



Payment Card Industry Estándar de Seguridad de Datos

Atestación de Cumplimiento para el Informe de Cumplimiento - Proveedores de Servicios

Versión 4.0.1

Fecha de Publicación: Agosto de 2024

Atestación de Cumplimiento para el Informe de Cumplimiento con PCI DSS v4.0.1 - Proveedores de Servicios

Nombre de la Entidad:

Fecha del Informe como aparece en el Informe de Cumplimiento:

Fecha de Culminación de la Evaluación:

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

Sección 1: Información de la Evaluación

Instrucciones para la Presentación

La Atestación de Cumplimiento (AOC por sus siglas en inglés) deber ser completado como una declaración de los resultados de la evaluación del proveedor de servicios con respecto a los Requisitos y Procedimientos de Prueba del Estándar de Seguridad de Datos de Payment Card Industry (PCI DSS) ("Evaluación"). Complete todas las secciones. El proveedor de servicios es responsable de garantizar que cada sección sea completada por las partes pertinentes, según corresponda. Póngase en contacto con la(s) entidad(es) que recibirán el AOC para los procedimientos de elaboración de informe y presentación.

Este AOC refleja los resultados documentados en un Informe de Cumplimiento (ROC) relacionado. Las secciones del ROC relacionado se indican en cada Parte/Sección del AOC.

Los términos en mayúsculas utilizados pero no definidos de otro modo en este documento tienen el significado establecido en la Plantilla del Informe de Cumplimiento de PCI DSS.

Parte 1. Información de Contacto

Parte 1a. Entidad Evaluada (ROC Sección 1.1)

Nombre de la compañía:	
DBA (actuando comercialmente como):	
Dirección postal de la compañía:	
Sitio web principal de la compañía:	
Nombre del contacto de la compañía:	
Título del contacto de la compañía:	
Número de teléfono de contacto:	
Dirección de correo electrónico de contacto:	

Parte 1b. Asesor (ROC Sección 1.1)

Provea la siguiente información sobre todos los asesores que participaron en la evaluación. Si no hubo asesor para un tipo de asesor determinado, introduzca No aplicable.

Asesor(es) de Seguridad Interna del PCI SSC

Nombre del ISA:	
-----------------	--

Asesor de Seguridad Calificado

Nombre de la compañía:	
Dirección postal de la compañía:	
Página web de la compañía:	
Nombre del Asesor principal:	
Número de teléfono del asesor:	
Dirección de correo electrónico del asesor:	
Número de certificado del asesor:	

Parte 2. Resumen Ejecutivo

Parte 2a. Verificación del Alcance

Servicios que **SE INCLUYERON** en el ámbito de la evaluación (seleccione todos los que correspondan):

Nombre del/los servicios evaluados:

Tipo de servicios evaluados:

Proveedor de Hospedaje:

- ☐ Aplicaciones / software
- ☐ Hardware
- ☐ Infraestructura / Red
- ☐ Espacio Físico (co-locación)
- ☐ Almacenaje
- ☐ Servicios de Alojamiento Web
- ☐ Servicios de Seguridad
- ☐ Proveedor de Hospedaje 3-D:
- ☐ Proveedor de Servicios Multi-Usuarios
- ☐ Otro tipo de Hospedaje (especifique):

Servicios Gestionados:

- ☐ Servicios de Seguridad de Sistemas
- ☐ Respaldo Informático
- ☐ Seguridad Física
- ☐ Sistema de Gestión de Terminal
- ☐ Otros servicios (especifique):

Procesamiento de Pagos:

- ☐ POI - Tarjeta Presencial
- ☐ Internet / e-commerce
- ☐ MOTO / Centro de Llamadas
- ☐ ATM
- ☐ Otros procesamientos (especifique):

☐ Gestión de Cuenta

☐ Fraude y Devoluciones

☐ Pasarela de Pagos/Conmutador

☐ Servicios Administrativos

☐ Procesamiento de Emisor

☐ Servicios Prepago

☐ Gestión de Facturación

☐ Programas de Fidelización

☐ Gestión de Registros

☐ Compensación y Liquidación

☐ Servicios Comerciales

☐ Pagos de Impuestos/Gobierno

☐ Proveedor de Red

☐ Otros (especifique):

Nota: Estas categorías se proporcionan sólo como asistencia y no pretenden limitar o predeterminar la descripción del servicio de una entidad. Si estas categorías no aplican para el servicio evaluado, rellene "Otros". Si no está claro si una categoría podría aplicarse al servicio evaluado, consulte con la(s) entidad(es) a la(s) que se presentará esta AOC.

