

Preguntas que debe hacer a sus proveedores



PRINCIPIOS BÁSICOS DE SEGURIDAD DE DATOS PARA PEQUEÑOS COMERCIANTES

UN PRODUCTO DEL GRUPO DE TRABAJO DE PEQUEÑOS COMERCIANTES DE LA INDUSTRIA DE TARJETAS DE PAGO

VERSIÓN 2.0 | AGOSTO DE 2018

INTRODUCCIÓN..... 1

PROVEEDORES Y PROVEEDORES DE SERVICIOS..... 2

PREGUNTAS 3

**APÉNDICE: ¿Qué preguntas debe hacerles a sus vendedores/
proveedores de soluciones?** 9

Introducción

Preguntas para hacerles a sus proveedores se creó como un complemento de la [Guía de pagos seguros](#), que forma parte de los Principios básicos de seguridad de datos para pequeños comerciantes. El fin de brindarle preguntas para que les haga a sus vendedores y proveedores de servicios es ayudarle a comprender cómo esas entidades dan soporte a la protección de los datos de las tarjetas de sus clientes.

Consulte la [Guía de pagos seguros](#) y los demás Principios básicos de seguridad de datos para pequeños comerciantes en los siguientes sitios:

RECURSO	URL
Guía para realizar pagos seguros	https://www.pcisecuritystandards.org/pdfs/Small_Merchant_Guide_to_Safe_Payments.pdf
Sistemas de pago comunes	https://www.pcisecuritystandards.org/pdfs/Small_Merchant_Common_Payment_Systems.pdf
Glosario de términos sobre pagos y seguridad de la información	https://www.pcisecuritystandards.org/pdfs/Small_Merchant_Glossary_of_Payment_and_Information_Security_Terms.pdf
Herramienta de evaluación	https://www.pcisecuritystandards.org/pci_security/small_merchant_tool_resources Esta herramienta se proporciona a título informativo para los comerciantes únicamente. Pueden utilizarla para empezar a familiarizarse con las prácticas de seguridad aplicables a los medios de pago que aceptan, formular sus respuestas preliminares y ver sus resultados.

Vendedores y proveedores de servicios y cómo funcionan

Es importante que los pequeños comerciantes o pequeñas empresas que entren en contacto con proveedores de pago o proveedores de servicios comprendan el tipo de proveedor con el que están trabajando y se aseguren de que ha tomado las medidas adecuadas 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 vendedores o proveedores de servicios para ayudarles a comprender cuál es la función de estos en cuanto a la protección de datos de la tarjeta.

Vendedores y proveedores de servicios

La siguiente tabla describe los tipos más comunes de proveedores de pago y proveedores de servicios, sus funciones y las normas o programas de PCI que se aplican a esas funciones. El Apéndice contiene una lista de las preguntas aplicables a cada tipo de vendedor o proveedor de servicios.

Tipo de vendedor o proveedor de servicios	Función	Programa o norma de PCI	Buscar:
Proveedor de la aplicación de pago	Vender y dar soporte a aplicaciones que guarden, procesen y/o transmitan los datos del titular de la tarjeta.	Normas de seguridad de datos para las aplicaciones de pago (PA-DSS)	La aplicación está en la Lista de aplicaciones de pago validadas según las PA-DSS de PCI
Proveedores de terminales y soluciones de pago	Vender y dar soporte a dispositivos o soluciones (p. ej., terminales de pago o soluciones de cifrado) utilizados para aceptar pagos con tarjeta.	Seguridad de la transacción con PIN (PTS) Cifrado de punto a punto de PCI	La terminal de pago se encuentra en la Lista de dispositivos de PTS aprobados por PCI La solución de cifrado se encuentra en la Lista de soluciones P2PE de PCI
Procesadores de pago, proveedores de servicios de pago, puertas de enlace de pago y centros de contacto para comercio electrónico	Guardar, procesar o transmitir datos del titular de la tarjeta en nombre de usted.	Normas de seguridad de datos de PCI (PCI DSS)	Solicite su atestación de cumplimiento de las PCI DSS y pregunte si su evaluación incluyó el servicio que usted está utilizando. El proveedor de servicios figura en una de estas listas: Lista de proveedores de servicios que cumplen con los requisitos de MasterCard Registro global de proveedores de servicios de Visa Agentes comerciales registrados de Visa Europa
Proveedores de hosting para comercio electrónico	Hospedar y administrar su servidor/sitio web de comercio electrónico y darle soporte. Estos proveedores proporcionan servicios de hosting únicamente o junto con servicios de procesamiento de pago.		
Proveedores de software como un servicio y proveedores de hosting en la nube	Desarrollar, hospedar y/o administrar su aplicación web o aplicación de pago en la nube (p. ej., aplicación de reservas o venta de boletos en línea).		
Proveedores de servicios que pueden ayudarle a cumplir con los requisitos de las PCI DSS	Administrar/operar sistemas o servicios en nombre de usted (p. ej., centros de datos, proveedores de centros de coubicación, y servicios de tecnología de la información tales como administración de firewall, y servicios de parches/antivirus).		
Integradores y revendedores	Instalar los sistemas de pago de los comerciantes.	Integradores y revendedores certificados (QIR)	Pregunte si el proveedor es un integrador o revendedor certificado (QIR) por PCI. El proveedor figura en la Lista de QIR de PCI .

