



# **Industria de Tarjetas de Pago (PCI) Norma de seguridad de datos**

---

## **Atestación de cumplimiento de evaluaciones in situ – Comerciantes**

**Versión 3.2**

Abril de 2016

## Sección 1: Información sobre la evaluación

### Instrucciones para la presentación

Esta Atestación de cumplimiento debe completarse como una declaración de los resultados que tuvo la evaluación del comerciante con los *Requisitos de la Norma de seguridad de datos de la industria de tarjetas de pago (PCI DSS) y procedimientos de evaluación de seguridad*. Complete todas las secciones que correspondan: El comerciante es responsable de asegurarse de que las partes relevantes completen cada sección según corresponda: Comuníquese con el adquiriente (banco comercial) o las marcas de pago para establecer los procedimientos para la presentación y elaboración del informe.

#### Parte 1. Información sobre Comerciante y Asesor de Seguridad Certificado

##### Parte 1a. Información de la organización del comerciante

Nombre de la empresa:		DBA (operando bajo el nombre de):	
Nombre del contacto:		Cargo:	
Teléfono:		Correo electrónico:	
Dirección comercial:		Ciudad:	
Estado/Provincia:		País:	
			Código postal:
URL:			

##### Parte 1b. Información de la empresa del evaluador de seguridad certificado (QSA) (si corresponde)

Nombre de la empresa:			
Nombre del contacto del QSA principal:		Cargo:	
Teléfono:		Correo electrónico:	
Dirección comercial:		Ciudad:	
Estado/Provincia:		País:	
			Código postal:
URL:			

#### Parte 2. Resumen ejecutivo

##### Parte 2a. Tipo de actividad comercial del comerciante (marque todo lo que corresponda)

- Comercio minorista   
  Telecomunicaciones   
  Tiendas de comestibles y supermercados  
 Petróleo   
  Comercio electrónico   
  Pedidos por correo/teléfono (MOTO)  
 Otros (especifique):

¿Cuáles son los tipos de canales de pago a los que presta servicios su empresa?

¿Cuáles son los canales de pago que esta evaluación abarca?

- |  |  |
|--|--|
| <input type="checkbox"/> Pedidos por correo/teléfono (MOTO)<br><input type="checkbox"/> Comercio electrónico<br><input type="checkbox"/> Tarjeta presente (en persona) | <input type="checkbox"/> Pedidos por correo/teléfono (MOTO)<br><input type="checkbox"/> Comercio electrónico<br><input type="checkbox"/> Tarjeta presente (en persona) |
|--|--|

**Nota:** Si su organización cuenta con un canal de pago o un proceso que esta evaluación no abarca, comuníquese con su adquirente o marca de pago respecto de la validación para los otros canales.

### Parte 2b. Descripción del negocio de tarjeta de pago

¿De qué forma y en qué capacidad almacena, procesa y/o transmite su empresa los datos de titulares de tarjetas?

### Parte 2c. Ubicaciones

Indique los tipos de instalaciones (por ejemplo, tiendas minoristas, oficinas corporativas, centros de datos, centros de llamadas, etc.) y un resumen de las ubicaciones que se encuentran incluidas en la revisión de las PCI DSS.

Tipo de instalación	Número de instalaciones de este tipo	Ubicaciones de las instalaciones (ciudad, país)
<i>Ejemplo: Tiendas minoristas</i>	3	<i>Boston, MA, EE. UU.</i>

### Parte 2d. Aplicación de pago

¿La organización utiliza una aplicación de pago o más de una?  Sí  No

Proporcione la siguiente información relativa a las aplicaciones de pago que su organización utiliza:

Nombre de la aplicación de pago	Número de versión:	Proveedor de la aplicación	¿Se encuentra la aplicación en la lista de las PA-DSS?	Fecha de vencimiento de la lista de las PA-DSS (si corresponde)
			<input type="checkbox"/> Sí <input type="checkbox"/> No	
			<input type="checkbox"/> Sí <input type="checkbox"/> No	
			<input type="checkbox"/> Sí <input type="checkbox"/> No	
			<input type="checkbox"/> Sí <input type="checkbox"/> No	
			<input type="checkbox"/> Sí <input type="checkbox"/> No	

**Parte 2e. Descripción del entorno**

Proporcione una descripción **general** del entorno que esta evaluación abarca.

*Por ejemplo:*

- *Conexiones hacia y desde el entorno de datos del titular de la tarjeta (CDE).*
- *Componentes importantes que hay dentro del entorno de datos del titular de la tarjeta, incluidos los dispositivos POS, las bases de datos, los servidores web, etc. y cualquier otro componente de pago necesario, según corresponda.*

¿Su empresa utiliza la segmentación de red para influir en el alcance del entorno de las PCI DSS?

Sí  No

*(Consulte la sección “Segmentación de red” de las DSS PCI para obtener información acerca de la segmentación de red).*

**Parte 2f. Proveedores de servicio externos**

¿Su empresa utiliza un Integrador o revendedor certificado (QIR)?

