RECURSOS DE PROTECCIÓN DE PAGOS PARA PEQUEÑOS COMERCIANTES

Preguntas para Hacerles a sus proveedores

VERSIÓN 1.0 | JUNIO DE 2016

PCI Security Standards Council®

Introducción

Este documento ha sido diseñado para ayudar a los operadores y propietarios de pequeños comercios. El fin de brindarle preguntas para que les haga sus proveedores y proveedores de servicios es ayudarle a comprender cómo esas entidades respaldan la protección de los datos de la tarjeta de sus clientes.

Preguntas para hacerles a sus proveedores se creó como un complemento de la *Guía de pagos seguros*, que forma parte de los Recursos de protección de pagos para pequeños comerciantes. Consulte la *Guía de pagos seguros* y los otros Recursos de protección de pagos para pequeños comerciantes en los siguientes sitios:

RECURSO	URL
Guía de pagos seguros	https://es.pcisecuritystandards.org/pdfs/Small_Merchant_Guide_to_Safe_Payments.pdf
Sistemas de pago comunes	https://es.pcisecuritystandards.org/pdfs/Small_Merchant_Common_Payment_Systems.pdf
Glosario de términos sobre pagos y seguridad de la información	https://es.pcisecuritystandards.org/pdfs/Small_Merchant_Glossary_of_Payment_and_Information_Security_Terms.pdf

Proveedores y proveedores de servicios y cómo funcionan

Quizá los pequeños comerciantes/las pequeñas empresas pueden entrar en contacto con una cantidad de proveedores o proveedores de servicios y es importante que los comerciantes comprendan el tipo de proveedor con el que están trabajando y asegurarse de que el proveedor haya tomado las medidas necesarias para proteger los datos de la tarjeta.

La tabla de la página 2 describe los tipos más comunes de proveedores de pago y proveedores de servicios y qué deberían buscar los comerciantes con cada proveedor.

La tabla que comienza en la página 3 les brinda a los comerciantes preguntas que pueden hacerles a sus proveedores o proveedores de servicios para ayudarles a comprender cuál es la función del proveedor o proveedor de servicios en cuanto a la protección de datos de la tarjeta.

Proveedores y proveedores de servicios

La siguiente tabla describe los tipos más comunes de proveedores de pago y proveedores de servicios y qué deberían buscar los comerciantes con cada proveedor.

TIPO DE PROVEEDOR/ PROVEEDOR DE SERVICIOS	FUNCIÓN	PROGRAMA O NORMA DE LA PCI	BUSCAR:
Proveedor de la aplicación de pago	Vender y respaldar aplicaciones que guarden, procesen y/o transmitan los datos del titular de la tarjeta.	Norma de seguridad de datos para las aplicaciones de pago (PA DSS):	La aplicación está en la List of PCI PA-DSS of Validated Payment Applications (Lista de aplicaciones de pago validadas según la PA-DSS de la PCI).
Proveedor de terminal de pago	Vender y respaldar dispositivos que se utilizan para aceptar pagos con tarjetas (p. ej.: terminal de pago).	Seguridad de la transacción con PIN (PTS)	El terminal de pago se encuentra en la PCI Council's Approved PTS Devices (Lista de dispositivos PTS aprobados de la PCI).
Procesadores de pago, procesadores/proveedores de hosting de comercio electrónico	Guardar, procesar o transmitir datos del titular de la tarjeta en su nombre. Además, puede alojar su sitio web o servidor de comercio electrónico en un hosting o administrarlos, y/o desarrollar y dar soporte a su sitio web.	Norma de seguridad de datos de la PCI (PCI DSS)	Solicite la Declaración de cumplimiento de la PCI DSS y pregunte si la evaluación de este incluye el servicio que usted está utilizando. El proveedor de servicios se encuentra en una de estas listas: MasterCard's List of Compliant Service Providers (Lista de proveedores de servicios que cumplen con los requisitos de Mastercard) Visa's Global Registry of Service Providers (Registro mundial de proveedores de servicios de Visa) Visa Europe's Registered Member Agents (Agentes miembros registrados de Visa Europe)
Proveedores de software como un servicio	Desarrollar, alojar en un hosting o administrar su aplicación web o aplicación de pago en la nube (p. ej.: aplicación de reservas o ventas de tickets en línea).	PCI DSS	Solicite la Declaración de cumplimiento de la PCI DSS y pregunte si la evaluación de este incluye el servicio que usted está utilizando. El proveedor de servicios se encuentra en una de estas listas: MasterCard's List of Compliant Service Providers (Lista de proveedores de servicios que cumplen con los requisitos de Mastercard) Visa's Global Registry of Service Providers (Registro mundial de proveedores de servicios de Visa) Visa Europe's Registered Member Agents (Agentes miembros registrados de Visa Europe)
Integradores/revendedores	Instalar las aplicaciones de pago validadas por la PA-DSS en su nombre.	Integradores y revendedores calificados (QIR)	Preguntar si el proveedor es un integrador o revendedor calificado (QIR) de la PCI. El proveedor está en la List of PCI QIRs (Lista de QIR de la PCI).
Proveedores de servicios que cumplen con los requisitos de la PCI DSS	Administrar/operar sistemas o servicios en su nombre (p. ej.: administración de firewall, servicios de parches/antivirus).	PCI DSS	Solicite la Declaración de cumplimiento de la PCI DSS y pregunte si la evaluación de este incluye el servicio que usted está utilizando. El proveedor de servicios se encuentra en una de estas listas: MasterCard's List of Compliant Service Providers (Lista de proveedores de servicios que cumplen con los requisitos de Mastercard) Visa's Global Registry of Service Providers (Registro mundial de proveedores de servicios de Visa) Visa Europe's Registered Member Agents (Agentes miembros registrados de Visa Europe)