Preguntas

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

Nota: Si un vendedor o proveedor de soluciones no da respuestas afirmativas a las preguntas aplicables de esta tabla, debería considerar seriamente buscar a otro vendedor o proveedor de soluciones.

Pregunte:	Análisis de las respuestas del proveedor – Pasos útiles e información adicional para los comerciantes
<p>¿Qué tan segura(o) es la solución/el producto del proveedor?</p> <p>1. ¿Su solución/producto captura y transmite de forma segura los datos de la tarjeta de pago?</p> <p>Cuando un producto o servicio está incluido en la lista del PCI SSC o en la de marcas de tarjetas de pago aprobadas, significa que ha sido validado según las normas de seguridad de PCI. Su inclusión en esas listas indica que el proveedor o proveedor de servicios ha tomado medidas adicionales para proporcionar productos o servicios seguros.</p>	<p>En cuanto a las soluciones o productos con terminales o aplicaciones de pago:</p> <ul style="list-style-type: none">• Verifique aquí si la terminal de pago es un dispositivo de PTS aprobado por PCI: Lista de dispositivos de PTS aprobados por PCI <p>Y/O</p> <ul style="list-style-type: none">• Verifique aquí si la aplicación de pago está validada según las PCI PA-DSS: Lista de aplicaciones de pago validadas según las PCI PA-DSS <p>O</p> <ul style="list-style-type: none">• Verifique aquí si la solución es una solución de cifrado P2PE validada por PCI: Lista de soluciones P2PE validadas por PCI <p>El el caso de las transacciones de pago en las que no se presenta una tarjeta (comercio electrónico, pedido por correo o por teléfono):</p> <ul style="list-style-type: none">• Verifique aquí si el proveedor de servicios cumple con las PCI DSS: Lista de proveedores de servicios que cumplen con los requisitos de MasterCard Registro global de proveedores de servicios de Visa Agentes comerciales registrados de Visa Europa <p>O</p> <ul style="list-style-type: none">• Verifique aquí si la aplicación de pago está validada conforme a la PCI PA-DSS: Lista de aplicaciones de pago validadas conforme a la PCI PA-DSS

