto a Punto (P2PE) validada incluida en la lista PCI. No hay acceso a datos del titular de la tarjeta en texto claro ni almacenamiento electrónico de datos del titular de la tarjeta. *No aplicable a los canales de comercio electrónico. No aplicable a los proveedores de servicios.*
SPoC*	Comerciantes que utilicen un producto comercial disponible (por ejemplo, un teléfono o una tableta) con un lector de tarjetas seguro incluido en la lista PCI SSC de Soluciones SPoC validadas. No hay acceso a datos del titular de la tarjeta en texto claro ni almacenamiento electrónico de datos del titular de la tarjeta. *No se aplica a los canales de comercio electrónico con tarjeta presencial, los pedidos por correo o por teléfono (MOTO) desatendidos.* *No aplicable a los proveedores de servicios.*
D	***SAQ D para Comerciantes:*** Todos los comercios no incluidos en las descripciones de los tipos de SAQ anteriores. *No aplicable a los proveedores de servicios.*
	SAQ D para los Proveedores de Servicios: Todos los proveedores de servicios definidos por una marca de pago como elegibles para completar un SAQ.

** Nuevo SAQ para PCI DSS v4.x*

¿Qué hay de nuevo en los SAQ de PCI DSS v4.x?

Los SAQ v4.x se han actualizado para proporcionar más guías, información sobre los informes y recursos para apoyar a las entidades que completan el proceso de autoevaluación. En general, cada SAQ se actualizó para reflejar los cambios realizados en los requisitos PCI DSS v4.x, para reformular cada requisito SAQ de modo que reflejara la redacción utilizada en PCI DSS y para alinear las respuestas de los informes para cada requisito del SAQ con las utilizadas en la Plantilla de Informe de Conformidad PCI DSS v4.x. Para obtener más detalles sobre los cambios generales realizados en todos los SAQ, consulte el Anexo A: Cómo han cambiado los SAQ para PCI DSS v4.x.

Por qué algunos requisitos PCI DSS en los SAQ incluyen casillas de verificación de respuesta

Para la mayoría de los requisitos PCI DSS en los SAQ, solo hay una casilla de verificación para que una entidad seleccione; sin embargo, algunos requisitos incluyen una casilla de verificación para cada viñeta de ese requisito (por ejemplo, el Requisito 6.4.3 PCI DSS). Este enfoque se adoptó sólo para ciertos requisitos de los SAQ, generalmente para requisitos nuevos y/o complejos donde cada punto requiere un enfoque de prueba diferente, y para enfatizar que cada punto debe considerarse por sí mismo.

Se proporciona una guía e información adicional sobre el formato del SAQ en la sección "Cómo Completar el Cuestionario de Autoevaluación" de cada SAQ.

¿Cómo afectarán las actualizaciones del SAQ a mi organización?

Con PCI DSS v4.x, hay un nuevo SAQ, así como criterios de elegibilidad aclarados para los SAQ existentes. Las organizaciones tendrán que revisar los criterios de elegibilidad para entender qué SAQ es el adecuado para ellas. Por ejemplo, el nuevo SAQ puede ajustarse mejor al entorno particular de una organización que el SAQ utilizado anteriormente. Del mismo modo, una organización que haya completado previamente un tipo de SAQ tendrá que revisar los criterios de elegibilidad actualizados para ese SAQ para determinar si sigue siendo apropiado para su entorno.

Algunos SAQ se actualizaron para incluir requisitos adicionales PCI DSS que no estaban en ese SAQ para la versión 3.2.1 PCI DSS. Esto tendrá un impacto en la forma en que el comerciante aborde su autoevaluación.

Para comprender por qué se han añadido nuevos requisitos al SAQ A para PCI DSS v4.x, consulte *Descripción General: SAQ A y SAQ A-EP a continuación.*

Los comerciantes deben continuar eligiendo un SAQ aplicable según los criterios de elegibilidad definidos para cada SAQ y de acuerdo con las instrucciones de su adquirente o marca de pago. Se recomienda a los comerciantes que lean el SAQ pertinente a PCI DSS v4.0 para 1) confirmar que el comerciante sigue cumpliendo los criterios de elegibilidad y 2) familiarizarse con toda la redacción actualizada y todos los requisitos incluidos en dicho SAQ.

Los comerciantes no deben asumir que un SAQ particular para PCI DSS v3.2.1 y v4.x es el mismo.

SAQ SPoC – El nuevo SAQ para PCI DSS v4.0

El SAQ SPoC (Entrada de PIN basada en software en COTS) es un nuevo SAQ para comerciantes que utilizan un producto comercial disponible (por ejemplo, un teléfono o una tableta) con un lector de tarjetas seguro que forma parte de una solución SPoC de la lista del PCI SSC de Soluciones validadas de Entrada de PIN basada en Software en COTS (SPoC). Para ser elegible para este SAQ, los comerciantes solo deben ingresar datos del titular de la tarjeta a través de un PIN de lector de tarjeta seguro (SCRP) como parte de una Solución PCI SSC SPoC validada.

El listado de Soluciones SPoC puede encontrarse aquí: Soluciones PCI SPoC

¿Cuál es la intención del SAQ SPoC?

El SAQ SPoC se ha desarrollado para comerciantes con tarjeta presencial que utilizan productos comerciales disponibles (COTS). Esto significa que el dispositivo móvil (por ejemplo, un teléfono o una tableta) no tiene por qué utilizarse únicamente para pagar ni tiene por qué estar dedicado a un canal de pago. El dispositivo móvil COTS se utiliza junto con un dispositivo Lector de Tarjetas Seguro para PIN (SCRP**)** incluido en la lista PCI como parte de una Solución PCI SSC SPoC para procesar de forma segura los datos del titular de la tarjeta. Tenga en cuenta que este SAQ no se aplica a soluciones SPoC con lectores de banda magnética (MSR) que no figuran en la lista PTS. Este SAQ puede utilizarse con los SCRP incluidos en la lista de PTS que incluyan la funcionalidad MSR.

El SAQ SPoC reduce significativamente la cantidad de requisitos PCI DSS aplicables para los comerciantes que utilizan una solución SPoC de la lista PCI SSC.

¿Cómo se compara SAQ SPoC con SAQ P2PE?

La siguiente tabla ofrece una descripción de alto nivel de algunas de las principales similitudes y diferencias entre SAQ P2PE y SAQ SPoC.

	SAQ P2PE	**SAQ SPoC**
	Dispositivo POI aprobado por PTS en una solución P2PE incluida en la lista PCI	**Dispositivo COTS y un dispositivo SCRP en una Solución SPoC incluida en la lista PCI**
Se aplica a:	Comercios **con o sin tarjeta presencial** (pedido por correo o telefónica)	Sólo comerciantes atendidos con **tarjeta presencial** (chip de contacto, sin contacto, banda magnética basada en SCRP)
Terminales de Pago	El pago se procesa a través de un **POI aprobado por PTS** como parte de una solución P2PE incluida en la lista PCI	Los datos de tarjetahabiente se introducen en un **dispositivo SCRP aprobado por PTS** como parte de una solución SPoC incluida en la lista PCI
Transmisiones de datos del Titular de la Tarjeta	Sólo desde un dispositivo PTS POI como parte de una **solución P2PE validada incluida en la lista PCI**	Sólo con un dispositivo PTS SCRP como parte de una **solución SPoC incluida en la lista PCI validada**
Sistemas Comerciales	Sin acceso a datos del titular de la tarjeta en texto claro en ningún sistema informático El comerciante no recibe, transmite ni almacena electrónicamente los datos del titular de la tarjeta	
Retención de Datos	El comerciante sólo conserva los informes o recibos en papel con los datos del titular de la tarjeta, y estos documentos no se reciben electrónicamente	

Esta tabla pretende ofrecer una comparación entre el SAQ P2PE y el SAQ SPoC y no sustituye ni reemplaza los criterios de elegibilidad de ninguno de los dos SAQ.

