Industria de Tarjetas de Pago (PCI)

Norma de seguridad de datos

Atestación de cumplimiento para Evaluaciones in situ – Proveedores de servicios

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 proveedor de servicios 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 proveedor de servicios es responsable de asegurarse que las partes relevantes completen cada sección según corresponda: Comuníquese con la marca de pago solicitante para establecer los procedimientos para la presentación y elaboración del informe.

Parte 1. Información sobre el proveedor de servicios y el asesor de seguridad calificado

Parte 1a. Información sobre la organización del proveedor de servicios

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. Verificación del alcance

Servicios que SE INCLUYERON en el alcance de la evaluación de las PCI DSS (marque todas las opciones aplicables)

Nombre de los servicios evaluados:	

Tipo de los servicios evaluados:

Proveedor de hosting: ☐ Aplicación/software ☐ Hardware ☐ Infraestructura/red ☐ Espacio físico (coubicación) ☐ Almacenamiento ☐ Web ☐ Servicios de seguridad ☐ Proveedor de hosting 3-D Secure ☐ Proveedor de hosting compartido ☐ Otros hostings (especifique):	**Servicios administrados (especificar):** ☐ Servicios de seguridad de sistemas ☐ Soporte de TI ☐ Seguridad física ☐ Sistema de administración de terminales ☐ Otros servicios (especificar):	**Procesamiento de pago:** ☐ POS/tarjeta presente ☐ Internet/comercio electrónico ☐ MOTO/Centro de llamadas ☐ ATM ☐ Otro procesamiento (especifique):
☐ Administración de cuentas	☐ Fraude y reintegro de cobros	☐ Conmutador/Puerta de enlace de pagos
☐ Servicios administrativos	☐ Procesamiento del emisor	☐ Servicios prepagados
☐ Administración de facturación	☐ Programas de lealtad	☐ Administración de registros
☐ Compensación y liquidación	☐ Servicios de comerciantes	☐ Pagos de impuestos/gubernamentales
☐ Proveedor de red		
☐ Otros (especifique):		

***Nota**: Estas categorías se proporcionan únicamente a los fines de asistencia, y no tienen como finalidad limitar ni predeterminar la descripción de servicio de una entidad. Si considera que estas categorías no corresponden a su servicio, complete "Otras". Si tiene dudas respecto de la aplicabilidad de una categoría a su servicio, consulte con la marca de pago correspondiente.*

Parte 2a. Verificación de alcance *(continuación)*		
Servicios proporcionados por el proveedor de servicios pero que NO SE INCLUYERON en el alcance de la evaluación de las PCI DSS (marque todos los que correspondan)		
Nombre de los servicios no evaluados:		
Tipo de los servicios no evaluados:		
Proveedor de hosting: ☐ Aplicación/software ☐ Hardware ☐ Infraestructura/red ☐ Espacio físico (coubicación) ☐ Almacenamiento ☐ Web ☐ Servicios de seguridad ☐ Proveedor de hosting 3-D Secure ☐ Proveedor de hosting compartido ☐ Otros hostings (especifique):	**Servicios administrados (especificar):** ☐ Servicios de seguridad de sistemas ☐ Soporte de TI ☐ Seguridad física ☐ Sistema de administración de terminales ☐ Otros servicios (especificar):	**Procesamiento de pago:** ☐ POS/tarjeta presente ☐ Internet/comercio electrónico ☐ MOTO/Centro de llamadas ☐ ATM ☐ Otro procesamiento (especifique):
☐ Administración de cuentas	☐ Fraude y reintegro de cobros	☐ Conmutador/Puerta de enlace de pagos
☐ Servicios administrativos	☐ Procesamiento del emisor	☐ Servicios prepagados
☐ Administración de facturación	☐ Programas de lealtad	☐ Administración de registros
☐ Compensación y liquidación	☐ Servicios de comerciantes	☐ Pagos de impuestos/gubernamentales
☐ Proveedor de red		
☐ Otros (especifique):		
Proporcione una explicación breve de las razones por las que no se incluyeron servicios marcados en la evaluación:		

Parte 2b. Descripción del negocio de tarjeta de pago	
Describa de qué forma y en qué capacidad almacena, procesa y/o transmite su empresa los datos de titulares de tarjetas.	
Describa de qué forma y en qué capacidad su empresa está involucrada o tiene la capacidad de influir en la seguridad de 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):
Ejemplo: Tiendas minoristas	*3*	*Boston, MA, EE. UU.*

Parte 2d. Aplicaciones 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)
			☐ Sí ☐ No	
			☐ Sí ☐ No	
			☐ Sí ☐ No	
			☐ Sí ☐ No	
			☐ Sí ☐ No	
			☐ Sí ☐ No	
			☐ Sí ☐ No	
			☐ Sí ☐ 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? *(Consulte la sección "Segmentación de red" de las DSS PCI para obtener información acerca de la segmentación de red).*	☐ Sí ☐ No

Parte 2f. Proveedores de servicio externos	
¿Su empresa tiene una relación con un Integrador o revendedor certificado (QIR) con el propósito de que se validen los servicios? En caso de ser Sí: Nombre de la empresa QIR: Nombre individual del QIR: Descripción de los servicios proporcionados por QIR:	☐ Sí ☐ No
¿Su empresa mantiene relaciones 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.)? a los fines de validar los servicios?	☐ 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.*

Parte 2g. Resumen de los requisitos probados

Para cada uno de los requisitos de las PCI DSS, seleccione una de las siguientes opciones:

- **Completo**: el requisito y todos los subrequisitos se evaluaron para ese requisito, y no se marcaron subrequisitos como “No probado” o “No corresponde” en el ROC.
- **Parcial**: uno o más subrequisitos de ese requisito se marcaron como “No probado” o “No aplicable” en el ROC.
- **Ninguno**: todos los subrequisitos de ese requisito se marcaron como “No probado” y/o “No aplicable” en el ROC.

