
# Industria de Tarjetas de Pago (PCI)
# Norma de Seguridad de Datos
# Cuestionario de autoevaluación

## Instrucciones y directrices

**Versión 3.2.1**

Junio de 2018

## 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 la PCI DSS y aplicar los cambios menores observados desde la versión 1.1 original. |
| 28 de octubre de 2010 | 2.0 | Alinear el contenido con la nueva versión 2.0 de la PCI DSS y aclarar los tipos de entorno y los criterios de elegibilidad para el SAQ.<br>Incorporar SAQ C-VT para comerciantes de terminales virtuales basados en la web. |
| Junio de 2012 | 2.1 | Incorporar SAQ P2PE-HW para los comerciantes que procesan los datos del titular de la tarjeta solo a través de terminales de pago de hardware incluidos en una solución de cifrado punto a punto (P2PE) validada y aceptada por el PCI SSC.<br>Este documento debe usarse con la versión 2.0 de la PCI DSS. |
| Abril de 2015 | 3.1 | Alinear el contenido con la versión 3.1 de la PCI DSS, incluida la incorporación de los SAQ A-EP y B-IP, y aclarar los criterios de elegibilidad para los SAQ actuales. |
| Mayo de 2016 | 3.2 | Actualizada para alinearla con la versión 3.2 de la PCI DSS y aclarar los criterios de elegibilidad para los SAQ actuales. |
| Junio de 2018 | 3.2.1 | Actualizaciones menores para alinearse con la versión 3.2.1 de la PCI DSS. |

*DECLARACIONES: La versión en inglés del texto en este documento tal y como se encuentra en el sitio web de PCI SSC deberá considerar se, 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.*

# Índice

## Acerca de este documento

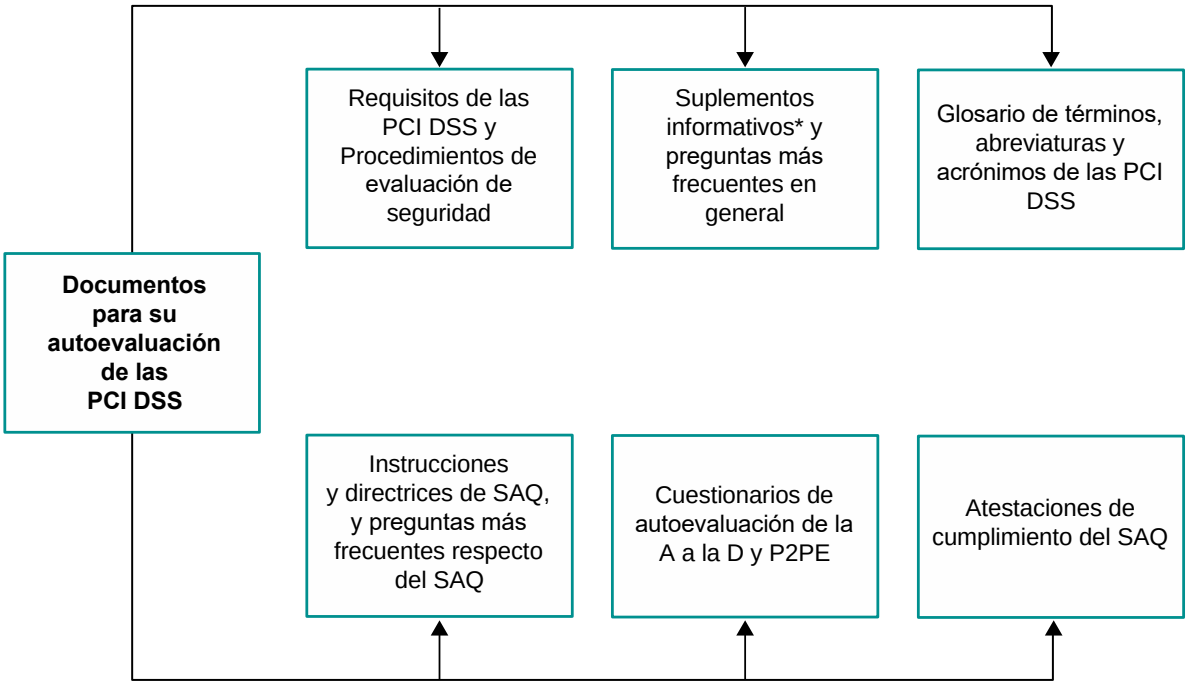
Este documento se elaboró para ayudar a los comerciantes y proveedores de servicios a entender los cuestionarios de autoevaluación (SAQ) de la norma de seguridad de datos de la industria de tarjetas de pago (PCI DSS). Para entender por qué la PCI DSS es importante para su empresa, qué estrategias puede utilizar su empresa para facilitar la validación del cumplimiento de la PCI DSS y si su empresa es elegible para completar uno de los SAQ más cortos, le recomendamos que lea este documento Instrucciones y directrices en su totalidad.