Preguntas

La siguiente tabla contiene una serie de preguntas para que los comerciantes les hagan a sus proveedores/proveedores de servicios para determinar si se implementaron los controles adecuados para proteger los datos de la tarjeta.

PREGUNTA *Pregunta realizada por el comerciante al proveedor*	**RESPUESTA DESEADA DE PARTE DEL PROVEEDOR**	**ACCIÓN RECOMENDADA** *Basada en la respuesta del proveedor*
¿QUÉ TAN SEGURA ES SU SOLUCIÓN O PRODUCTO?		
1. ¿Su solución/producto asegura la captura y transmisión seguras de los datos del titular de la tarjeta?	**Para transacciones de pago que se realizan en persona y con tarjeta de pago presente:** **SÍ** • Verifique aquí para ver si el terminal de pago es un PTS aprobado por la PCI: List of PCI Approved PTS Devices (Lista de dispositivos PTS aprobados de la PCI) O • Verifique aquí para ver si la aplicación de pago está validada según la PA-DSS de la PCI: List of PCI PA-DSS of Validated Payment Applications (Lista de aplicaciones de pago validadas según la PA-DSS de la PCI) O • Verifique aquí para ver si la solución de cifrado es una solución de P2PE validada de la PCI: List of PCI P2PE Validated Solutions (Lista de soluciones de P2PE validadas de la PCI) **Para transacciones de pago realizadas con tarjeta ausente (incluso comercio electrónico, pedido por correo/pedido por teléfono):** **SÍ** • Verifique aquí para ver si la aplicación de pago está validada según la PA-DSS de la PCI: List of PCI PA-DSS of Validated Payment Applications (Lista de aplicaciones de pago validadas según la PA-DSS de la PCI) O • Verifique aquí para ver si el proveedor de servicios cumple con los requisitos de la PCI DSS: MasterCard's List of Compliant Service Providers (Lista de proveedores de servicios que cumplen con los requisitos de Mastercard) Visa's Global Registry of Service Providers (Registro mundial de proveedores de servicios de Visa) Visa Europe's Registered Member Agents (Agentes miembros registrados de Visa Europe)	Si la respuesta es **NO**, haga la pregunta 2.