En el caso de todos los requisitos identificados como “Parcial” o “Ninguno", proporcione detalles en la columna “Justificación del enfoque", incluidos:

- Detalles de los subrequisitos específicos que se marcaron como “No probado” y/o “No aplicable” en el ROC.
- La razón por la que los subrequisitos no se probaron o no eran aplicables.

Nota: *Se debe completar una tabla para cada servicio que se abarca en este AOC. En el sitio web del PCI SSC, se encuentran disponibles copias adicionales de esta sección*.

Nombre del servicio evaluado:	

	Detalles del requisito evaluado			
Requisito de las PCI DSS	**Completo**	**Parcial**	**Ninguno**	**Justificación del enfoque** (Obligatorio en el caso de las respuestas “Parcial” y “Ninguno". Identifique cuáles son los subrequisitos que no se probaron y la razón).
Requisito 1:	☐	☐	☐	
Requisito 2:	☐	☐	☐	
Requisito 3:	☐	☐	☐	
Requisito 4:	☐	☐	☐	
Requisito 5:	☐	☐	☐	
Requisito 6:	☐	☐	☐	
Requisito 7:	☐	☐	☐	
Requisito 8:	☐	☐	☐	
Requisito 9:	☐	☐	☐	
Requisito 10:	☐	☐	☐	
Requisito 11:	☐	☐	☐	
Requisito 12:	☐	☐	☐	
Anexo A1:	☐	☐	☐	

Anexo A2:	☐	☐	☐	

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?	☐ *Sí*	☐ No
¿Se identificó algún requisito en el ROC como no aplicable (N/A)?	☐ *Sí*	☐ No
¿Hubo algún requisito que no se haya probado?	☐ *Sí*	☐ No
¿No se pudo cumplir con algún requisito en el ROC debido a una limitación legal?	☐ *Sí*	☐ 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):***

☐	**En cumplimiento:** 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 **EN CUMPLIMIENTO**, y, por consiguiente, *(nombre de la empresa del proveedor de servicios)* ha demostrado un cumplimiento total con la PCI DSS.
☐	**Falta de cumplimiento:** 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 **FALTA DE CUMPLIMIENTO**, y, por consiguiente, *(nombre de la empresa del proveedor de servicios)* no ha demostrado un cumplimiento total con la PCI DSS. **Fecha objetivo** para el cumplimiento: 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. *Consulte con las marcas de pago antes de completar la Parte 4.*
☐	**En cumplimiento pero con una excepción legal:** 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. *Si está marcado, complete lo siguiente:*

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)

☐	El informe sobre cumplimiento (ROC) se completó de acuerdo con los *Requisitos de la PCI DSS y procedimientos para la evaluación de la seguridad*, versión *(número de versión)*, y de conformidad con las instrucciones allí consideradas.
☐	Toda la información dentro del arriba citado ROC y en esta atestación representa razonablemente los resultados de mi evaluación en todos los aspectos sustanciales.
☐	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.
☐	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[1], ni datos de PIN[2] después de encontrarse la autorización de la transacción en NINGÚN sistema revisado durante la presente evaluación.[3]
☐	Los análisis del ASV completados por un Proveedor aprobado de escaneo (ASV) certificado por el PCI SSC *(nombre del ASV)*

Parte 3b. Atestación del proveedor de servicios

Firma del Oficial Ejecutivo del proveedor de servicios ↑	*Fecha:*
Nombre del Oficial Ejecutivo del proveedor de servicios:	*Cargo:*

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:	

Firma del Oficial debidamente autorizado de la empresa del QSA ↑	*Fecha:*
Nombre del Oficial debidamente autorizado :	*Empresa de QSA:*

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:	

[1] 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.

[2] 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.

[3] 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 las marcas de pago correspondientes 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.	☐	☐	
2	No usar los valores predeterminados suministrados por el proveedor para las contraseñas del sistema y otros parámetros de seguridad	☐	☐	
3	Proteger los datos almacenados del titular de la tarjeta.	☐	☐	
4	Cifrar la transmisión de los datos del titular de la tarjeta en las redes públicas abiertas.	☐	☐	
5	Proteger todos los sistemas de malware y actualizar los programas o software antivirus regularmente.	☐	☐	
6	Desarrollar y mantener sistemas y aplicaciones seguros.	☐	☐	
7	Restringir el acceso a los datos del titular de la tarjeta según la necesidad de saber que tenga la empresa.	☐	☐	
8	Identificar y autenticar el acceso a los componentes del sistema.	☐	☐	
9	Restringir el acceso físico a los datos del titular de la tarjeta.	☐	☐	
10	Rastree y supervise los accesos a los recursos de red y a los datos de los titulares de las tarjetas	☐	☐	
11	Probar periódicamente los sistemas y procesos de seguridad.	☐	☐	
12	Mantener una política que aborde la seguridad de la información para todo el personal	☐	☐	
Anexo A1	Requisitos adicionales de las PCI DSS para proveedores de hosting compartido	☐	☐	

Anexo A2	Requisitos adicionales de las PCI DSS para las entidades que utilizan SSL/TLS temprana	☐	☐