Acrónimos, Estándar y Listas de P2PE y SPoC

Acrónimos	Definición y Estándar Afines	Listas de Soluciones/Dispositivos*
P2PE	Estándar de Encriptación Punto a Punto	Soluciones PCI P2PE
PTS POI	Estándar de Seguridad de Transacciones con PIN (PTS) Clase de Aprobación del Punto de Interacción (POI)	Dispositivos PTS Aprobados
SPoC	Estándar de Entrada de PIN basada en Software en COTS (producto comercial disponible)	Soluciones PCI SPoC
PTS SCRP	Estándar de Seguridad de Transacciones con PIN (PTS) Clase de Aprobación de PIN de Lector de Tarjetas Seguro (SCRP)	Dispositivos PTS Aprobados

* Se confirma que las soluciones y dispositivos enumerados cumplen con los requisitos definidos en ese Estándar PCI y la Guía del Programa relacionada.

Descripción General: SAQ A y SAQ A-EP

El **SAQ A** está destinado a comerciantes sin tarjeta presencial (pedidos por correo/teléfono o comercio electrónico) que han subcontratado completamente todas las funciones de datos del titular de la tarjeta a un proveedor de servicios externo (TPSP) validado y en conformidad con PCI DSS. Los comerciantes SAQ A no almacenan, procesan ni transmiten electrónicamente datos del titular de la tarjeta en sus sistemas o instalaciones.

El **SAQ A-EP** está destinado a los comerciantes que han subcontratado parcialmente la gestión de sus transacciones de comercio electrónico, pero que tienen funcionalidades en sus sitios web que afectan la seguridad de la transacción de pago.

Al igual que con SAQ A, los comerciantes de SAQ A-EP no almacenan, procesan ni transmiten electrónicamente ningún dato del titular de la tarjeta en sus sistemas o instalaciones, sino que dependen completamente de un TPSP para manejar estas funciones. Todo el procesamiento de los datos del titular de la tarjeta se subcontrata a un TPSP/procesador de pagos validado por PCI DSS tanto para SAQ A como para SAQ A-EP.

El SAQ A-EP incluye controles de seguridad adicionales necesarios para proteger los sitios web de los comerciantes que controlan o gestionan la transacción de pago, aunque estos sitios web no almacenen, procesen ni transmitan datos del titular de la tarjeta. Con ello se pretende reducir la probabilidad de que las violaciones de estos sitios web puedan utilizarse para comprometer los datos del titular de la tarjeta.

¿Qué tipos de implementaciones de comercio electrónico son elegibles para SAQ A frente al SAQ A-EP?

Para ser elegible para el SAQ A, los comerciantes de comercio electrónico deben cumplir con todos los criterios de elegibilidad detallados en el SAQ A, incluido el hecho de que no existen programas o códigos de aplicación que capturen información de pago en la página web del comerciante. Entre los ejemplos de implementaciones de comercio electrónico que aborda el SAQ A se incluyen:

- El comerciante no tiene acceso a su página web, y la página web está completamente alojado y administrado en conformidad con un procesador de pagos/TPS.
- La página web del comerciante redirige a los usuarios (por ejemplo, con una URL que redirige a un procesador /TPSP en conformidad con PCI DSS que facilita el proceso de pago.
- La página web del comerciante proporciona un marco en línea (iframe) a un TPSP/procesador en conformidad con PCI DSS y que facilita el proceso de pago.

Si cualquier elemento de una página de pago entregada a los navegadores de los consumidores se origina en el sitio web del comerciante, el SAQ A no se aplica; sin embargo, puede ser aplicable el SAQ A-EP. Ejemplos de implementaciones de comercio electrónico abordadas por el SAQ A-EP incluyen:

- El sitio web del comerciante crea el formulario de pago y los datos de pago se envían directamente desde el navegador del consumidor al procesador de pagos (a menudo denominado "Publicación directa").
- El sitio web del comerciante carga o entrega scripts que se ejecutan en los navegadores de los consumidores (por ejemplo, JavaScript) y proporciona una funcionalidad que respalda la creación de la página de pago y/o cómo se transmiten los datos al procesador de pagos.

La siguiente tabla ilustra los métodos comunes de comercio electrónico y qué SAQ se puede aplicar:

Método de Comercio Electrónico	Tipo de SAQ para Comerciantes Elegibles	Número de Requisitos PCI DSS v4.x
Totalmente subcontratado. El comerciante no tiene acceso a su propia página web.	SAQ A	14*
Totalmente subcontratado. La página web del comerciante redirige a los clientes a un TPSP conforme (por ejemplo, una URL redirigida).		27*
Totalmente subcontratado. La página web del comerciante incluye una página/formulario de pago integrado de TPSP en conformidad (por ejemplo, un iframe).		27*
Totalmente subcontratado, excepto la página de pago. El sitio web del comerciante crea el formulario de pago y los datos de pago se envían directamente desde el navegador del consumidor al TPSP (a menudo denominado "Publicación Directa").	SAQ A-EP	139
Totalmente subcontratado, excepto la página de pago. El sitio web del comerciante carga o entrega scripts que se ejecutan en el navegador del consumidor (por ejemplo, JavaScript).		
Todos los demás métodos e implementaciones de comercio electrónico.	SAQ D para Comerciantes	Todos los Requisitos PCI DSS

Los criterios para los canales de pedidos por correo/teléfono (MOTO) del SAQ A no se incluyen en esta tabla.

** Los requisitos aplicables se identifican mediante notas explicativas en el SAQ A.*

Importancia de los nuevos requisitos añadidos al SAQ A para PCI DSS v4.x

El SAQ A para PCI DSS v4.x incluye controles de seguridad adicionales necesarios para abordar infracciones comunes que tienen como objetivo a los comerciantes SAQ A, específicamente para proteger la página web que 1) redirigen transacciones de pago a un TPSP en conformidad con PCI DSS o 2) incluyen una página/formulario de pago integrado a un TPSP en conformidad con PCI DSS. Para mitigar estas infracciones comunes, se incluyen los Requisitos 11.3.2 y 11.3.2.1 en el SAQ A (***Nota***: *Esta lista destaca los requisitos agregados para abordar específicamente las recientes infracciones del comercio electrónico; Esta no es una lista de todos los requisitos nuevos incluidos en el SAQ A).*

¿Cómo se compara el SAQ A con el SAQ A-EP?

La siguiente tabla proporciona una descripción de alto nivel de algunas de las principales similitudes y diferencias entre el SAQ A y el SAQ A-EP.