Parte 2. Resumen Ejecutivo (continuación)

Parte 2a. Verificación del Alcance (continuación)

Servicios que presta el proveedor de servicios pero que NO SE INCLUYERON en el ámbito de la Evaluación (seleccione todo lo que aplique):

Nombre del servicio(s) no evaluado(s):

Tipo de servicio(s) no evaluado(s):

Proveedor de Hospedaje:

- ☐ Aplicaciones / software
- ☐ Hardware
- ☐ Infraestructura / Red
- ☐ Espacio Físico (co-locación)
- ☐ Almacenaje
- ☐ Servicios de Alojamiento Web
- ☐ Servicios de Seguridad
- ☐ Proveedor de Hospedaje 3-D:
- ☐ Proveedor de Servicios Multi-Usuarios
- ☐ Otro tipo de Hospedaje (especifique):

Servicios Gestionados:

- ☐ Servicios de Seguridad de Sistemas
- ☐ Respaldo Informático
- ☐ Seguridad Física
- ☐ Sistema de Gestión de Terminal
- ☐ Otros servicios (especifique):

Procesamiento de Pagos:

- ☐ POI - Tarjeta Presencial
- ☐ Internet / e-commerce
- ☐ MOTO / Centro de Llamadas
- ☐ ATM
- ☐ Otros procesamientos (especifique):

☐ Gestión de Cuenta

☐ Fraude y Devoluciones

☐ Pasarela de Pagos/Conmutador

☐ Servicios Administrativos

☐ Procesamiento de Emisor

☐ Servicios Prepago

☐ Gestión de Facturación

☐ Programas de Fidelización

☐ Gestión de Registros

☐ Compensación y Liquidación

☐ Servicios Comerciales

☐ Pagos de Impuestos/Gobierno

☐ Proveedor de Red

☐ Otros (especifique):

Explique brevemente por qué no se han incluido en la evaluación algún servicio comprobado:

Parte 2b. Descripción de la Función con Tarjetas de Pago (ROC Sección 2.1 y 3.1)

Describe cómo la empresa almacena, procesa y/o transmite los datos del titular de la tarjeta.

Describe cómo la empresa participa o tiene la capacidad de influir en la seguridad de los datos del titular de la tarjeta.

Describe los componentes del sistema que podrían afectar la seguridad de los datos del titular de la tarjeta.

Parte 2. Resumen Ejecutivo (continuación)

Parte 2c. Descripción del Entorno de las Tarjetas de Pago

Proporcione una descripción de alto nivel del entorno cubierto por esta Evaluación.

Por ejemplo:

- *Conexiones desde y hacia el entorno de datos de tarjetahabiente (CDE).*
- *Componentes críticos del sistema dentro del CDE, tales como dispositivos POI, bases de datos, servidores web, etc., y cualquier otro componente de pago necesario, según corresponda.*
- *Componentes del sistema que podrían afectar la seguridad de los datos del titular de la tarjeta.*

Indique si el entorno incluye la segmentación para reducir el alcance de la Evaluación.
(Refiérase a la sección "Segmentación" de PCI DSS para obtener orientación sobre la segmentación.)

☐ Sí ☐ No

Parte 2d. Localidades e Instalaciones en el Ámbito de Aplicación (ROC Sección 4.6)

Enumere todos los tipos de ubicaciones físicas/instalaciones (por ejemplo, oficinas corporativas, centros de datos, centros de llamadas y salas de correo) dentro del ámbito de esta Evaluación.

Tipo de Instalaciones	Número total de Instalaciones (Cuántas instalaciones de este tipo se encuentran dentro del ámbito)	Ubicación(ones) de las Instalaciones (ciudad, país)
<i>Ejemplo: Centros de Datos</i>	3	<i>Boston, MA, EUA</i>

Parte 2. Resumen Ejecutivo (continuación)

Parte 2e. Productos y Soluciones validados por PCI SSC (ROC Sección 3.3)

¿Utiliza la entidad algún elemento identificado en alguna de las Listas de Productos y Soluciones* validados por PCI SSC?