Preguntas

Pregunte:	Análisis de las respuestas del proveedor – Pasos útiles e información adicional para los comerciantes
<p>¿Qué tan segura(o) es la solución/el producto del proveedor?</p> <p>2. ¿El producto o solución del proveedor guarda la información de la tarjeta de pago en mis sistemas (por ejemplo, los de mi(s) tienda(s), con mi aplicación web, o con mi sitio web de comercio electrónico)? En caso afirmativo, ¿el producto o solución protege los datos?</p>	<p>Los productos o soluciones que tokenizan o cifran los datos de la tarjeta de pago permiten a los comerciantes asegurar esos datos. Consulte la Guía de pagos seguros para ver mayores detalles sobre el cifrado y la tokenización.</p>
<p>3. El producto o solución del proveedor protege los datos de la tarjeta de pago con un cifrado sólido durante la transmisión?</p>	<p>El cifrado convierte la información a un formato que solo es útil para aquellos que conocen una clave digital específica. Al asegurar los datos de la tarjeta de pago de esta manera se reduce la probabilidad de que sean robados y utilizados de manera fraudulenta.</p> <p>En cuanto a las terminales de pago y las terminales de pago integradas:</p> <ul style="list-style-type: none">Si le es posible seleccione en la Lista de soluciones P2PE validadas por PCI un producto o solución en que estén cifrados los datos de la tarjeta. El uso de una solución P2PE significa que los datos de la tarjeta de pago se protegen en el momento en que usted los recibe y mientras se transmiten a través de su red a su procesador de pago. <p>En cuanto a las aplicaciones de pago:</p> <ul style="list-style-type: none">Verifique con su proveedor, revendedor o integrador que la aplicación de pago esté validada según las PCI PA-DSS. <p>En cuanto a los sitios web de comercio electrónico y las aplicaciones web o de pago hospedados:</p> <ul style="list-style-type: none">Pregunte a su proveedor de servicios si está utilizando una versión segura del protocolo de Seguridad de la capa de transporte (TLS) para proteger las transmisiones de los datos de la tarjeta de pago.
<p>4. ¿Es necesario integrar la solución o el producto del proveedor a mis otros sistemas (p. ej., terminales de pago, cuentas por cobrar u otros sistemas que contienen datos del titular de la tarjeta)?</p>	<p>Una terminal de pago independiente es más fácil de proteger que un sistema de pago más complejo que puede tener muchos sistemas conectados.</p> <p>Si la solución requiere integración con otros sistemas en su entorno, considere lo siguiente:</p> <ul style="list-style-type: none">¿Simplifica esto su entorno de procesamiento?¿Cómo agrega valor a su negocio?¿Necesita este tipo de solución? Tenga en cuenta que aumentará el riesgo y la complejidad de sus operaciones puesto que ampliará su entorno de datos de titulares de tarjetas y hará más difícil asegurarlo. <p>Quizá le convenga considerar a otro proveedor u otro producto, a menos que exista una fuerte necesidad comercial de tener una solución más sofisticada con conexiones a sus otros sistemas.</p>

Preguntas

Pregunte:	Análisis de las respuestas del proveedor – Pasos útiles e información adicional para los comerciantes
<p>¿El proveedor me ayuda a instalar o configurar de forma segura el producto o solución?</p> <p>5. Si el proveedor está instalando una aplicación de pago o un sistema en mi entorno, pregunte:</p> <ul style="list-style-type: none">• ¿El proveedor es un integrador o revendedor certificado por PCI?• Si el proveedor no instala la aplicación de pago o el sistema, ¿espera que usted lo haga?	<p>Los QIR son integradores y revendedores especialmente capacitados por el Consejo para encargarse de los controles de seguridad críticos y la instalación de sistemas de pago de comerciantes. Se concentran en esos controles a fin de reducir el riesgo de los comerciantes y mitigar las causas más comunes de violaciones de los datos de pago.</p> <p>Verifique aquí si el proveedor aparece en la Lista de integradores y revendedores certificados por PCI.</p>
<p>6. Independientemente de que el proveedor sea un QIR, si está instalando un sistema o aplicación de pago, pregunte:</p> <ul style="list-style-type: none">• ¿El proveedor me brinda soporte durante la instalación y verifica que se realice de manera segura?• ¿El proveedor me proporciona una guía de implementación para ayudarme a configurar la aplicación de manera segura?	<p>Una instalación inadecuada puede hacer su sistema vulnerable al riesgo. El proveedor debe instalar el sistema o aplicación de forma segura o ayudarle a usted con una guía de implementación. La implementación debe cubrir, como mínimo, cómo cambiar las contraseñas predeterminadas y establecer contraseñas seguras, cómo administrar los parches y actualizaciones, y una descripción de cómo utiliza el software de acceso remoto para acceder a su empresa (y cuál es la función de usted con respecto a ese software). En las preguntas 7-9 siguientes se incluyen más detalles sobre cada una de estas tres áreas.</p>