## Autoevaluación de la PCI DSS: Cómo se ajusta todo

La PCI DSS y los documentos de referencia representan un conjunto común de herramientas de la industria para ayudar a garantizar el manejo seguro de los datos del titular de la tarjeta. La norma en sí proporciona un marco procesal para desarrollar un sólido proceso de seguridad, que incluye prevenir y detectar los incidentes de seguridad, así como responder a estos. Para reducir el riesgo de compromiso y mitigar el impacto en caso de que ocurra, es importante que todas las entidades que almacenan procesos o transmiten datos del titular de la tarjeta cumplan con las normas.

En el cuadro que figura a continuación se describen las herramientas para ayudar a las empresas en el cumplimiento y la autoevaluación de la PCI DSS.

Estos y otros documentos complementarios pueden encontrarse en www.pcisecuritystandards.org.




** Cabe mencionar que los Suplementos informativos solo contienen información complementaria y la guía, pero no reemplazan ni sustituyen los requisitos de las PCI DSS.*

* ***Nota:*** *Los suplementos de información proporcionan solo información complementaria y orientación, y no sustituyen ni reemplazan ningún requisito de la PCI DSS.*

## Información general del SAQ

Los *cuestionarios de autoevaluación (SAQ) de la PCI DSS* son herramientas de validación destinadas a ayudar a los comerciantes y proveedores de servicios a autoevaluar su cumplimiento de la PCI DSS. Existen varias versiones de los SAQ de la PCI DSS para satisfacer diversos escenarios. Este documento se elaboró para ayudar a su empresa a determinar qué SAQ se adapta mejor a su entorno.

El SAQ de la PCI DSS es una herramienta de validación para los comerciantes y proveedores de servicios a los que sus respectivos adquirentes o marcas de pago no les exigen que presenten un informe de cumplimiento (ROC) de la PCI DSS. Consulte a su adquirente o marca de pago para obtener más información sobre los requisitos de validación de la PCI DSS.

Cada SAQ de la PCI DSS consta de los siguientes componentes:

1. Preguntas relacionadas con los requisitos de la PCI DSS, según corresponda para los diferentes entornos: consulte “Cómo seleccionar el SAQ y la atestación que mejor se adapten a su empresa” en este documento. Esta sección también incluye una columna para “Pruebas esperadas” que se basa en los procedimientos de prueba de la PCI DSS.
2. Atestación de cumplimiento: la Atestación incluye su declaración de elegibilidad para completar el SAQ aplicable y los subsiguientes resultados de una autoevaluación de la PCI DSS.

## Por qué es importante la PCI DSS

Los miembros fundadores de PCI Security Standards Council (American Express, Discover, JCB, Mastercard y Visa) supervisan continuamente los casos en que los datos de las cuentas están en riesgo. Estos riesgos incluyen todo el espectro de empresas, desde las más pequeñas hasta las más grandes y proveedores de servicios.

Una vulneración a la seguridad y el consiguiente riesgo de los datos de las tarjetas de pago tienen consecuencias de gran alcance para las empresas afectadas, tales como:

1. Requisitos reglamentarios de notificación;
2. Pérdida de reputación;
3. Pérdida de clientes;
4. Posibles responsabilidades financieras (por ejemplo, cargos y multas reglamentarias y de otro tipo);
5. Litigios.

El análisis forense de los riesgos ha demostrado que las vulnerabilidades comunes de seguridad, que se abordan con los controles de la PCI DSS, a menudo se explotan porque los controles de la PCI DSS o bien no existían o se aplicaban mal cuando se produjo el riesgo. La PCI DSS se creó, e incluye requisitos detallados, por esta misma razón para minimizar la posibilidad de riesgo y los efectos en caso de que se produzca.

Entre los ejemplos de fallas comunes en el control de la PCI DSS, se encuentran:

- Almacenamiento de datos confidenciales de autenticación (SAD), como datos de la pista, después de la autorización (requisito 3.2). Muchas entidades en riesgo desconocían que sus sistemas almacenaban estos datos.
- Los controles de acceso son inadecuados debido a sistemas de punto de venta (POS) mal instalados, que permiten la entrada de usuarios malintencionados por vías destinadas a proveedores de POS (requisitos 7.1, 7.2, 8.2 y 8.3).
- La configuración del sistema y las contraseñas predeterminadas no se modificaron cuando se instaló el sistema (requisito 2.1).
- Los servicios innecesarios y no seguros no se eliminaron o protegieron cuando se instaló el sistema (requisitos 2.2.2 y 2.2.3).
- Las aplicaciones web están mal codificadas y dan lugar a la inyección SQL y otras vulnerabilidades, que permiten el acceso a la base de datos que guarda los datos del titular de la tarjeta directamente desde el sitio web (requisito 6.5).
- Faltan parches de seguridad y están desactualizados (requisito 6.2).
- Faltan registros (requisito 10).
- Falta supervisión (mediante revisiones de los registros, detección/prevención de intrusos, análisis trimestrales de vulnerabilidades y mecanismos de detección de cambios) (requisitos 10.6, 11.2, 11.4 y 11.5).