	SAQ A	SAQ A-EP
	Todas las Funciones de Datos del Titular de la Tarjeta Completamente Subcontratadas	**Canal de Pago de Comercio Electrónico Comercialmente Subcontratado**
Se aplica a:	**Comerciantes sin tarjeta presencial** (comercio electrónico o pedido por correo/teléfono)*	Comerciantes de **comercio electrónico**
Funciones Subcontratadas	**Todo el procesamiento** de datos del titular de la tarjeta se subcontrata por completo a un proveedor de servicios de terceros (TPSP)/procesador de pagos que se encuentre en conformidad con PCI DSS	Todo el procesamiento de los datos del titular de la tarjeta, **excepto la página de pago**, está totalmente subcontratado a un TPSP/procesador de pagos en conformidad con PCI DSS
Página de Pago	Todos los elementos de todas las páginas/formularios de pago enviadas al navegador del cliente se **originan única y directamente** desde un TPSP/procesador en conformidad con PCI DSS El comerciante ha confirmado que la página web del comerciante no es susceptible a ataques mediante scripts	Cada elemento de las páginas de pago enviadas al navegador del cliente se **origina en el sitio web** del comerciante **o** en un TPSP en conformidad con PCI DSS
Conformidad de Terceros	El comerciante ha confirmado que todos los TPSP están en conformidad con PCI DSS para los servicios que utiliza el comerciante	
Sistemas Comerciales	El comerciante no almacena, procesa ni transmite electrónicamente ningún dato del titular de la tarjeta en los sistemas o instalaciones del comerciante, pero depende por completo de un TPSP(s) para que se encargue de todas estas funciones	
Retención de Datos	Cualquier dato del titular de la tarjeta retenido por el comerciante está en papel (por ejemplo, informes impresos o recibos), y estos documentos no se reciben electrónicamente	

** Los criterios para los canales de pedidos por correo/teléfono (MOTO) del SAQ A no se incluyen en esta comparación.*

Esta tabla pretende proporcionar una comparación entre el SAQ A y el SAQ A-EP y no sustituye ni reemplaza los criterios de elegibilidad de ninguno de los dos SAQ.

Descripción General: SAQ B y SAQ B-IP

El **SAQ B** está destinado a los comerciantes que procesan datos del titular de la tarjeta a través de máquinas de impresión o terminales autónomos de marcación de salida. Los comerciantes del SAQ B pueden ser tanto comerciantes que venden en establecimientos físicos (con tarjeta presencial) como comerciantes de pedidos por correo o por teléfono. Para ser elegible a este SAQ, los terminales autónomos de marcación de salida no se conectan a otros sistemas en el entorno comercial y no se conectan a Internet. Los comerciantes de SAQ B no almacenan datos del titular de la tarjeta en formato electrónico. Este SAQ no es aplicable a los canales de comercio electrónico.

SAQ B-IP está destinado a comerciantes que utilizan únicamente terminales de pago autónomos que se conectan a sus procesadores de pagos a través de una conexión basada en IP. Para ser elegible a SAQ B-IP, los comerciantes deben estar utilizando terminales de pago que sean dispositivos de punto de interacción (POI) con Seguridad de Transacciones con PIN (PTS) aprobados e incluidos en la lista PCI. Tenga en cuenta que los comerciantes que utilicen los dispositivos PTS POI clasificados como Lectores de Tarjetas Seguros (SCR) o Lectores de Tarjetas Seguros con PIN (SCRP) NO son elegibles para el SAQ B-IP.

Otros criterios de elegibilidad para SAQ B-IP incluyen que los dispositivos PTS POI aprobados no estén conectados a ningún otro tipo de sistema en el entorno comercial. Esto se puede lograr mediante una segmentación que aísle los dispositivos PTS POI de otros sistemas dentro del entorno. Las conexiones a otros tipos de sistemas que no cumplirían con los criterios de elegibilidad del SAQ B-IP incluyen, entre otras, conexiones a sistemas de caja registradora y si los dispositivos PTO POI dependen de cualquier otro dispositivo (por ejemplo, una computadora, un teléfono móvil , tableta, etc.) para conectarse al procesador de pagos. Además, para ser elegible al SAQ B-IP, la única transmisión permitida de datos del titular de la tarjeta es desde el dispositivo PTS POI al procesador de pagos, y el comerciante no debe almacenar datos del titular de la tarjeta en formato electrónico. SAQ B-IP, al igual que SAQ B, no es aplicable a canales de comercio electrónico.

¿Cómo se compara SAQ B-IP con SAQ B?

La siguiente tabla proporciona una descripción general de alto nivel de algunas de las similitudes y diferencias clave entre SAQ B y SAQ B-IP.

	SAQ B	SAQ B-IP
	Máquinas de impresión o terminales autónomos de marcación de salida	**Terminales de pago autónomos, aprobados por PTS y con conexión IP**
Se aplica a:	Tarjeta física (tarjeta presencial) o Comerciantes de pedidos por correo/teléfono (sin tarjeta presencial)	
Terminales de Pago	Terminales **autónomos de marcación de salida**	**Dispositivos autónomo de punto de interacción (POI), aprobados por PTS** (excluye lectores de tarjetas seguros (SCR y lectores de tarjetas seguros para PIN (SCRP))
Conexiones	**Conectado por línea telefónica** al procesador **Sin conexiones** a otros sistemas comerciales o a Internet	**Conectado vía IP** al procesador **Otros dispositivos POI aprobados por PTS conectados por IP pueden estar en la misma zona de red,** pero deben estar **aislados** de todos los demás tipos de sistemas.
Transmisiones de Datos del Titular de la Tarjeta	Sólo vía **línea telefónica** al procesador	Sólo vía **IP** desde los dispositivos POI aprobados por PTS al procesador
Sistemas Comerciales	El comerciante no almacena datos del titular de la tarjeta en formato electrónico	
Retención de Datos	El comerciante sólo conserva los informes o recibos en papel con los datos del titular de la tarjeta, y estos documentos no se reciben electrónicamente	

Esta tabla tiene como objetivo proporcionar una comparación entre SAQ B y SAQ B-IP y no sustituye ni reemplaza los criterios de elegibilidad para ninguno de los SAQ.

Descripción General: SAQ C-VT y SAQ C

SAQ C-VT está destinado a comerciantes que procesan datos del titular de la tarjeta únicamente a través de soluciones de terminales de pago virtuales de terceros en un dispositivo informático aislado conectado a Internet. El comerciante ingresa manualmente los datos del titular de la tarjeta en la solución de terminal de pago virtual desde un dispositivo informático aislado a través de un navegador web conectado de forma segura, y las transacciones con tarjeta de pago se envían para su autorización por parte del proveedor de servicios externo en conformidad con el PCI DSS que está alojando la solución de terminal de pago virtual. Los comerciantes de SAQ C-VT pueden ser comerciantes físicos (con tarjeta presencial) o comerciantes de pedidos por correo o por teléfono.

Para ser elegible para este SAQ, el comerciante solo accede a la solución de terminal de pago virtual en conformidad con PCI DSS a través de un dispositivo informático que está aislado en una única ubicación y que no está conectado a otras ubicaciones o sistemas en el entorno del comerciante. Esto puede lograrse mediante un firewall o segmentación de la red que aisla los sistemas del comerciante que acceden al terminal de pago virtual de otros sistemas del comerciante. Las conexiones a otros tipos de sistemas que NO son elegibles para este SAQ incluyen, pero no se limitan a, las conexiones

con sistemas de caja registradora, y si el terminal de pago virtual depende de cualquier otro dispositivo para conectarse al proveedor de la solución de terminal de pago virtual. Además, para ser elegible para el SAQ C-VT, la única transmisión permitida de datos del titular de la tarjeta es desde el terminal de pago virtual hacia la solución de terminal de pago virtual del tercero, y el comerciante no debe almacenar datos del titular de la tarjeta en formato electrónico.