Preguntas

Pregunte:	Análisis de las respuestas del proveedor – Pasos útiles e información adicional para los comerciantes
<p>¿El proveedor me ayuda a instalar o configurar de forma segura el producto o solución?</p> <p>7. ¿El proveedor me brinda soporte durante la instalación o configuración del producto o solución para ayudarme a cambiar las contraseñas predeterminadas por él?</p> <ul style="list-style-type: none">• ¿El vendedor me ayuda a establecer una contraseña fuerte?	<p>Las contraseñas débiles y las predeterminadas por el proveedor constituyen una de las tres causas principales de violaciones de los datos de los comerciantes (las otras dos se abordan en las preguntas 8 y 9 siguientes).</p> <p>Las contraseñas predeterminadas por el proveedor son las que vienen con un producto o solución, como la primera contraseña para un nuevo sistema o aplicación, un sitio web de comercio electrónico hospedado por un comerciante o una aplicación de reservaciones de hotel. Estas contraseñas suelen ser simples y comúnmente conocidas por los hackers (como "admin", "contraseña" o el nombre de la compañía o el producto del proveedor). Es por ello que hay que cambiarlas por contraseñas fuertes al instalar o configurar el producto por primera vez. Si usted las cambia por una contraseña simple (como "12345"), será más fácil que un hacker entre a sus sistemas de pago.</p> <p>Si el proveedor no cambia las contraseñas predeterminadas al instalar o configurar el sistema o aplicación, debe proporcionarle una guía de implementación que explique cómo cambiarlas por contraseñas fuertes.</p>
<p>¿El proveedor ofrece soporte y mantenimiento para el producto o solución?</p> <p>8. Para entender los parches (correcciones de seguridad del software) y las actualizaciones del producto o solución, pregunte al proveedor:</p> <ul style="list-style-type: none">• ¿Qué soporte y orientación le brinda el proveedor a mi empresa durante el proceso de parchado y actualización?• ¿El proveedor proporciona e instala automáticamente los parches y actualizaciones?• ¿Espera que yo obtenga e instale esos parches y actualizaciones?• ¿Cómo me notifica cuándo están disponibles los parches y actualizaciones o que se han aplicado en forma automática?• Para los sitios web de comercio y las aplicaciones web y de pago hospedados, ¿el proveedor se responsabiliza de parchar y actualizar la solución que me proporciona?	<p>Las aplicaciones y los sistemas sin parches constituyen una de las tres causas principales de violaciones de los datos de los comerciantes (las otras dos se abordan en las preguntas 7 y 9 siguientes).</p> <p>Los sistemas sin parches suelen presentar vulnerabilidades que los hackers aprovechan para acceder a los datos de las tarjetas de pago. El proveedor debe ofrecer mantenimiento y soporte continuos para sus aplicaciones o sistemas por medio de actualizaciones y parches de seguridad del software (correcciones de seguridad). Por ejemplo, debe enviarle los parches de seguridad necesarios, avisarle cuándo están disponibles y orientarlo para su instalación.</p> <p>Los proveedores que más le convienen son aquellos que le brindan soporte completo para sus productos y soluciones y se responsabilizan de los parches y actualizaciones necesarios para mantener seguro su negocio, o le ayudan con ellos.</p>

Preguntas

Pregunte:	Análisis de las respuestas del proveedor – Pasos útiles e información adicional para los comerciantes
¿El proveedor ofrece soporte y mantenimiento para el producto o solución? 9. Para dar soporte a su producto o solución, ¿el proveedor necesita acceso remoto a mi aplicación o sistema de pago? <ul style="list-style-type: none">• ¿El proveedor necesita acceso remoto para estar activo siempre?• ¿Qué medidas toma el proveedor para asegurar el acceso remoto?• ¿El proveedor utiliza la misma contraseña para todos sus clientes o una distinta para cada uno de ellos?	<p>El acceso remoto siempre disponible o “siempre activo” es una de las tres causas principales de las infracciones a los comerciantes (las otras dos se abordan en las preguntas 7 y 8 anteriores). El acceso remoto proporciona una ruta del exterior de la red del comerciante a su interior, que un hacker puede usar fácilmente para violar su sistema (o un sistema hospedado) y acceder a los datos de titulares de tarjetas. Esto puede incluir el acceso remoto a la red de un comerciante, utilizado por el proveedor para dar soporte a una terminal o aplicación de pago, o dar soporte a un entorno de comerciante o aplicación web hospedados.</p> <p>Para protegerse usted, debe asegurarse de que los proveedores le ayuden de las siguientes maneras:</p> <ul style="list-style-type: none">• Limitando el acceso remoto a periodos breves.• Desactivando el acceso remoto cuando no lo estén usando.• Utilizando la autenticación multifactorial (una forma de verificar la identidad de una persona que accede a un sistema por medio de dos o más factores, como algo que sabe y algo que hace o es).• Utilizando un nombre de usuario y una contraseña diferentes para cada cliente al que el proveedor accede de forma remota (a fin de evitar que el uso de un nombre de usuario y una contraseña comunes ponga en riesgo a todos sus clientes).
¿El servicio que el proveedor me está ofreciendo cumple con las PCI DSS? 10. ¿Este producto o solución se ejecuta desde sistemas del proveedor y mantenidos (alojados) por él? Esto significa que su proveedor es un proveedor de servicios. Pregunte: <ul style="list-style-type: none">• ¿El entorno del proveedor de servicios cumple con las PCI DSS?• ¿La evaluación del proveedor de servicios según las PCI DSS cubre los servicios específicos que me está ofreciendo?	<p>¿Esto se considera un “servicio administrado”? Solicite la atestación de cumplimiento de las PCI DSS del proveedor de servicios y verifique si su evaluación incluyó el servicio que usted está utilizando.</p> <p>Verifique si el proveedor de servicios figura en una de estas listas:</p> <p>Lista de proveedores de servicios que cumplen con los requisitos de MasterCard</p> <p>Registro global de proveedores de servicios de Visa</p> <p>Agentes comerciales registrados de Visa Europa</p>
11. ¿El acuerdo del proveedor conmigo incluye cláusulas que establecen que mantendrá el cumplimiento de su servicio con las PCI DSS (o que será validado conforme a esta norma)?	<p>Los proveedores de servicios que cumplen o cumplirán con las PCI DSS deben estar dispuestos a incluir esa condición en un acuerdo por escrito.</p> <p>Verifique si el proveedor de servicios figura en una de las listas incluidas en la pregunta 10 anterior.</p>