- El alcance de las decisiones es deficiente; por ejemplo, la exclusión de parte de la red del alcance de la PCI DSS debido a una segmentación inadecuada de la red que no se ha comprobado que sea eficaz (requisito 11.3.4). Ello da lugar a que el entorno de datos del titular de la tarjeta quede expuesto, sin saberlo, a deficiencias en otras partes de la red que no se han protegido de acuerdo con la PCI DSS (por ejemplo, por puntos de acceso inalámbrico no protegidos y vulnerabilidades introducidas por el correo electrónico y la navegación web de los empleados) (requisitos 1.2, 1.3 y 1.4).

## Cuál es la diferencia entre cumplimiento y seguridad

Es importante reconocer la diferencia entre cumplimiento y seguridad. Cumplir con la PCI DSS en un momento dado no evita que las cosas cambien en su entorno, lo cual, si no se implementan los controles adecuados, podría afectar su seguridad. Por lo tanto, debe asegurarse de que los controles de la PCI DSS se sigan aplicando correctamente como parte de las actividades habituales (BAU) y según lo definido por su estrategia de seguridad general. Esto le permitirá supervisar la eficacia de los controles de seguridad de su empresa de forma continua y mantener su entorno de conformidad con la PCI DSS entre las evaluaciones de la PCI DSS. En la sección “Prácticas recomendadas para implementar las PCI DSS en los procesos habituales”, se ofrecen ejemplos de cómo debe incorporarse la PCI DSS a las actividades BAU.

Además, los requisitos de seguridad de la PCI DSS están destinados a la protección de los datos de tarjetas de pago, y su empresa puede tener otros datos y activos confidenciales que necesitan protección y que podrían estar fuera del ámbito de la PCI DSS. Por lo tanto, aunque el cumplimiento de la PCI DSS, si se mantiene adecuadamente, puede contribuir sin duda a la seguridad general, no debe considerarse como un sustituto de un sólido programa de seguridad para toda la empresa.

## Consejos y estrategias generales para el cumplimiento de la PCI DSS

A continuación, se presentan algunos consejos y estrategias generales para comenzar con sus iniciativas de cumplimiento de la PCI DSS. Estas recomendaciones pueden ayudarle a eliminar el almacenamiento de datos del titular de la tarjeta que no necesita, y aislar los datos que sí necesita en áreas centralizadas definidas y controladas, y pueden permitirle limitar el alcance de su esfuerzo de validación del cumplimiento de la PCI DSS. Por ejemplo, al eliminar los datos del titular de la tarjeta que no necesita y/o aislar los datos que sí necesita en áreas definidas y controladas, puede eliminar del alcance de su autoevaluación los sistemas y redes que no almacenan, procesan o transmiten datos del titular de la tarjeta, y que no se conectan a los sistemas que sí lo hacen.

1. **Datos confidenciales de autenticación (incluye el contenido completo de la pista de la banda magnética o datos equivalentes en un chip, los códigos y valores de verificación de la tarjeta, los PIN y los bloqueos de PIN):**

   Asegúrese de ***no almacenar nunca estos datos*** después de la autorización:

2. **Consulte con su proveedor POS cuál es la seguridad de su sistema mediante las siguientes preguntas sugeridas:**

   a. ¿Se han cambiado las configuraciones y contraseñas predeterminadas en los sistemas y bases de datos que forman parte del sistema POS?

   b. ¿Tiene acceso a mi sistema POS de forma remota? En caso afirmativo, ¿ha implementado los controles adecuados para evitar que otras personas accedan a mi sistema de POS, como por ejemplo utilizar métodos de acceso remoto seguro y no utilizar contraseñas comunes o predeterminadas? ¿Con qué frecuencia accede a mi dispositivo POS de forma remota y por qué? ¿Quién está autorizado a acceder a mi dispositivo POS de forma remota?

   c. ¿Se han eliminado todos los servicios innecesarios y no seguros de los sistemas y bases de datos que forman parte del sistema POS?

   d. ¿Mi software de POS está validado de acuerdo con la Norma de Seguridad de Datos para las Aplicaciones de Pago (PA-DSS)? (Consulte la lista de solicitudes de pago validadas de la PCI SSC.)

e. ¿Mi software de POS almacena datos confidenciales de autenticación, como datos de seguimiento o bloqueos de PIN? Si es así, este almacenamiento está prohibido: ¿qué tan pronto puede ayudarme a eliminarlo?

f. ¿Mi software de POS almacena números de cuenta principales (PAN)? Si es así, este almacenamiento debe estar protegido: ¿cómo protege el POS estos datos?

g. ¿Documentará la lista de archivos redactada por la aplicación con un resumen del contenido de cada archivo para verificar que no se almacenen los datos prohibidos mencionados anteriormente?

h. ¿Mi software de POS impone contraseñas complejas y únicas para todos los accesos de usuarios?

i. ¿Puede confirmar que no utiliza contraseñas comunes o predeterminadas para el acceso a mi sistema y a otros sistemas comerciales que usted mantiene?

j. ¿Todos los sistemas y bases de datos que forman parte del sistema POS se han corregido con todas las actualizaciones de seguridad aplicables?