SAQ C está destinado a comerciantes con sistemas de aplicaciones de pago (por ejemplo, sistemas de punto de venta) conectados a Internet. Los comerciantes de SAQ C pueden ser comerciantes físicos (con tarjeta presencial) o comerciantes de pedidos por correo o por teléfono. Para ser elegible para este SAQ, los sistemas de aplicaciones de pago del comerciante no se conectan a otros sistemas en el entorno del comerciante, y la ubicación física del entorno no está conectada a otras instalaciones o ubicaciones (solo una sola tienda).

El SAQ C y el SAQ C-VT no son aplicables a los canales de comercio electrónico.

¿Cómo se compara SAQ C-VT con SAQ C?

La siguiente tabla proporciona una descripción general de alto nivel de algunas de las similitudes y diferencias clave entre SAQ C-VT y SAQ C.

	SAQ C-VT	**SAQ C**
	Solución de Terminal de Pago Virtual de Terceros Basada en la Web	**Sistema de Aplicación de Pagos Conectado a Internet**
Se aplica a:	Tienda física (**tarjeta presencial)** o Comerciantes de pedidos por correo/teléfono (**sin tarjeta presencial**)	
Pago Método	Los datos del titular de la tarjeta se **ingresan manualmente** en una **solución de terminal de pago virtual de terceros** Dispositivo informático aislado y navegador web conectado de forma segura	**Punto de venta (POS)** u **otro sistema de aplicación de pagos**
Conexiones	Conectados a **Internet** **Sin conexiones a otras ubicaciones o sistemas**	Conectados a **Internet** **Sin conexiones a otros sistemas comerciales** Sin conexiones con otros locales o ubicaciones (**solo tienda única**)
Transmisiones de Datos del Titular de la Tarjeta	Solo a través de Internet a un **proveedor de Sistema de Terminal de Pago Virtual de Terceros en conformidad con PCI DSS**	Solo a través de Internet al procesador
Sistemas Comerciales	El comerciante no almacena datos del titular de la tarjeta en formato electrónico	
Retención de Datos	El comerciante sólo conserva los informes o recibos en papel con los datos del titular de la tarjeta, y estos documentos no se reciben electrónicamente	

Esta tabla tiene como objetivo proporcionar una comparación entre SAQ C-VT y SAQ C y no reemplaza ni reemplaza los criterios de elegibilidad para ninguno de los SAQ.

SAQ A – Comerciantes sin Tarjeta Presencial, Todas las Funciones de Datos del Titular de la Tarjeta Totalmente Subcontratadas

El SAQ A sólo incluye aquellos Requisitos de PCI DSS aplicables a los comerciantes con funciones de datos del titular de la tarjeta completamente externalizadas con terceros validados y conformes con PCI DSS, en los que el comerciante sólo conserva informes o recibos en papel con datos del titular de la tarjeta.

Para obtener una guía gráfica para elegir su tipo de SAQ, consulte "¿Cuál SAQ Se Aplica Mejor a Mi Entorno?" en las páginas 25 y 26.

Los comerciantes SAQ A pueden ser ya sea, comerciantes de comercio electrónico o de pedidos por correo o por teléfono (tarjeta no presente) y no almacenan, procesan ni transmiten ningún dato del titular de la tarjeta en formato electrónico en sus sistemas o locales.

Este SAQ no es aplicable a los canales de cara al público.

Este SAQ no es aplicable a los proveedores de servicios.

Los comerciantes del SAQ A confirmarán que cumplen con los siguientes criterios de elegibilidad para este canal de pago:

- El comerciante sólo acepta transacciones sin tarjeta (comercio electrónico o pedidos por correo o teléfono);
- Todo el procesamiento de datos del titular de la tarjeta se subcontrata íntegramente a un proveedor de servicios de terceros (TPSP)/procesador de pagos que esté en conformidad con PCI DSS;
- El comerciante no almacena, procesa o transmite electrónicamente ningún dato del titular de la tarjeta en los sistemas o instalaciones del comerciante, sino que depende enteramente de un TPSP para gestionar todas esas funciones;
- El comerciante ha confirmado que los TPSP se encuentran en conformidad con PCI DSS para los servicios utilizados por el comerciante; y
- Cualquier dato del titular de la tarjeta que el comerciante pueda conservar está impreso (por ejemplo, informes o recibos impresos), y estos documentos no se reciben electrónicamente.

Adicionalmente, para los canales de comercio electrónico:

- Todos los elementos de los formularios de las páginas de pago que se entregan al navegador del cliente se originan única y directamente en un procesador de pagos TPSP en conformidad con PCI DSS.
- El comerciante ha confirmado que su sitio no es susceptible a ataques mediante scripts que puedan afectar los sistemas de comercio electrónico del comerciante.

SAQ A-EP – Comerciantes de Comercio Electrónico Parcialmente Subcontratados Que Utilizan un Sitio Web de Terceros para el Procesamiento de Pagos

El SAQ A-EP sólo incluye aquellos Requisitos de PCI DSS aplicables a los comerciantes de comercio electrónico con un sitio web que no reciben por sí mismo los datos del titular de la tarjeta, pero que afectan a la seguridad de la transacción de pago y/o a la integridad de la página que acepta los datos del titular de la tarjeta.

Los comerciantes del SAQ A-EP son comercios de comercio electrónico que subcontratan parcialmente sus canales de pago de comercio electrónico a terceros validados y en conformidad con PCI DSS que no almacenan, procesan o transmiten electrónicamente ningún dato del titular de la tarjeta en sus sistemas o instalaciones.

Para obtener una guía gráfica para elegir su tipo de SAQ, consulte "¿Cuál SAQ Se Aplica Mejor a Mi Entorno?" en las páginas 25 y 26.

Este SAQ sólo aplica para los canales de comercio electrónico.

Este SAQ no aplica para los proveedores de servicios.

Los comercios SAQ A-EP confirmarán que cumplen con los siguientes criterios de elegibilidad para este canal de pago:

- El comerciante sólo acepta transacciones de comercio electrónico;
- Todo el procesamiento de los datos del titular de la tarjeta, a excepción de la página de pago, se subcontrata íntegramente a un proveedor de servicios de terceros (TPSP)/procesador de pagos que esté en conformidad con PCI DSS;
- El sitio web de comercio electrónico del comerciante no recibe los datos del titular de la tarjeta, sino que controla cómo los clientes, o sus datos del titular de la tarjeta, son redirigidos a un TPSP/procesador de pagos que esté en conformidad con PCI DSS;
- Si el sitio web del comerciante está alojado en un TPSP, éste cumple con todos los requisitos aplicables PCI DSS (incluyendo el Anexo A PCI DSS si el TPSP es un proveedor de alojamiento multiusuarios);
- Cada elemento de las páginas de pago entregadas al navegador del cliente se origina en el sitio web del comerciante o en un TPSP de conformidad con PCI DSS;
- El comerciante no almacena, procesa o transmite electrónicamente ningún dato del titular de la tarjeta en los sistemas o instalaciones del comerciante, sino que depende enteramente de un TPSP para gestionar todas esas funciones;
- El comerciante ha confirmado que se encuentran en conformidad con PCI DSS para los servicios utilizados por el comerciante; y
- Cualquier dato del titular de la tarjeta que el comerciante pueda conservar está impreso (por ejemplo, informes o recibos impresos), y estos documentos no se reciben electrónicamente.