☐ Sí ☐ No

Provea la siguiente información sobre cada elemento que la entidad utilice de las Listas de Productos y Soluciones Validados por PCI SSC:

Nombre del Producto o Solución Validado por PCI SSC	Versión del Producto o Solución	Estándar PCI SSC según el cual se validó el producto o solución	Número de Referencia de la Lista PCI SSC	Fecha de Expiración de la Lista
				DD-MM-AAAA
				DD-MM-AAAA
				DD-MM-AAAA
				DD-MM-AAAA
				DD-MM-AAAA
				DD-MM-AAAA

* Para los fines de este documento, se entenderá por "Listas de Productos y Soluciones Validados" las listas de productos, soluciones y/o componentes validados que aparecen en el sitio web de PCI SSC (www.pcisecuritystandards.org) (por ejemplo, los Kits de Desarrollo de Software 3DS, los Dispositivos PTS Aprobados, el Software de Pago Validado, las Soluciones Cifradas de Punto a Punto (P2PE), las Soluciones de Introducción de PIN basadas en software en COTS (SPoC), las Soluciones de Pago sin contacto en COTS (CPoC) y los Productos de Métodos de Pagos Móviles en COTS (MPoC).

Parte 2. Resumen Ejecutivo (continuación)

Parte 2f. Proveedores de Servicios Externos (ROC Sección 4.4)

Para los servicios que se están validando, tiene la entidad relaciones con uno o más proveedores de servicios externos que:

- | | |
|--|---|
| <ul style="list-style-type: none"> Almacenan, procesan o transmiten datos del titular de la tarjeta en nombre de la entidad (por ejemplo, pasarelas de pago, procesadores de pago, proveedores de servicios de pago (PSP por sus siglas en inglés) y almacenamiento externo) | <input type="checkbox"/> Sí <input type="checkbox"/> No |
| <ul style="list-style-type: none"> Gestionar los componentes del sistema incluidos en la Evaluación de la entidad (por ejemplo, a través de servicios de control de seguridad de la red, servicios <i>anti-malware</i>, gestión de eventos e incidentes de seguridad (SIEM), centros de contacto y de llamadas, servicios de alojamiento web y proveedores de IaaS, PaaS, SaaS y FaaS en la nube) | <input type="checkbox"/> Sí <input type="checkbox"/> No |
| <ul style="list-style-type: none"> Podría afectar a la seguridad del CDE de la entidad (por ejemplo, proveedores que prestan asistencia a través de acceso remoto, y/o desarrolladores de software a la medida). | <input type="checkbox"/> Sí <input type="checkbox"/> No |

En caso afirmativo:

Nombre del Proveedor de Servicios:

Descripción del Servicio Suministrado:

Nota: El Requisito 12.8 aplica a todas las entidades que aparecen en la lista.

Parte 2. Resumen Ejecutivo (continuación)

Parte 2g. Resumen de la Evaluación (ROC Sección 1.8.1)

Indique a continuación todas las respuestas proporcionadas dentro de cada requisito principal PCI DSS. Para todos los requisitos identificados como "No Aplicable" o "No Probado", llene la tabla de "Justificación del Enfoque" que se encuentra a continuación.

Nota: Debe llenarse una tabla por cada servicio cubierto por este AOC. En el sitio web del PCI SSC encontrará copias adicionales de esta sección.

Nombre del Servicio Evaluado:

Requisito de PCI DSS	Hallazgo del Requisito Se puede seleccionar más de una respuesta para un requisito determinado. Indique todas las respuestas que correspondan.				Seleccione si se Utilizaron Control(es) Compensatorio(s)
	Implementado	No Aplicable	No Probado	No Implementado	
Requisito 1:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requisito 2:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requisito 3:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requisito 4:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requisito 5:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requisito 6:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requisito 7:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requisito 8:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requisito 9:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requisito 10:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requisito 11:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requisito 12:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Anexo A1:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Anexo A2:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Justificación del Enfoque

En el caso de que las respuestas sean "No Aplicable", indique qué sub-requisitos no eran aplicables y el motivo.