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

l. Si las versiones anteriores de mi software de POS almacenaban datos confidenciales de autenticación, ¿se ha eliminado esta función durante las actualizaciones actuales del software de POS? ¿Se ha utilizado una limpieza segura para eliminar estos datos?

**3. Datos del titular de la tarjeta: si no los necesita, no los guarde.**

a. Las reglas de marcas de pago permiten el almacenamiento de los números de cuenta principales (PAN), la fecha de vencimiento, el nombre del titular de la tarjeta y el código de servicio.

b. Haga un inventario de todos los motivos y lugares donde almacena estos datos. Si los datos no sirven para un propósito comercial legítimo, considere eliminarlos.

c. Piense si el almacenamiento de esos datos y el proceso comercial que respaldan justifica lo siguiente:

   i. El riesgo de comprometer los datos.

   ii. Los controles adicionales de la PCI DSS que deben aplicarse para proteger dichos datos.

   iii. Los esfuerzos actuales para mantener el cumplimiento de la PCI DSS a lo largo del tiempo.

**4. Datos del titular de la tarjeta; si los necesita, debe consolidarlos y aislarlos.**

Puede limitar el alcance de una evaluación de PCI DSS consolidando el almacenamiento de datos en un entorno definido y aislando los datos mediante el uso de una adecuada segmentación de la red. Por ejemplo, si sus empleados navegan por Internet y reciben un correo electrónico en la misma máquina o segmento de red que los datos del titular de la tarjeta, considere la posibilidad de segmentar (aislar) estos datos en su propia máquina o segmento de red (por ejemplo, mediante routers o firewalls). Si puede aislarlos de manera eficaz, es posible que pueda centrar sus esfuerzos de PCI DSS solo en la parte aislada en lugar de incluir todas sus máquinas.

## 5. Controles de compensación

Se puede considerar la posibilidad de establecer controles compensatorios para la mayoría de los requisitos de la PCI DSS cuando una empresa no pueda cumplir la especificación técnica de un requisito, pero haya mitigado suficientemente el riesgo asociado mediante controles alternativos. Si su organización no tiene el control exacto especificado en la PCI DSS, pero tiene otros controles que satisfacen la definición de controles de compensación de la PCI DSS (consulte "Controles de compensación" en el Apéndice B de la PCI DSS, y también en el *Glosario de términos, abreviaturas y acrónimos de la PCI DSS y PA-DSS*), su empresa debe hacer lo siguiente:

a. Seguir los procedimientos para los controles de compensación tal como se indica en el Apéndice B de la PCI DSS.

b. Para todos los requisitos que se cumplieron con la ayuda de un control de compensación, responda a la pregunta del SAQ marcando la columna "SÍ con CCW".

c. Documente cada control de compensación completando la hoja de trabajo respectiva en el Apéndice B del SAQ.

   Se debe completar una hoja de trabajo de controles de compensación para cada requisito que se cumpla con un control de compensación.

d. Presente todas las hojas de trabajo de controles de compensación completadas, junto con su SAQ y/o la atestación de cumplimiento completada, de acuerdo con las instrucciones de su adquirente o marca de pago.

## 6. Asistencia y capacitación profesional

a. Si desea contratar a un profesional de seguridad para que le ayude con su autoevaluación, le sugerimos que considere la posibilidad de ponerse en contacto con un Asesor de Seguridad Certificado (QSA), quien se ha sometido a capacitaciones del PCI SSC para llevar a cabo evaluaciones del PCI DSS y figura en el sitio web de la PCI SSC.

b. El sitio web de la PCI SSC es una fuente primaria para recursos adicionales, tales como:

   - El *glosario de términos, abreviaturas y acrónimos de la PCI DSS*
   - Preguntas frecuentes (FAQ)
   - Seminarios web
   - Suplementos informativos y directrices
   - Formularios de SAQ y atestaciones de cumplimiento

c. La PCI SSC también proporciona varios programas de capacitación para ayudar a crear conciencia en el personal de una empresa. Algunos ejemplos incluyen Concientización de PCI, y los programas Profesional PCI (PCIP) y Asesor de seguridad interna (ISA).

   Consulte www.pcisecuritystandards.org para obtener más información.

d. Los programas y recursos de capacitación relacionados con el pago también pueden estar disponibles con las marcas de pago y/o el adquirente del comerciante.

***Nota:*** *Los suplementos de información complementan la PCI DSS e identifican consideraciones y recomendaciones adicionales para cumplir los requisitos de la PCI DSS; no cambian, eliminan ni sustituyen la PCI DSS ni ninguno de sus requisitos.*

## Cómo seleccionar el SAQ y el certificado que mejor se adapten a su empresa

Todos los comerciantes y proveedores de servicios deben cumplir con la PCI DSS aplicable a sus entornos en todo momento. Hay varios tipos de SAQ, que se muestran brevemente 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 empresa, y luego lea las descripciones detalladas para asegurarse de que cumple con todos los requisitos para dicho SAQ.