Nota: *A los efectos de este SAQ A-EP, los Requisitos de PCI DSS que se refieren al "entorno de datos del tarjetahabiente" son aplicables al sitio web del comerciante. Esto se debe a que el sitio web del comerciante afecta directamente a la forma en que se transmiten los datos del titular de la tarjeta, aunque el sitio web en sí no reciba datos del titular de la tarjeta.*

SAQ B – Comerciantes con Sólo Máquinas de Impresión o Sólo Terminales Autónomos de Marcación Saliente, sin Almacenamiento Electrónico de Datos del Titular de la Tarjeta

El SAQ B sólo incluye aquellos Requisitos de PCI DSS aplicables a los comerciantes que procesan datos del titular de la tarjeta únicamente a través de impresoras o terminales autónomos de marcación. Los comerciantes SAQ B pueden ser comerciantes de tiendas físicas (con tarjeta) o de pedidos por correo o teléfono (sin tarjeta) y no almacenan datos del titular de la tarjeta en ningún sistema informático.

Este SAQ no es aplicable a los canales de comercio electrónico.

Este SAQ no aplica para los proveedores de servicios.

Los comercios SAQ B confirmarán que cumplen con los siguientes criterios de elegibilidad para este canal de pago:

- El comerciante utiliza únicamente una impresora y/o utiliza únicamente terminales autónomos de marcación (conectados a través de una línea telefónica al procesador del comerciante) para recabar la información de las tarjetas de pago de los clientes;
- Los terminales autónomos de acceso telefónico no están conectados a ningún otro sistema del entorno comercial;
- Los terminales autónomos de acceso telefónico no están conectados a Internet;
- El comerciante no almacena datos del titular de la tarjeta en formato electrónico; y
- Cualquier dato del titular de la tarjeta que el comerciante pueda conservar está impreso (por ejemplo, informes o recibos impresos), y estos documentos no se reciben electrónicamente.

Para obtener una guía gráfica para elegir su tipo de SAQ, consulte "¿Cuál SAQ Se Aplica Mejor a Mi Entorno?" en las páginas 25 y 26.

SAQ B-IP – Comerciantes con dispositivos PTS POI Independientes, Aprobados e incluidos en la lista PCI, sin Almacenamiento Electrónico de los Datos del Titular de la Tarjeta

El SAQ B-IP sólo incluye aquellos Requisitos de PCI DSS aplicables a los comerciantes que procesan los datos del titular de la tarjeta únicamente a través de dispositivos de punto de interacción (POI) autónomos y aprobados por[1] PCI PIN Transaction Security (PTS) con una conexión IP al procesador de pagos.

Para obtener una guía gráfica para elegir su tipo de SAQ, consulte "¿Cuál SAQ Se Aplica Mejor a Mi Entorno?" en las páginas 25 y 26.

Se aplica una excepción para los dispositivos PTS POI clasificados como Lectores de Tarjetas Seguros (SCR) y Lectores de Tarjetas Seguros para PIN (SCRP); los comerciantes que utilizan SCR o SCRP no son elegibles para este SAQ.

Los comerciantes SAQ B-IP pueden ser comerciantes de tiendas físicas (con tarjeta) o de pedidos por correo o teléfono (sin tarjeta) y no almacenan datos del titular de la tarjeta en ningún sistema informático.

Este SAQ no es aplicable a los canales de comercio electrónico.

Este SAQ no aplica para los proveedores de servicios.

Los comercios SAQ B-IP confirmarán que cumplen con los siguientes criterios de elegibilidad para este canal de pago:

- El comerciante sólo utiliza dispositivos PTS POI autónomos y aprobados por PCI[1] Los dispositivos PTS POI (excluidos los SCR y los SCRP) conectados vía IP al procesador de pagos del comerciante para tomar la información de las tarjetas de pago de los tarjetahabientes;
- Los dispositivos POI autónomos, conectados por IP, están validados para el programa PTS POI, tal como aparece en el sitio web de PCI SSC (excluye los SCR y los SCRP);
- Los dispositivos PTS POI autónomos y conectados por IP no están conectados a ningún otro sistema dentro del entorno del comerciante (esto puede lograrse mediante la segmentación de la red para aislar los dispositivos PTS POI de otros sistemas)[2];
- La única transmisión de los datos del titular de la tarjeta se realiza desde los dispositivos PTS POI aprobados al procesador de pagos;
- El dispositivo PTS POI no depende de ningún otro dispositivo,— por ejemplo, computadora, teléfono móvil, tableta, etc.— para conectarse al procesador de pagos;
- El comerciante no almacena datos del titular de la tarjeta en formato electrónico; y
- Cualquier datos del titular de la tarjeta que el comerciante pueda conservar está impreso (por ejemplo, informes o recibos impresos), y estos documentos no se reciben electrónicamente.

[1] Un comerciante que utilice un dispositivo PTS POI expirado deberá comprobar con su adquirente o con las marcas de pago individuales la aceptabilidad de este SAQ. Consulte la lista PCI de Dispositivos de Seguridad para Transacciones PIN con Aprobaciones Expiradas.

[2] Este criterio no pretende prohibir que haya más de un tipo de sistema permitido (es decir, dispositivos POI conectados por IP) en la misma zona de red, siempre y cuando los sistemas permitidos estén aislados de otros tipos de sistemas (por ejemplo, implementando la segmentación de la red). Además, este criterio no pretende impedir que el tipo de sistema definido pueda transmitir la información de las transacciones a un tercero para su procesamiento, como un adquirente o un procesador de pagos, a través de una red.

SAQ C-VT – Comerciantes con Soluciones de Terminales de Pago Virtuales de Terceros Basadas en la Web, sin Almacenamiento Electrónico de Datos del Titular de la Tarjeta

El SAQ C-VT sólo incluye aquellos Requisitos de PCI DSS aplicables a los comerciantes que procesan los datos del titular de la tarjeta sólo a través de soluciones de terminales de pago virtuales de terceros en un dispositivo informático aislado conectado a Internet.

El terminal de pago virtual es una solución de terceros que se utiliza para enviar transacciones de tarjetas de pago para su autorización a un sitio web de un proveedor de servicios de terceros (TPSP) que se encuentre en conformidad con PCI DSS. Mediante esta solución, el comerciante ingresa los datos del titular de la tarjeta manualmente desde un dispositivo informático aislado a través de un navegador web conectado de forma segura. A diferencia de los terminales físicos, los terminales de pago virtuales no leen los datos directamente de una tarjeta de pago.

Para obtener una guía gráfica para elegir su tipo de SAQ, consulte "Cuál SAQ se Aplica Mejor a Mi Entorno" en las páginas 25 y 26.