Preguntas

Pregunte:	Análisis de las respuestas del proveedor – Pasos útiles e información adicional para los comerciantes
¿El proveedor me ofrecerá soporte si ocurre una violación de mis datos de titulares de tarjetas?	
12. Si ocurre una violación de datos que tiene que ver con el producto o solución del proveedor, pregunte: <ul style="list-style-type: none">• ¿Qué tipo de supervisión de violaciones de datos y actividades sospechosas ofrece?• ¿Cómo y cuándo me notificará si ocurre una violación?• ¿Qué tipo de protección me ofrece si incurro en multas y penalizaciones?	<p>El vendedor/proveedor de servicios debe proporcionar soporte en caso de una violación de los datos del titular de la tarjeta.</p> <p>Si hay preguntas sobre el servicio administrado o el producto o solución que ofrece, el vendedor/proveedor de servicios debe aceptar cooperar con un investigador forense.</p> <p>El vendedor/proveedor de servicios debe aceptar ayudarlo a pagar las multas en que incurra por algún incumplimiento si se determina que la causa es el producto o solución del proveedor.</p>
13. ¿El vendedor/proveedor de servicios tiene contratado un seguro que cubra las violaciones de datos relacionadas con su producto o solución?	El hecho de que el vendedor/proveedor de servicios tenga contratado un seguro muestra que ha pensado en su responsabilidad con respecto a las violaciones de datos de titulares de tarjetas. Si tiene contratado un seguro, pregúntele sobre el alcance de la cobertura y si ampara la implementación que le está ofreciendo.
14. ¿El vendedor/proveedor de servicios ayuda con la notificación a mis clientes en caso de una violación cuando la causa es su producto o solución?	El vendedor/proveedor de servicios debe estar dispuesto a ayudar a los comerciantes con la notificación cuando la causa de una violación de datos es su sistema de pago.
15. Si la respuesta a la pregunta 14 es afirmativa, ¿hasta qué punto ayuda con la notificación el proveedor? ¿El vendedor: <ul style="list-style-type: none">• cubre el costo?• envía la notificación?• se encarga de la supervisión del crédito para los clientes afectados?	Si el proveedor no ayuda con la notificación, usted debe formular un plan para notificar a sus clientes en caso de una violación de datos de titulares de tarjetas.

Apéndice

¿Qué preguntas debe hacerles a sus vendedores/proveedores de soluciones?

Tipo de vendedor o proveedor de servicios	Preguntas aplicables
Proveedor de la aplicación de pago	1–15
Proveedores de terminales y soluciones de pago	1–15
Procesadores de pago, proveedores de servicios de pago, puertas de enlace de pago y centros de contacto para comercio electrónico	1–15
Proveedores de hosting para comercio electrónico	1–15
Proveedores de software como un servicio y proveedores de hosting en la nube	1–4 y 10–15
Proveedores de servicios que pueden ayudarle a cumplir con los requisitos de las PCI DSS	1–15
Integradores y revendedores	5–9