***Nota para todos los SAQ excepto para el SAQ D:*** Estos SAQ incluyen preguntas que se aplican a un tipo específico de entorno comercial, según se define en los criterios de elegibilidad del SAQ correspondiente. Si existen requisitos de la PCI DSS aplicables a su entorno que no están cubiertos en un determinado SAQ, puede ser un indicador de que este SAQ no es adecuado para su entorno. Además, debe satisfacer todos los requisitos de la PCI DSS aplicables para poder cumplir con esta.

| SAQ | Descripción |
|---|---|
| **A** | Comerciantes sin tarjeta (comercio electrónico o pedidos por correo o teléfono), que han delegado completamente todas las funciones de datos del titular de la tarjeta a proveedores de servicios de terceros que cumplen con la PCI DSS, sin almacenamiento electrónico, procesamiento o transmisión de ningún dato del titular de la tarjeta en los sistemas o locales del comerciante.<br>*No se aplica a los canales presenciales.* |
| **A-EP** | Comerciantes de comercio electrónico que subcontratan todo el procesamiento de pagos a terceros validados por la PCI DSS, y que tienen uno o más sitios web que no reciben directamente los datos del titular de la tarjeta, pero que pueden afectar la seguridad de la transacción de pago. No hay almacenamiento, procesamiento o transmisión electrónica de datos del titular de la tarjeta en los sistemas o locales del comerciante.<br>*Aplicable solo a los canales de comercio electrónico.* |
| **B** | Solo para comerciantes:<br>▪ Máquinas transcriptoras sin almacenamiento electrónico de datos del titular de la tarjeta, y/o<br>▪ Terminales independientes de acceso telefónico de salida sin almacenamiento electrónico de datos del titular de la tarjeta.<br>*No se aplica a los canales de comercio electrónico.* |
| **B-IP** | Comerciantes que utilizan solo terminales de pago independientes y aprobadas por la PTS con una conexión IP al procesador de pago sin almacenamiento electrónico de datos del titular de la tarjeta.<br>*No se aplica a los canales de comercio electrónico.* |
| **C-VT** | Comerciantes que introducen manualmente una sola transacción a la vez mediante un teclado en una solución de terminal de pago virtual basada en Internet proporcionada y alojada por un proveedor de servicios de terceros validado por la PCI DSS. Sin almacenamiento electrónico de datos del titular de la tarjeta.<br>*No se aplica a los canales de comercio electrónico.* |

| SAQ | Descripción |
|---|---|
| **C** | Comerciantes con sistemas de aplicación de pago conectados a Internet, sin almacenamiento electrónico de datos del titular de la tarjeta.<br>*No se aplica a los canales de comercio electrónico.* |
| **P2PE** | Comerciantes que utilizan únicamente terminales de pago de hardware incluidos en una solución validada de cifrado de punto a punto (P2PE) y gestionada a través de ella, sin almacenamiento electrónico de datos del titular de la tarjeta.<br>*No se aplica a los canales de comercio electrónico.* |
| **D** | ***SAQ D para los comerciantes:*** Todos los comerciantes no incluidos en las descripciones de los SAQ anteriores. |
| | ***SAQ D para los proveedores de servicios:*** Todos los proveedores de servicios definidos por una marca de pago como elegibles para completar un SAQ. |

## SAQ A: Comerciantes sin tarjeta; todas las funciones de datos del titular de la tarjeta se delegan completamente

*El SAQ A se ha elaborado para abordar los requisitos aplicables a los comerciantes cuyas funciones de datos de titulares de tarjetas se subcontratan completamente a terceros validados, en los que el comerciante solo conserva informes o recibos en papel con los datos del titular de la tarjeta.*

*Consulte "¿Qué SAQ se aplica mejor a mi entorno?" en la página 20 para obtener una guía gráfica que le permita elegir su tipo de SAQ.*

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

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

- Su empresa solo acepta transacciones sin tarjeta (comercio electrónico o pedidos por correo o por teléfono);
- Todo el procesamiento de los datos del titular de la tarjeta se subcontrata totalmente a proveedores de servicios de terceros validados por la PCI DSS;
- Su empresa no almacena, ni procesa ni transmite electrónicamente ningún dato del titular de la tarjeta en sus sistemas o locales, sino que se apoya por completo en uno o más terceros para que se encarguen de todas estas funciones;
- Su empresa ha confirmado que todos los terceros que manejan el almacenamiento, el procesamiento y/o la transmisión de los datos del titular de la tarjeta cumplen con la PCI DSS; **y**
- Cualquier dato del titular de la tarjeta que su empresa conserve está en papel (por ejemplo, informes impresos o recibos), y estos documentos no se reciben electrónicamente.