Esta opción SAQ está orientada para aplicarse sólo a los comerciantes que introducen manualmente una sola transacción a la vez a través de un teclado en una solución de terminal de pago virtual basada en Internet. Los comerciantes SAQ C-VT pueden ser comerciantes de tiendas físicas (con tarjeta) o de pedidos por correo o teléfono (sin tarjeta) y no almacenan datos del titular de la tarjeta en ningún sistema informático.

Este SAQ no es aplicable a los canales de comercio electrónico.

Este SAQ no aplica para los proveedores de servicios.

Los comerciantes de SAQ C-VT confirmarán que cumplen con los siguientes criterios de elegibilidad para este canal de pago:

- El único procesamiento de pagos se realiza a través de un terminal de pago virtual al que se accede mediante un navegador web conectado a Internet;
- La solución de terminal de pago virtual es suministrada y alojada por un proveedor de servicios externo que se encuentre en conformidad con PCI DSS;
- La solución de terminal de pago virtual que de conformidad con PCI DSS sólo es accesible a través de un dispositivo informático que está aislado en una única locación, y no está conectado a otras locaciones o sistemas (esto se puede conseguir mediante un firewall o segmentación de la red para aislar los sistemas del comerciante que acceden al terminal de pago virtual de otros sistemas del comerciante)[3];
- El dispositivo informático no tiene instalado ningún software que almacene datos del titular de la tarjeta (por ejemplo, no hay ningún software para el procesamiento por lotes o el almacenamiento y reenvío);

[3] Este criterio no tiene por objeto prohibir que más de un tipo de sistema permitido (es decir, navegador web conectado a Internet accediendo a una solución de terminal de pago virtual) se encuentre en la misma zona de red, siempre y cuando los sistemas permitidos estén aislados de otros tipos de sistemas (por ejemplo, mediante la implementación de una segmentación de red). Además, este criterio no tiene por objeto impedir que el tipo de sistema definido pueda transmitir información de transacciones a un tercero para su procesamiento, como un comprador o un procesador de pagos, a través de una red.

- El dispositivo informático no tiene ningún dispositivo de hardware conectado que se utilice para capturar o almacenar datos del titular de la tarjeta (por ejemplo, no hay lectores de tarjetas conectados);
- El comerciante no recibe, transmite o almacena los datos del titular de la tarjeta electrónicamente a través de ningún canal (por ejemplo, a través de una red interna o de Internet); y
- Cualquier dato del titular de la tarjeta que el comerciante pueda conservar está en papel (por ejemplo, informes o recibos impresos), y esos documentos no se reciben electrónicamente.

SAQ C – Comerciantes con Sistemas de Aplicaciones de Pago Conectados a Internet, Sin Almacenamiento Electrónico de Datos del Titular de la Tarjeta

El SAQ C sólo incluye aquellos Requisitos de PCI DSS aplicables a las empresas que cuentan con sistemas de aplicaciones de pago (por ejemplo, sistemas de puntos de venta) conectados a Internet, y que no almacenan datos del titular de la tarjeta electrónicos.

Las empresas SAQ C procesan los datos del titular de la tarjeta a través del sistema de punto de venta (POS por sus siglas en inglés) u otros sistemas de aplicación de pagos conectados a Internet, no almacenan los datos del titular de la tarjeta en ningún sistema informático y pueden ser tiendas físicas (presencial con tarjeta) o de pedidos por correo o teléfono (virtual sin tarjeta).

Para obtener una guía gráfica para elegir su tipo de SAQ, consulte "¿Cuál SAQ Se Aplica Mejor a Mi Entorno?" en las páginas 25 y 26.

Este SAQ no es aplicable a los canales de comercio electrónico.

Este SAQ no aplica para los proveedores de servicios.

Los comerciantes del SAQ C confirmarán que cumplen los siguientes criterios de elegibilidad para este canal de pago:

- El comerciante tiene un sistema de aplicación de pago y una conexión a Internet en el mismo dispositivo y/o en la misma red de área local (LAN);
- El sistema de aplicación de pagos no está conectado a ningún otro sistema dentro del entorno del comerciante (esto puede lograrse mediante la segmentación de la red para aislar el sistema de la aplicación de pago/dispositivo de Internet de todos los demás sistemas);
- La ubicación física del entorno del entorno POS no está conectada a otros locales o ubicaciones, y cualquier LAN es sólo para una tienda;
- El comerciante no almacena datos del titular de la tarjeta en formato electrónico; y
- Cualquier dato del titular de la tarjeta que el comerciante pueda conservar está en impreso (por ejemplo, informes o recibos impresos), y esos documentos no se reciben electrónicamente.

SAQ P2PE – Comerciantes que utilizan únicamente Terminales de Pago en una Solución P2PE de la lista PCI, Sin Almacenamiento Electrónico de Datos del Titular de la Tarjeta

El SAQ P2PE sólo incluye aquellos requisitos de PCI DSS aplicables a los comerciantes que procesan datos del titular de la tarjeta únicamente a través de soluciones [4] P2PE respaldadas por PCI. Los comerciantes de SAQ P2PE no tienen acceso a los datos del titular de la tarjeta en texto claro en ningún sistema informático, y sólo introducen los datos del titular de la tarjeta a través de los terminales de pago desde una solución P2PE validada[4] que figure en la lista PCI.

Los comerciantes SAQ P2PE pueden ser comerciantes de tiendas físicas (con tarjeta) o de pedidos por correo o teléfono (sin tarjeta). Por ejemplo, un comerciante de pedidos por correo o teléfono podría ser elegible para el SAQ P2PE si recibe datos del titular de la tarjeta en papel o por teléfono, y los introduce directamente y sólo en el terminal de pago desde una solución P2PE validada[4] que figure en la lista PCI.

Para obtener una guía gráfica para elegir su tipo de SAQ, consulte "¿Cuál SAQ Se Aplica Mejor a Mi Entorno?" en las páginas 25 y 26.

Este SAQ no es aplicable a los canales de comercio electrónico.

Este SAQ no aplica para los proveedores de servicios.

Los comercios SAQ P2PE confirmarán que cumplen con los siguientes criterios de elegibilidad para este canal de pago:

- Todo el procesamiento de pagos se realiza a través de una solución validada[4] solución P2PE de la lista PCI;
- Los únicos sistemas del entorno del comerciante que almacenan, procesan o transmiten datos del titular de la tarjeta son los terminales de pago de una solución P2PE[4] de la lista PCI validada;
- El comerciante no recibe, transmite ni almacena datos del titular de la tarjeta medios electrónicos;
- Cualquier dato del titular de la tarjeta que el comerciante pueda conservar está impreso (por ejemplo, informes o recibos impresos), y estos documentos no se reciben electrónicamente.
- El comerciante ha implementado todos los controles del *Manual de Instrucciones P2PE (PIM)* suministrado por el Proveedor de Soluciones P2PE.

[4] Las soluciones P2PE en la lista PCI de Soluciones Punto a Punto con Validaciones Expiradas ya no se consideran "validadas" según la Guía del Programa P2PE. Un comerciante que utilice una solución P2PEd expirada deberá comprobar con su adquirente o con las marcas de pago individuales la aceptabilidad de este SAQ.