Preguntas

PREGUNTA *Pregunta realizada por el comerciante al proveedor*	RESPUESTA DESEADA DE PARTE DEL PROVEEDOR	ACCIÓN RECOMENDADA *Basada en la respuesta del proveedor*
¿QUÉ TAN SEGURA ES SU SOLUCIÓN O PRODUCTO? *(continuación)*		
2. ¿Incluye nuestro acuerdo con usted (el proveedor) cláusulas que establecen que usted mantendrá el cumplimiento de producto/servicio con la PCI DSS (o que recibirá validación de la PCI DSS)?	**SÍ** Los proveedores con productos/soluciones que cumplen o cumplirán con la PCI DSS deben estar dispuestos a incluir esa condición en un acuerdo por escrito. Para recibir información adicional sobre la evidencia que debe buscar relacionada con productos/soluciones que cumplen con la PCI DSS, consulte la Pregunta 1 anterior.	Si la respuesta es **NO**, considere otro proveedor u otra solución.
3. ¿Su producto/solución almacena información de tarjetas de pago de manera local (en el lugar donde se encuentra mi tienda/comercio)?	**NO** Si lo hace, los comerciantes pueden considerar la implementación de una solución de cifrado o tokenización para proteger mejor los datos de la tarjeta. Consulte la *Guía de pagos seguros* para obtener más información sobre cifrado y tokenización.	Si la respuesta es **SÍ**, el comerciante debe confirmar con el proveedor que los datos se almacenan según los requisitos de la PCI DSS. Si la respuesta es no, considere otro proveedor.
4. ¿Protege su solución/producto la información de tarjetas de pago con un cifrado seguro?	**SÍ** El cifrado es una forma de proteger la información por lo que la probabilidad de que la roben es menor. Si puede, seleccione de la List of PCI P2PE Validated Solutions (Lista de soluciones de P2PE validadas de la PCI), en cuyo caso los datos de la tarjeta se protegen apenas usted los recibe y están protegidos mientras se transfieren a través de su red.	Si la respuesta es **NO**, considere otro proveedor u otra solución.

Preguntas

PREGUNTA *Pregunta realizada por el comerciante al proveedor*	RESPUESTA DESEADA DE PARTE DEL PROVEEDOR	ACCIÓN RECOMENDADA *Basada en la respuesta del proveedor*
¿QUÉ TAN SEGURA ES LA INSTALACIÓN DE MI PRODUCTO?		
5. Si el proveedor instala una aplicación de pago de la List of Validated Payment Applications (Lista de aplicaciones de pago validadas) del Consejo de la PCI, pregunte: ¿Es usted un integrador o revendedor calificado (QIR) de la PCI?	**SÍ** Un QIR está entrenado y capacitado por el Consejo para instalar e integrar las aplicaciones de pago de la PA-DSS. Las instalaciones que realiza dan la seguridad de que la aplicación de pago que cumple con las PA-DSS se ha implementado de tal forma que respalda su cumplimiento según la PCI DSS. Verifique aquí para ver si el proveedor aparece en esta lista: List of PCI QIRs (Lista de QIR de la PCI).	Si la respuesta es **NO**, haga las preguntas de seguimiento a la izquierda.
Si la respuesta a la pregunta de arriba es NO, haga las preguntas de seguimiento: Si la aplicación que el proveedor está instalando no está validada por el PCI SSC o si el proveedor no es un QIR, pregunte: • ¿Ofrece soporte durante la instalación para asegurar que nuestra implementación cumple con los requisitos de la PCI DSS? • ¿Ofrece una guía de implementación? • ¿Ofrece una guía de instalación sobre cómo asegurar que los datos de la tarjeta permanezcan protegidos cuando se almacenan, procesan o transmiten?	**SÍ** El proveedor debe tener procesos definidos para ayudarle con la instalación de la solución que cumpla con los requisitos de la PCI DSS. Una instalación incorrecta puede derivar en una solución vulnerable que pone en riesgo los datos. Usted busca una declaración del proveedor que explique cómo le ayuda a garantizar que cumple o cumplirá con los requisitos de la PCI DSS en relación con el producto/la solución.	Si la respuesta es **NO**, considere otro proveedor.