En el caso de que las respuestas sean "No Probado", indique qué sub-requisitos no se han comprobado y el motivo.

Sección 2: Informe de Cumplimiento

(ROC Secciones 1.2 y 1.3)

Fecha en que comenzó la evaluación: Nota: Se refiere a la primera fecha en la que se recogieron pruebas o se realizaron observaciones.	DD-MM-AAAA
Fecha en que terminó la evaluación: Nota: Se refiere a la última fecha en que se recopilaban pruebas o se hicieron observaciones.	DD-MM-AAAA
¿No se pudo cumplir con algún requisito del ROC debido a restricciones legales?	<input type="checkbox"/> Sí <input type="checkbox"/> No
¿Se realizaron algunas actividades de prueba a distancia?	<input type="checkbox"/> Sí <input type="checkbox"/> No

Sección 3: Detalles de Validación y Certificación

Parte 3. Validación PCI DSS (ROC Sección 1.7)

Este AOC se basa en los resultados anotados en el ROC fechado (*Fecha del informe como aparece en el ROC DD-MM-AAAA*).

Indique a continuación si se ha realizado una evaluación completa o parcial de PCI DSS:

- ☐ **Evaluación Completa** - Se han evaluado todos los requisitos y, por lo tanto, no se ha marcado ningún requisito como No Probado en el ROC.
- ☐ **Evaluación Parcial** - Uno o más requisitos no se han sido evaluados y, por lo tanto, han sido marcados como No Probados en el ROC. Cualquier requisito no evaluado se anota como No Probado en la Parte 2g que precede.

Sobre la base de los resultados documentados en el ROC indicado anteriormente, cada signatario identificado en cualquiera de las Partes 3b-3d, según corresponda, hace valer el siguiente estado de Conformidad para la entidad identificada en la Parte 2 de este documento (*seleccione una*):

<input type="checkbox"/>	<p>En Conformidad: Todas las secciones del ROC de PCI DSS han sido completadas, y todos los requisitos evaluados están marcados como Implementado o No aplicable, lo que resulta en una calificación general de EN CONFORMIDAD; por lo tanto, (<i>Nombre del Proveedor de Servicios</i>) ha demostrado que cumple con todos los requisitos de PCI DSS con la excepción de aquellos señalados anteriormente como No Probado.</p>									
<input type="checkbox"/>	<p>No-Conformidad: No se completaron todas las secciones del ROC de PCI DSS, o uno o más requisitos están marcados como No Implementado, lo que resulta en una calificación general de NO-CONFORMIDAD; por lo tanto, (<i>Nombre del Proveedor de Servicios</i>) no ha demostrado estar en conformidad con los requisitos de PCI DSS.</p> <p>Fecha Límite para estar en Conformidad: DD-MM-AAAA</p> <p>A una entidad que presente este formulario con un estado de No-Conformidad se le puede solicitar que complete el Plan de Acción en la Parte 4 de este documento. Confirme con la entidad a la que se presentará este AOC antes de completar la Parte 4.</p>									
<input type="checkbox"/>	<p>Conforme pero con una excepción legal: Uno o más de los requisitos evaluados en el ROC están marcados como No Implementado debido a una restricción legal que impide que se cumpla con el requisito y todos los demás requisitos evaluados están marcados como Implementado o No Aplicable, lo que da como resultado una calificación general de EN CUMPLIMIENTO PERO CON EXCEPCIÓN LEGAL; por lo tanto, (<i>Nombre del Proveedor de Servicios</i>) ha demostrado estar en conformidad con todos los requisitos de PCI DSS excepto los señalados anteriormente como No Probado o como No en Orden debido a una restricción legal.</p> <p>Esta opción requiere una revisión adicional por parte de la entidad a la que se presentará este AOC.</p> <p><i>Si la selecciona, complete lo siguiente:</i></p> <table border="1"> <thead> <tr> <th>Requisito Concerniente</th> <th>Detalles de cómo la restricción legal impide que se cumpla con el requisito</th> </tr> </thead> <tbody> <tr> <td> </td> <td> </td> </tr> <tr> <td> </td> <td> </td> </tr> <tr> <td> </td> <td> </td> </tr> </tbody> </table>		Requisito Concerniente	Detalles de cómo la restricción legal impide que se cumpla con el requisito						
Requisito Concerniente	Detalles de cómo la restricción legal impide que se cumpla con el requisito									