SAQ SPoC – Comerciantes que Utilizan únicamente un Dispositivo SCRP PTS Aprobado de la lista PCI y un Dispositivo COTS como Parte de una Solución SPoC de la Lista PCI Validada

El SAQ SPoC incluye solo aquellos requisitos PCI DSS aplicables a los comerciantes que procesan datos del titular de la tarjeta a través de un dispositivo Lector de Tarjetas Seguro de PIN (SCRP) y un dispositivo móvil de productos comerciales disponibles (COTS) que lo acompaña (por ejemplo, un teléfono o una tableta), como parte de una Solución SPoC validada por PCI SCC para la Entrada de PIN basada en Software en sistemas COTS.

Los comerciantes de SAQ SPoC no tienen acceso a datos del titular de la tarjeta en texto claro en ningún sistema informático y solo ingresan datos del titular de la tarjeta a través de un SCRP como parte de una Solución PCI SSC SPoC validada, utilizando un dispositivo móvil COTS del comerciante. Estos dispositivos móviles COTS son dispositivos móviles de uso general; esto significa que el dispositivo móvil no tiene que ser utilizado únicamente para pagos o estar dedicado a un canal de pago.

Los comerciantes de SAQ SPoC procesan transacciones con tarjeta presencial (transacciones con chip de contacto, transacciones sin contacto y transacciones con banda magnética basadas en SCRP).

Se aplica una excepción a los comerciantes que utilizan lectores de banda magnética (MSR) que no figuran en la lista de PTS; estos comerciantes no son elegibles para este SAQ. Este SAQ puede utilizarse para los SCRP incluidos en la lista de PTS que cuentan con funcionalidad de MSR.

Este SAQ no es aplicable a transacciones con tarjeta presencial sin supervisión (por ejemplo, quioscos, autoservicio), pedidos por correo/teléfono (MOTO) o canales de comercio electrónico.

Este SAQ no es aplicable a los proveedores de servicios.

Los comerciantes de SAQ SPoC confirmarán que reúnen los siguientes criterios de elegibilidad para este canal de pago:

- Todo el procesamiento de pagos se realiza únicamente a través de un canal de pago con tarjeta presencial;
- Toda la entrada de datos de tarjetahabiente se realiza a través de un SCRP que forma parte de una solución SPoC validada, aprobada de la lista de PCI SSC;
- Los únicos sistemas en el entorno SPoC del comerciante que almacenan, procesan o transmiten datos del titular de la tarjeta son aquellos utilizados como parte de la solución SPoC[5] validada, aprobada de la lista de PCI SSC;
- El comerciante no recibe, transmite ni almacena datos del titular de la tarjeta de medios electrónicos
- Este canal de pago no está conectado a ningún otro sistema o red dentro del entorno comercial;
- Cualquier dato del titular de la tarjeta que el comerciante pueda conservar está impreso (por ejemplo, informes o recibos impresos), y estos documentos no se reciben electrónicamente; y
- El comerciante ha implementado todos los controles en la guía del usuario de SPoC proporcionada por el Proveedor de Soluciones SPoC.

[5] Las soluciones SPoC que figuran en la lista PCI SSC con una Validación Expirada ya no se consideran “validada” según la Guía del Programa SPoC. Un comerciante que utilice una solución SPoC expirada deberá comprobar con su adquirente o con las marcas de pago individuales la aceptabilidad de este SAQ.

SAQ D para Comerciantes – Todos los Demás Comerciantes Elegibles para el SAQ

El SAQ D para Comerciantes se aplica a los comerciantes que son elegibles para completar un cuestionario de autoevaluación pero que no reúnen los criterios de ningún otro tipo de SAQ. Ejemplos de entornos comerciales a los que se puede aplicar el SAQ D incluyen, entre otros:

- Comerciantes de comercio electrónico que aceptan datos del titular de la tarjeta en su sitio web;
- Comerciantes que almacenan electrónicamente los datos del titular de la tarjeta;
- Comerciantes que no almacenan datos del titular de la tarjeta electrónicamente pero que no cumplen con los criterios de otro tipo de SAQ;
- Comerciantes con entornos que podrían cumplir los criterios de otro tipo de SAQ, pero que tienen requisitos adicionales PCI DSS aplicables a su entorno.

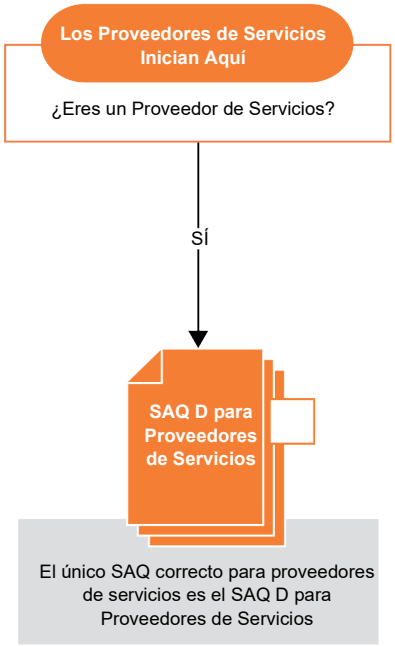
SAQ D para Proveedores de Servicios – Proveedores de Servicios Elegibles para el SAQ

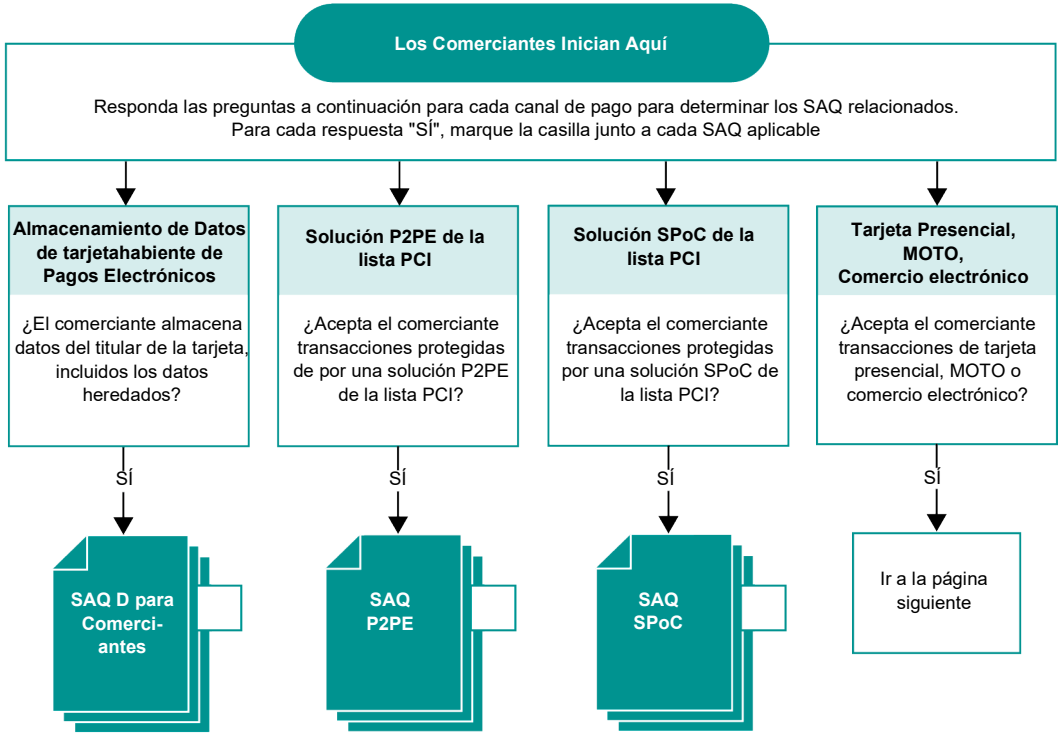
El SAQ D para proveedores de servicios se aplica a todos los proveedores de servicios definidos por una marca de pago como elegibles para completar un cuestionario de autoevaluación.