Preguntas

PREGUNTA *Pregunta realizada por el comerciante al proveedor*	RESPUESTA DESEADA DE PARTE DEL PROVEEDOR	ACCIÓN RECOMENDADA *Basada en la respuesta del proveedor*
¿ME OFRECE SOPORTE Y MANTENIMIENTO CONTINUOS PARA SU PRODUCTO/SERVICIO? SI ES ASÍ, ¿CÓMO?		
6. ¿Se instala su producto/solución en mi red o en mis sistemas?	**SÍ** El proveedor debe ofrecer soporte y mantenimiento continuos de parches de seguridad y actualizaciones de software. Además, debería brindar y ofrecer soporte para los lanzamientos de versiones futuras. Lo mejor para usted es contar con proveedores que ofrezcan soporte completo de sus productos y que le ayuden con las instalaciones/parches para garantizarle que cualquier cambio que sufra el sistema cumpla con los requisitos de la PCI.	Si la respuesta es **SÍ**, consulte las preguntas de seguimiento a la izquierda. Si la respuesta es **NO**, vaya a la pregunta 7.
Si la respuesta a la pregunta de arriba es SÍ, haga las preguntas de seguimiento: • ¿Instala parches y actualizaciones al sistema/a la solución? • ¿Lo hace en conformidad con los requisitos de la PCI DSS? • ¿Cómo me notifica; cómo tengo acceso a los parches y qué tipo de soporte ofrece?	**SÍ** Si la solución nunca se actualiza, puede volverse vulnerable a riesgos futuros.	Si la respuesta es **NO**, considere otro proveedor.
7. ¿La solución instalada en los sistemas es de propiedad del proveedor de servicios y este la mantiene (alojados en hosting)?	**SÍ** Esto se considera un Servicio administrado. Si el proveedor de servicios aloja la solución en un hosting, solicite la Declaración de cumplimiento de la PCI DSS y pregunte si la evaluación de este incluye el servicio que usted está utilizando. Verifique si el proveedor de servicios se encuentra en una de estas listas: MasterCard's List of Compliant Service Providers (Lista de proveedores de servicios que cumplen con los requisitos de Mastercard) Visa's Global Registry of Service Providers (Registro mundial de proveedores de servicios de Visa) Visa Europe's Registered Member Agents (Agentes miembros registrados de Visa Europe)	Si la respuesta es **SÍ**, haga las preguntas de seguimiento a la izquierda. Si la respuesta es **NO** (si el servicio administrado no cumple con la PCI DSS) considere otra solución.
Si la respuesta a la pregunta de arriba es **SÍ**, haga las preguntas de seguimiento: ¿Cumple el entorno del proveedor de servicios con las PCI DSS?		

Preguntas

PREGUNTA *Pregunta realizada por el comerciante al proveedor*	RESPUESTA DESEADA DE PARTE DEL PROVEEDOR	ACCIÓN RECOMENDADA *Basada en la respuesta del proveedor*
¿ME OFRECE SOPORTE Y MANTENIMIENTO CONTINUOS PARA SU PRODUCTO/SERVICIO? *continuación*		
8. ¿Necesita tener acceso remoto para darle soporte a mi solución/sistema de pago?	**NO** Generalmente, el acceso remoto es aprovechado para las filtraciones de datos de pagos. La funcionalidad del acceso remoto debe limitarse a un período breve y debe permanecer desactivada en todo otro momento.	Si la respuesta es **NO**, vaya a la pregunta 9. Si la respuesta es **SÍ**, haga las preguntas de seguimiento a la izquierda.
Si la respuesta a la pregunta de arriba es SÍ, haga las preguntas de seguimiento: • ¿Necesita tener acceso remoto para estar siempre activo?	**NO** La funcionalidad del acceso remoto debe limitarse a un período breve y debe permanecer desactivada en todo otro momento.	Si la respuestas es **SÍ** —Si el acceso remoto debe permanecer activo todo el tiempo— considere otro proveedor u otra solución.
• ¿Qué medidas toma para proteger las conexiones de acceso remoto?	**Su proveedor debe utilizar autenticación de múltiples factores Y una contraseña y un nombre de usuario diferentes para cada cliente al que accede de manera remota.** Las conexiones de acceso remoto pueden protegerse a través de identificaciones de usuario y contraseñas únicas para cada persona que usa el sistema. Además, se deben utilizar varias formas de verificación de identidad de la persona que accede al sistema (autenticación de múltiples factores). Los proveedores que utilizan contraseñas/nombre de usuario únicos para cada uno de sus clientes evitan que el riesgo que corre uno de sus clientes no se convierta en un riesgo para muchos o todos los demás clientes con el uso de contraseñas y nombres de usuarios comunes.	Si el producto/servicio no ofrece autenticación de múltiples factores para el acceso remoto, considere otra solución.
9. ¿Es necesario integrar la solución o el producto a mis otros sistemas (por ejemplo, terminales de pago, cuentas por cobrar u otros sistemas que contienen datos del titular de la tarjeta)?	**NO** Un terminal de pago independiente es más fácil de proteger que un sistema de pago más complejo que puede tener muchos sistemas conectados. Si la solución requiere integración con otros sistemas, ¿simplifica esto su entorno de procesamiento o de qué forma le aportará valor a su empresa? Debe tener una necesidad comercial sólida para la integración, ya que el uso de una solución integrada aumentará el alcance de la PCI DSS porque su entorno de datos del titular de la tarjeta se hace más extenso y más complejo. MasterCard's List of Compliant Service Providers (Lista de proveedores de servicios que cumplen con los requisitos de Mastercard)	Si la respuestas es **SÍ**, considere otro proveedor o producto a menos de que exista un requisito comercial sólido que indique que debe tener una solución más sofisticada con conexiones a otros sistemas.