*Además, para los canales de comercio electrónico:*

- Todos los elementos de todas las páginas de pago que se entregan al navegador del consumidor proceden única y directamente de uno o más proveedores de servicios de terceros validados por la PCI DSS.

***Este SAQ no se aplica a los canales presenciales.***

## SAQ A-EP: Parcialmente subcontratado Comerciantes de comercio electrónico que utilizan un sitio web de terceros para el procesamiento de pagos.

*El SAQ A-EP se ha elaborado para abordar los requisitos aplicables a los comerciantes de comercio electrónico con uno o más sitios web que no reciben los 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 consumidor.*

Los comerciantes del SAQ A-EP son comerciantes de comercio electrónico que subcontratan parcialmente su canal de pago de comercio electrónico a terceros validados por la PCI DSS y no almacenan, ni procesan ni transmiten electrónicamente ningún dato del titular de la tarjeta en sus sistemas o locales.

*Consulte "¿Qué SAQ se aplica mejor a mi entorno?" en la página 20 para obtener una guía gráfica que le permita elegir su tipo de SAQ.*

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

- Su empresa solo acepta transacciones de comercio electrónico;
- Todo el procesamiento de los datos del titular de la tarjeta, con excepción de la página de pago, se subcontrata totalmente a un procesador de pagos de terceros validado por la PCI DSS;
- Su sitio web de comercio electrónico no recibe los datos del titular de la tarjeta, sino que controla cómo se redirigen los consumidores, o los datos del titular de la tarjeta, a un procesador de pagos de terceros validado por la PCI DSS;
- Si el sitio web del comerciante está alojado en un proveedor de terceros, el proveedor está validado de acuerdo con todos los requisitos de la PCI DSS aplicables (por ejemplo, incluyendo el Apéndice A de la PCI DSS si el proveedor es un proveedor de alojamiento compartido);
- Cada elemento de las páginas de pago que se entrega al navegador del consumidor se origina en el sitio web del comerciante o en un proveedor de servicios que cumple con la PCI DSS;
- Su empresa no almacena, ni procesa ni transmite electrónicamente ningún dato del titular de la tarjeta en sus sistemas o locales, sino que se apoya por completo en uno o más terceros para que se encarguen de todas estas funciones;
- Su empresa ha confirmado que todos los terceros que manejan el almacenamiento, el procesamiento y/o la transmisión de los datos del titular de la tarjeta cumplen con la PCI DSS; **y**
- Cualquier dato del titular de la tarjeta que su empresa conserve está en papel (por ejemplo, informes impresos o recibos), y estos documentos no se reciben electrónicamente.

***Este SAQ es aplicable a los canales de comercio electrónico.***

***Nota:*** *Para los fines del SAQ A-EP, los requisitos de la PCI DSS que se refieren al "entorno de datos del titular de la tarjeta" son aplicables a los sitios web de los comerciantes. Esto se debe a que afectan directamente la forma en que se transmiten los datos de la tarjeta de pago, aunque los sitios web en sí no reciben datos del titular de la tarjeta.*

## SAQ B: Comerciantes solo con máquinas transcriptoras o solo con terminales independientes de acceso telefónico; sin almacenamiento electrónico de datos del titular de la tarjeta

*El SAQ B se ha elaborado para abordar los requisitos aplicables a los comerciantes que procesan los datos del titular de la tarjeta solo a través de máquinas transcriptoras o terminales independientes de acceso telefónico.*

Los comerciantes del SAQ B pueden ser comerciantes físicos (con tarjeta) o comerciantes de pedidos por correo o por teléfono (sin tarjeta), y no almacenan los datos del titular de la tarjeta en ningún sistema informático. Los comerciantes del SAQ B confirmarán que cumplen con los siguientes criterios de elegibilidad para este canal de pago:

*Consulte "¿Qué SAQ se aplica mejor a mi entorno?" en la página 20 para obtener una guía gráfica que le permita elegir su tipo de SAQ.*

- Su empresa utiliza solo una máquina transcriptora y/o utiliza solo terminales independientes de acceso telefónico (conectadas a través de una línea telefónica a su procesador) para tomar la información de las tarjetas de pago de sus clientes;
- Las terminales independientes de acceso telefónico no están conectadas a ningún otro sistema de su entorno;
- Las terminales independientes de acceso telefónico no están conectadas a Internet;
- Su empresa no transmite datos del titular de la tarjeta a través de una red (ya sea una red interna o Internet);
- Cualquier dato del titular de la tarjeta que su empresa conserve está en papel (por ejemplo, informes impresos o recibos), y estos documentos no se reciben electrónicamente; **y**
- Su empresa no almacena los datos del titular de la tarjeta en formato electrónico.

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

## SAQ B-IP: Comerciantes con terminales de punto de interacción (PTS) independientes y conectadas a IP, sin almacenamiento electrónico de datos del titular de la tarjeta.