Sí  No

En caso de ser Sí:

Nombre de la empresa QIR:

Nombre individual del QIR:

Descripción de los servicios proporcionados por QIR:

¿Su empresa comparte los datos de los titulares de tarjeta con uno o más proveedores de servicio externos (por ejemplo, Integrador o revendedor certificado (QIR), empresas de puertas de enlace, procesadores de pago, proveedores de servicio de pago (PSP), empresas de Web hosting, agentes de reservas en aerolíneas, agentes del programa de lealtad, etc.)?

Sí  No

**En caso de ser Sí:**

Nombre del proveedor de servicios:	Descripción de los servicios proporcionados:

**Nota:** El requisito 12.8 rige para todas las entidades en esta lista.

## Sección 2: Informe de cumplimiento

---

Esta Atestación de cumplimiento refleja los resultados de una evaluación in situ, que está documentada en un Informe sobre Cumplimiento (ROC) adjunto.

La evaluación documentada en esta atestación y en el ROC se completó el:		
¿Se utilizaron controles de compensación para cumplir con algún requisito en el ROC?	<input type="checkbox"/> Sí	<input type="checkbox"/> No
¿Se identificó algún requisito en el ROC como no aplicable (N/A)?	<input type="checkbox"/> Sí	<input type="checkbox"/> No
¿Hubo algún requisito que no se haya probado?	<input type="checkbox"/> Sí	<input type="checkbox"/> No
¿No se pudo cumplir con algún requisito en el ROC debido a una limitación legal?	<input type="checkbox"/> Sí	<input type="checkbox"/> No

## Sección 3: Detalles de la validación y la atestación

### Parte 3. Validación de la PCI DSS

Esta AOC se basa en los resultados observados en el ROC con fecha (*fecha de finalización del ROC*).

Según los resultados observados en el ROC mencionado anteriormente, los firmantes que se identifican en las Partes 3b-3d, según corresponda, hacen valer el siguiente estado de cumplimiento de la entidad identificada en la Parte 2 del presente documento (**marque una**):

<input type="checkbox"/>	<p><b>En cumplimiento:</b> Se han completado todas las secciones del ROC de la PCI DSS y se ha respondido afirmativamente a todas las preguntas, lo que resulta en una calificación general de <b>EN CUMPLIMIENTO</b>, y, por consiguiente, (<i>nombre de la empresa del comerciante</i>) ha demostrado un cumplimiento total con la PCI DSS.</p>						
<input type="checkbox"/>	<p><b>Falta de cumplimiento:</b> No se han completado todas las secciones del ROC de la PCI DSS o se ha respondido en forma negativa a algunas de las preguntas, lo que resulta en una calificación general de <b>FALTA DE CUMPLIMIENTO</b>, y, por consiguiente, (<i>nombre de la empresa del comerciante</i>) no ha demostrado un cumplimiento total con la PCI DSS.</p> <p><b>Fecha objetivo</b> para el cumplimiento:</p> <p>Es posible que se exija a una entidad que presente este formulario con un estado de Falta de cumplimiento que complete el Plan de acción en la Parte 4 de este documento. <i>Consulte con su adquirente o la(s) marca(s) de pago antes de completar la Parte 4.</i></p>						
<input type="checkbox"/>	<p><b>En cumplimiento pero con una excepción legal:</b> Uno o más requisitos están marcados como “No implementado” debido a una restricción legal que impide el cumplimiento con un requisito. Esta opción requiere una revisión adicional del adquirente o la marca de pago.</p> <p><i>Si está marcado, complete lo siguiente:</i></p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 30%;">Requisito afectado</th> <th>Detalles respecto de cómo la limitación legal impide que se cumpla el requisito</th> </tr> </thead> <tbody> <tr> <td style="height: 20px;"> </td> <td> </td> </tr> <tr> <td style="height: 20px;"> </td> <td> </td> </tr> </tbody> </table>	Requisito afectado	Detalles respecto de cómo la limitación legal impide que se cumpla el requisito				
Requisito afectado	Detalles respecto de cómo la limitación legal impide que se cumpla el requisito						

### Parte 3a. Reconocimiento de estado

Los firmantes confirman:

(**marque todo lo que corresponda**)

<input type="checkbox"/>	El informe sobre cumplimiento (ROC) se completó de acuerdo con los <i>Requisitos de la PCI DSS y procedimientos para la evaluación de la seguridad</i> , versión ( <i>número de versión</i> ), y de conformidad con las instrucciones allí consideradas.
<input type="checkbox"/>	Toda la información dentro del arriba citado ROC y en esta atestación representa razonablemente los resultados de mi evaluación en todos los aspectos sustanciales.
<input type="checkbox"/>	He confirmado con mi proveedor de la aplicación de pago que mi sistema de pago no almacena datos confidenciales de autenticación después de la autorización.
<input type="checkbox"/>	He leído la PCI DSS y reconozco que debo mantener el pleno cumplimiento de dicha norma, según se aplica a mi entorno, en todo momento.