Preguntas

PREGUNTA *Pregunta realizada por el comerciante al proveedor*	RESPUESTA DESEADA DE PARTE DEL PROVEEDOR	ACCIÓN RECOMENDADA *Basada en la respuesta del proveedor*
¿QUÉ SUCEDE SI HAY UNA FILTRACIÓN DE DATOS?		
10. En el caso de que exista una filtración de datos y su producto/solución esté involucrado: • Si tengo que enfrentar multas, ¿usted me ofrece respaldo y protección? • ¿Cómo y cuándo me notifica si es que hay una filtración? • ¿Qué tipo de monitoreo ofrece para detectar filtraciones de datos y actividades sospechosas?	**SÍ** El proveedor/proveedor de servicios debe brindar respaldo en el caso de que exista una filtración de datos del titular de la tarjeta. El proveedor/proveedor de servicios debe aceptar que debe cooperar con un investigador forense, si es se hacen preguntas sobre la solución o el servicio administrados que ofrece. El proveedor/proveedor de servicios debe indemnizar al comerciante por las multas incurridas en el caso de que exista una filtración y se determine que la solución del proveedor es la causa raíz.	Si la respuesta es **NO**, considere otro proveedor u otra solución.
11. ¿El proveedor/proveedor de servicios cuenta con seguro para cubrir las filtraciones de datos relacionadas con su solución/producto?	**SÍ** Contar con un seguro demuestra que el proveedor/proveedor de servicios ha analizado detalladamente su responsabilidad y obligación en relación con las filtraciones de datos de la tarjeta. Si la respuestas es **SÍ**, pregunte sobre el alcance de la cobertura y si su implementación estará cubierta.	Si la respuestas es **NO** — si el proveedor no tiene seguro o no está dispuesto a autoasegurarse— considere la posibilidad de obtener su propio seguro o contratar a otro proveedor.
12. ¿Contribuye el proveedor/proveedor de servicios con la notificación a mis clientes en el caso de una filtración de datos en la cual su solución/producto es la causa raíz?	**SÍ** El proveedor/proveedor de servicios debe estar dispuesto a asistir a los comerciantes con una notificación sobre filtración cuando el sistema de pago que ofrece es la raíz de la filtración.	Si la respuesta es **SÍ**, haga las preguntas de seguimiento a la izquierda. Si la respuesta es **NO** —si el proveedor no contribuye con la notificación— usted debe elaborar un plan de notificación y/o considerar otro proveedor.
Si la respuestas es **SÍ**, ¿en qué medida ayuda con la notificación? • ¿Cubre el costo? • ¿Envía las notificaciones? • ¿Ofrece supervisión de crédito para los clientes afectados?		