*El SAQ B-IP se ha elaborado para abordar los requisitos aplicables a los comerciantes que procesan los datos del titular de la tarjeta solo a través de dispositivos de punto de interacción (POI) independientes y aprobados por la PTS con una conexión IP al procesador de pagos.*

*Consulte "¿Qué SAQ se aplica mejor a mi entorno?" en la página 20 para obtener una guía gráfica que le permita elegir su tipo de SAQ.*

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

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

- Su empresa solo utiliza dispositivos de punto de interacción (POI) independientes y aprobados por la PTS (sin incluir los SCR) conectados vía IP a su procesador de pagos para tomar la información de las tarjetas de pago de sus clientes;
- Los dispositivos POI independientes conectados por IP son validados por el programa POI para PTS, tal como aparece en el sitio web de la PCI SSC (sin incluir los SCR);
- Los dispositivos POI independientes y conectados a IP no están conectados a ningún otro sistema dentro de su entorno (esto puede lograrse mediante la segmentación de la red para aislar los dispositivos POI de otros sistemas);
- La única transmisión de datos del titular de la tarjeta es desde los dispositivos POI aprobados por PTS al procesador de pagos;
- El dispositivo POI no depende de ningún otro dispositivo (por ejemplo, computadora, teléfono celular, tableta, etc.) para conectarse al procesador de pagos;
- Cualquier dato del titular de la tarjeta que su empresa conserve está en papel (por ejemplo, informes impresos o recibos), y estos documentos no se reciben electrónicamente; **y**
- Su empresa no almacena los datos del titular de la tarjeta en formato electrónico.

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

## SAQ C-VT: Comerciantes de terminales virtuales basados en la web; sin almacenamiento electrónico de datos del titular de la tarjeta

*El SAQ C-VT se ha elaborado para abordar los requisitos aplicables a los comerciantes que procesan los datos del titular de la tarjeta únicamente a través de terminales de pago virtuales aisladas en una computadora personal conectada a Internet.*

*Consulte "¿Qué SAQ se aplica mejor a mi entorno?" en la página 20 para obtener una guía gráfica que le permita elegir su tipo de SAQ.*

Una terminal de pago virtual es un acceso basado en un navegador a un sitio web de un adquirente, procesador o proveedor de servicios de terceros para autorizar transacciones con tarjetas de pago, en el que el comerciante introduce manualmente los datos de la tarjeta de pago a través de un navegador web conectado de forma segura. A diferencia de las terminales físicas, las terminales de pago virtuales no leen los datos directamente de una tarjeta de pago. Las transacciones con tarjetas de pago se introducen manualmente.

Los comerciantes del SAQ C-VT procesan los datos del titular de la tarjeta únicamente a través de una terminal de pago virtual y no almacenan estos en ningún sistema informático. Estas terminales virtuales se conectan a Internet para acceder a un tercero que alberga la función de procesamiento de pago de la terminal virtual. Este tercero puede ser un procesador, adquirente u otro proveedor de servicios de terceros que almacena, procesa y/o transmite datos del titular de la tarjeta para autorizar y/o liquidar las transacciones de pago con terminal virtual de los comerciantes.

Esta opción de SAQ tiene por objeto aplicarse únicamente a los comerciantes que introducen manualmente una sola transacción a la vez mediante un teclado en una solución de terminal virtual basada en Internet. Los comerciantes del SAQ C-VT pueden ser comerciantes físicos (con tarjeta) o comerciantes de pedidos por correo o por teléfono (sin tarjeta).

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

- El único procesamiento de pagos de su empresa es a través de una terminal de pago virtual a la que se accede mediante un navegador web conectado a Internet;
- La solución de la terminal de pago virtual de su empresa es proporcionada y alojada por un proveedor de servicios de terceros validado por la PCI DSS;
- Su empresa accede a la solución de terminal de pago virtual que cumple con la norma PCI DSS a través de una computadora que está aislada en un solo lugar, y no está conectada a otras ubicaciones o sistemas dentro de su entorno (esto puede lograrse mediante un firewall o la segmentación de la red para aislar la computadora de otros sistemas);
- La computadora de su empresa no tiene instalado ningún software que haga que se almacenen los datos del titular de la tarjeta (por ejemplo, no hay ningún software para el procesamiento por lotes o para el almacenamiento y envío);
- La computadora de su empresa no tiene instalados dispositivos de hardware que se utilicen para capturar o almacenar los datos del titular de la tarjeta (por ejemplo, no hay lectores de tarjetas conectados);
- Su empresa no recibe ni transmite electrónicamente los datos del titular de la tarjeta por ningún otro medio (por ejemplo, a través de una red interna o de Internet);

- Cualquier dato del titular de la tarjeta que su empresa conserve está en papel (por ejemplo, informes impresos o recibos), y estos documentos no se reciben electrónicamente; **y**
- Su empresa no almacena los datos del titular de la tarjeta en formato electrónico.