- Si ocurre un cambio en mi entorno, reconozco que debo evaluar nuevamente mi entorno e implementar los requisitos adicionales de las PCI DSS que correspondan.

**Parte 3a. Reconocimiento de estado (cont.)**

- No existe evidencia de almacenamiento de datos completos de la pista, datos de CAV2, CVC2, CID, o CVV2<sup>1</sup>, ni datos de PIN<sup>2</sup> después de encontrarse la autorización de la transacción en NINGÚN sistema revisado durante la presente evaluación<sup>3</sup>.
- Los análisis del ASV completados por un Proveedor aprobado de escaneo (ASV) certificado por el PCI SSC (*nombre del ASV*)

**Parte 3b. Declaración del comerciante**

<i>Firma del director ejecutivo del comerciante</i> ↑	<i>Fecha:</i>
<i>Nombre del Oficial Ejecutivo del comerciante:</i>	<i>Cargo:</i>

**Parte 3c. Reconocimiento del Evaluador de seguridad certificado (QSA) (si corresponde)**

Si un QSA participó o brindó ayuda durante esta evaluación, describa la función realizada:

<i>Firma del Oficial debidamente autorizado de la empresa del QSA</i> ↑	<i>Fecha:</i>
<i>Nombre del Oficial debidamente autorizado :</i>	<i>Empresa de QSA:</i>

**Parte 3d. Participación del Asesor de seguridad interna (ISA) (si corresponde)**

Si un ISA participó o brindó ayuda durante esta evaluación, describa al Personal de ISA y describa la función realizada:

--	--

<sup>1</sup> Datos codificados en la banda magnética, o su equivalente, utilizada para la autorización durante una transacción con tarjeta presente. Es posible que las entidades no retengan los datos completos de la pista después de la autorización de la transacción. Los únicos elementos de los datos de la pista que se pueden retener son el número de cuenta principal (PAN), la fecha de vencimiento y el nombre del titular de la tarjeta.

<sup>2</sup> El valor de tres o cuatro dígitos impreso junto al panel de firma, o en el frente de una tarjeta de pago, que se utiliza para verificar las transacciones sin tarjeta presente.

<sup>3</sup> El número de identificación personal ingresado por el titular de la tarjeta durante una transacción con tarjeta presente o el bloqueo de PIN cifrado presente en el mensaje de la transacción.

#### Parte 4. Plan de acción para los requisitos por falta de cumplimiento

Seleccione la respuesta apropiada para “En cumplimiento con los requisitos de las PCI DSS” correspondiente para cada requisito. Si la respuesta a cualquier requisito es “No”, debe proporcionar la fecha en la que la empresa espera cumplir con el requisito y una breve descripción de las medidas que se tomarán para cumplirlo.

Consulte con su adquirente o la(s) marca(s) de pago antes de completar la Parte 4.

Requisito de las PCI DSS	Descripción del requisito	En cumplimiento con los requisitos de las PCI DSS (seleccione uno)		Fecha y medidas de corrección (si se seleccionó “NO” para algún requisito)
		SÍ	NO	
1	Instalar y mantener una configuración de firewall para proteger los datos del titular de la tarjeta.	<input type="checkbox"/>	<input type="checkbox"/>	
2	No usar los valores predeterminados suministrados por el proveedor para las contraseñas del sistema y otros parámetros de seguridad	<input type="checkbox"/>	<input type="checkbox"/>	
3	Proteger los datos almacenados del titular de la tarjeta.	<input type="checkbox"/>	<input type="checkbox"/>	
4	Cifrar la transmisión de los datos del titular de la tarjeta en las redes públicas abiertas.	<input type="checkbox"/>	<input type="checkbox"/>	
5	Proteger todos los sistemas de malware y actualizar los programas o software antivirus regularmente.	<input type="checkbox"/>	<input type="checkbox"/>	
6	Desarrollar y mantener sistemas y aplicaciones seguros	<input type="checkbox"/>	<input type="checkbox"/>	
7	Restringir el acceso a los datos del titular de la tarjeta según la necesidad de saber que tenga la empresa.	<input type="checkbox"/>	<input type="checkbox"/>	
8	Identifique y autentique el acceso a los componentes del sistema.	<input type="checkbox"/>	<input type="checkbox"/>	
9	Restringir el acceso físico a los datos del titular de la tarjeta.	<input type="checkbox"/>	<input type="checkbox"/>	
10	Rastree y supervise los accesos a los recursos de red y a los datos de los titulares de las tarjetas	<input type="checkbox"/>	<input type="checkbox"/>	
11	Probar periódicamente los sistemas y procesos de seguridad.	<input type="checkbox"/>	<input type="checkbox"/>	
12	Mantener una política que aborde la seguridad de la información para todo el personal	<input type="checkbox"/>	<input type="checkbox"/>	



Anexo A2	Requisitos adicionales de las PCI DSS para las entidades que utilizan SSL/TLS temprana	<input type="checkbox"/>	<input type="checkbox"/>	
----------	--	--------------------------	--------------------------	--