Tenga en cuenta que, para PCI DSS v4.0, el SAQ D para proveedores de servicios ahora requiere documentación adicional en la Sección 2a y especifica que los proveedores de servicios "Describen los Resultados" para cada requisito de PCI DSS.

Para obtener una guía gráfica para elegir su tipo de SAQ, consulte "¿Cuál SAQ Se Aplica Mejor a Mi Entorno?" en las páginas 25 y 26.

¿Qué SAQ se Aplica Mejor a Mi Entorno?

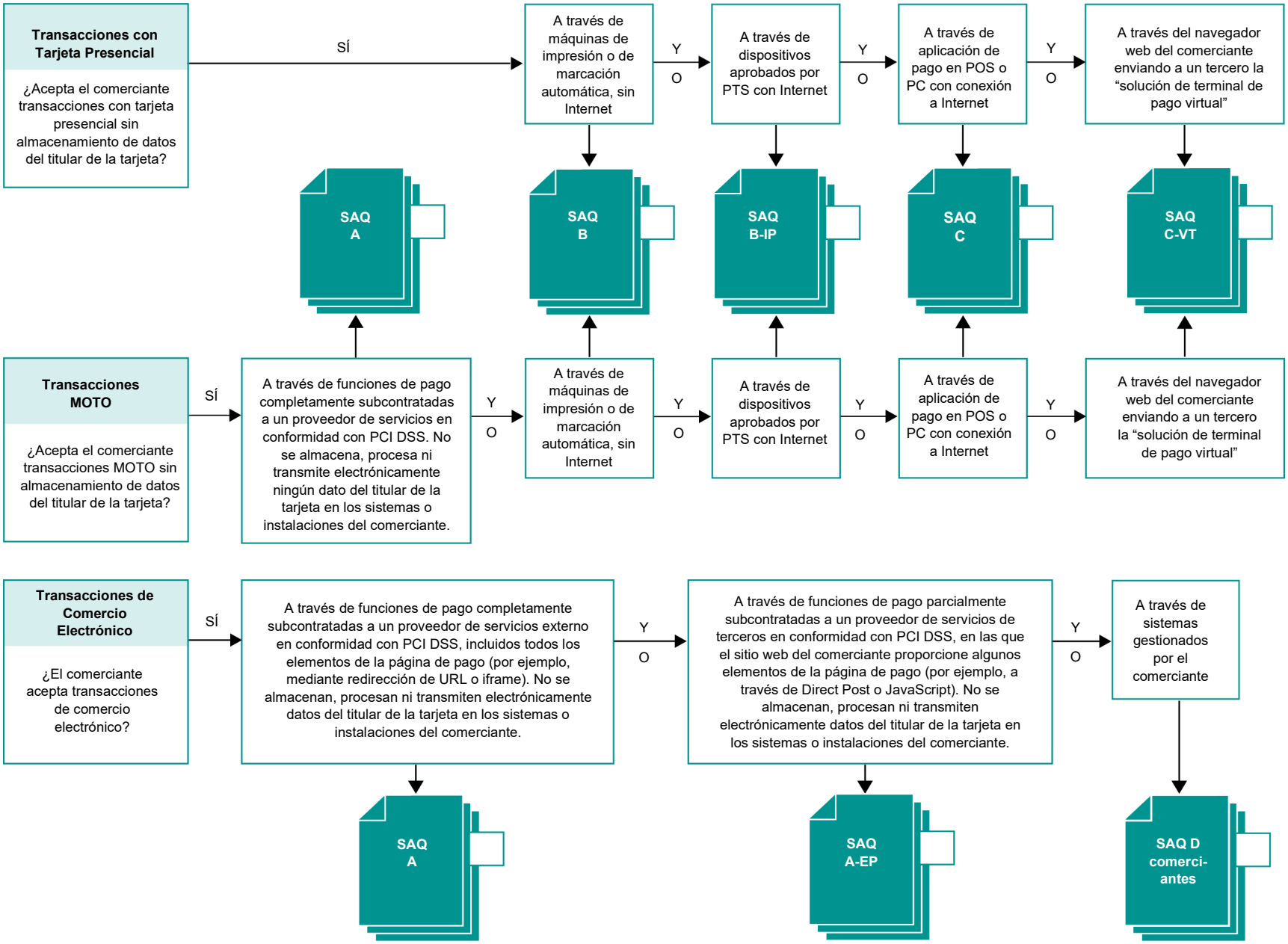




✔ Los comerciantes con más de un canal de pago deben consultar con las entidades que aceptan su conformidad (por ejemplo, las marcas de pago y las entidades adquirentes) acerca de los requisitos de validación e informe.

Y

✔ Los comerciantes deben cumplir todos los criterios de elegibilidad para cualquier SAQ aplicable



Anexo A: Cómo Cambiaron los SAQ para PCI DSS v4.x

El siguiente es un resumen de los cambios generales realizados en todos los SAQ en la transición de v3.2.1 a v4.x.

- Se agregó una tabla "Definición de Datos del Titular de la Tarjeta, Datos del Titular de la Tarjeta y Datos de Autenticación Sensibles" desde PCI DSS v4.x para definir los diversos términos utilizados en PCI DSS.
- Se agregó una tabla de “Respuestas de Presentación de Informes” para describir el significado de cada respuesta de presentación de informes que las entidades seleccionan para cada requisito PCI DSS al completar un SAQ.
- Los requisitos de cada SAQ se han actualizado para reflejar los cambios realizados en PCI DSS v4.x y para alinearse más estrechamente con otros documentos PCI DSS v4.x. Por ejemplo:
  - La redacción de cada requisito de PCI DSS ahora refleja la redacción de PCI DSS v4.x, en lugar de expresarse en forma de preguntas.
  - Algunos requisitos complejos se dividieron en subrequisitos y otros requisitos se aclararon.
  - Las respuestas de presentación de informes para cada requisito PCI DSS se actualizaron para alinearlas con el lenguaje de la Plantilla del Informe de Conformidad (ROC) PCI DSS v4.x - por ejemplo, "Sí" está ahora "Implementado."
  - Las secciones del Certificado de Conformidad (AOC) se actualizaron para alinearlas con la redacción y el contenido de los AOC del ROC.
- Para algunos de los requisitos más complicados, se añadieron explicaciones[6] para ayudar a los comerciantes a entender cómo evaluar ese requisito en el contexto de un SAQ determinado.
- Se añadieron nuevos anexos para llenar la información adicional sobre las respuestas de presentación de informes específicas.

Además de los cambios descritos anteriormente, el SAQ D para Proveedores de Servicios exige ahora la documentación adicional en la Sección 2a y especifica que los proveedores de servicios "Describan los Resultados" para cada requisito PCI DSS.

[6] Excepto el SAQ D para comerciantes y el SAQ D para Proveedores de Servicios.