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

## SAQ C: Comerciantes con sistemas de aplicación de pago conectados a Internet; sin almacenamiento electrónico de datos del titular de la tarjeta

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

Los comerciantes del SAQ C procesan los datos del titular de la tarjeta a través de un sistema de punto de venta (POS) u otros sistemas de aplicación de pagos conectados a Internet, no almacenan estos datos en ningún sistema informático, y pueden ser comerciantes físicos (con tarjeta) o de pedidos por correo o por teléfono (sin tarjeta).

*Consulte "¿Qué SAQ se aplica mejor a mi entorno?" en la página 20 para obtener una guía gráfica que le permita elegir su tipo de SAQ.*

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

- Su empresa 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 pago/dispositivo de Internet no está conectado a ningún otro sistema dentro de su entorno (esto puede lograrse mediante la segmentación de la red para aislar el sistema de aplicación de pago/dispositivo de Internet de todos los demás sistemas);
- La ubicación física del entorno del punto de venta no está conectada a otros locales o lugares, y cualquier LAN es para una sola tienda;
- Cualquier dato del titular de la tarjeta que su empresa conserve está en papel (por ejemplo, informes impresos o recibos), y estos documentos no se reciben electrónicamente; **y**
- Su empresa no almacena los datos del titular de la tarjeta en formato electrónico.

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

## SAQ P2PE: Comerciantes que utilizan únicamente terminales de pago de hardware en una solución P2PE aceptada por PCI SSC, sin almacenamiento electrónico de datos del titular de la tarjeta.

*El SAQ P2PE se ha elaborado para abordar los requisitos aplicables a los comerciantes que procesan los datos del titular de la tarjeta únicamente a través de terminales de pago incluidas en una solución de cifrado punto a punto (P2PE) validada que figura en el PCI SSC.*

*Consulte "¿Qué SAQ se aplica mejor a mi entorno?" en la página 20 para obtener una guía gráfica que le permita elegir su tipo de SAQ.*

Los comerciantes del SAQ P2PE no tienen acceso a datos de cuentas de texto simple en ningún sistema informático, y solo introducen datos de cuentas a través de terminales de pago de hardware de una solución P2PE aprobada por el PCI SSC. Los comerciantes del SAQ P2PE pueden ser comerciantes físicos (con tarjeta) o comerciantes de pedidos por correo o por teléfono (sin tarjeta). Por ejemplo, un comerciante de pedidos por correo o por teléfono podría ser elegible para el SAQ P2PE si recibe los datos del titular de la tarjeta en papel o por teléfono, y los introduce directamente y solo en un dispositivo de hardware validado P2PE.

Los comerciantes del 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 P2PE de PCI validada, aprobada y registrada por el PCI SSC;
- Los únicos sistemas del entorno comercial que almacenan, procesan o transmiten datos de cuentas son los dispositivos de punto de interacción (POI) que están aprobados para su uso con la solución P2PE validada y registrada por la PCI;
- Su empresa no recibe ni transmite electrónicamente los datos del titular de la tarjeta.
- No existe un almacenamiento legado de datos del titular de la tarjeta electrónica en el entorno;
- Su empresa no almacena, ni procesa ni transmite electrónicamente ningún dato del titular de la tarjeta en sus sistemas o locales, sino que se apoya por completo en uno o más terceros para que se encarguen de todas estas funciones; y
- Su empresa ha implementado todos los controles del *Manual de Instrucciones de P2PE (PIM)* proporcionado por el Proveedor de la Solución P2PE.

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

## SAQ D para los comerciantes: Todos los demás comerciantes elegibles para el SAQ

*El SAQ D para Comerciantes se aplica a los comerciantes elegibles para el SAQ que no cumplen los criterios para cualquier otro tipo de SAQ.*

Los ejemplos de entornos comerciales que utilizarían el SAQ D pueden incluir, entre otros:

- Comerciantes de comercio electrónico que aceptan datos del titular de la tarjeta en su sitio web;
- Comerciantes con almacenamiento electrónico de datos del titular de la tarjeta;
- Comerciantes que no almacenan electrónicamente los datos del titular de la tarjeta, pero que no cumplen 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 de PCI DSS aplicables a su entorno.

## SAQ D para los 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 el SAQ.*

***Nota para el SAQ D para los comerciantes y el SAQ D para los proveedores de servicios:*** Aunque muchas empresas que completen el SAQ D tendrán que validar el cumplimiento de todos los requisitos de la PCI DSS, algunas empresas con modelos de negocio muy específicos pueden encontrarse con que algunos requisitos no son aplicables. Por ejemplo, no se esperaría que una empresa que no utiliza la tecnología inalámbrica en forma alguna validara el cumplimiento de las secciones de la PCI DSS que son específicas para la gestión de la tecnología inalámbrica. Consulte la guía específica en el SAQ D correspondiente para obtener información sobre la exclusión de otros requisitos específicos.

*Consulte "¿Qué SAQ se aplica mejor a mi entorno?" en la página 20 para obtener una guía gráfica que le permita elegir su tipo de SAQ.*

# ¿Qué SAQ se aplica mejor a mi entorno?