Parte 3. Validación PCI DSS (continuación)

Parte 3a. Reconocimiento por parte del Proveedor de Servicios

El signatario confirma:

(Seleccione todos lo que aplican)

<input type="checkbox"/>	El ROC se completó de acuerdo con el PCI DSS, versión 4.0.1, y según las instrucciones de la misma.
<input type="checkbox"/>	Toda la información contenida en el ROC mencionado anteriormente y en esta certificación representa fielmente los resultados de la Evaluación en todos los aspectos materiales.
<input type="checkbox"/>	Los controles PCI DSS se mantendrán en todo momento, según sea aplicable al entorno de la entidad.

Parte 3b. Certificación del Proveedor de Servicios

Firma del Ejecutivo del Proveedor de Servicios. ↑	Fecha: DD-MM-AAAA
Nombre del Ejecutivo del Proveedor de Servicios:	Título:

Parte 3c. Declaración del Asesor de Seguridad Calificado (QSA)

Si un QSA ha participado o asistido en esta evaluación, indique la función que desempeñó:	<input type="checkbox"/> El QSA realizó los procedimientos de prueba.
	<input type="checkbox"/> El QSA prestó otro tipo de asistencia. Si ha seleccionado, describa todas las funciones desempeñadas:

Firma del QSA principal ↑	Fecha: DD-MM-AAAA
Nombre del QSA principal:	

Firma del Funcionario Debidamente Autorizado de la Compañía QSA ↑	Fecha: DD-MM-AAAA
Nombre del Funcionario Debidamente Autorizado:	Compañía QSA:

Parte 3d. Participación del Asesor de Seguridad Interna (ISA) del PCI SSC

Si un ISA ha participado o ha prestado asistencia en esta Evaluación, indique la función desempeñada:	<input type="checkbox"/> El ISA(s) realizó procedimientos de prueba.
	<input type="checkbox"/> El ISA(s) prestó otro tipo de asistencia. Si ha seleccionado, describa todas las funciones desempeñadas:

Parte 4. Plan de Acción para Requisitos No Conformidad

Sólo complete la Parte 4 si es solicitado por la entidad a la que se va a presentar este AOC, y sólo si la Evaluación presenta resultados de No-Conformidad señalados en la Sección 3.

Si se le pide que rellene esta sección, seleccione la respuesta adecuada para "Cumple con los requisitos de PCI DSS" para cada uno de los requisitos que aparecen a continuación. Para cualquier respuesta "No", incluya la fecha en la que la entidad espera poder cumplir con el requisito y proporcione una breve descripción de las acciones que se están llevando a cabo para cumplir con el requisito.

Requisito de PCI DSS	Descripción del Requisito	Cumple con los requisitos de PCI DSS (Seleccione Uno)		Fecha de Rehabilitación y Acciones (Si selecciona "NO" para cualquier Requisito)
		SÍ	NO	
1	Instalar y mantener los controles de seguridad de la red	<input type="checkbox"/>	<input type="checkbox"/>	
2	Aplicar configuraciones seguras a todos los componentes del sistema	<input type="checkbox"/>	<input type="checkbox"/>	
3	Proteger los datos del titular de la tarjeta almacenados	<input type="checkbox"/>	<input type="checkbox"/>	
4	Proteger los datos de tarjetahabiente con criptografía robusta durante la transmisión a través de redes abiertas y públicas	<input type="checkbox"/>	<input type="checkbox"/>	
5	Proteger todos los sistemas y redes de software malicioso	<input type="checkbox"/>	<input type="checkbox"/>	
6	Desarrollar y mantener sistemas y softwares seguros	<input type="checkbox"/>	<input type="checkbox"/>	
7	Restringir el acceso a los componentes del sistema y a los datos de tarjetahabiente según la necesidad de conocimiento de la empresa	<input type="checkbox"/>	<input type="checkbox"/>	
8	Identificar a los usuarios y autenticar el acceso a los componentes del sistema	<input type="checkbox"/>	<input type="checkbox"/>	
9	Restringir el acceso físico a los datos de tarjetahabiente	<input type="checkbox"/>	<input type="checkbox"/>	
10	Registrar y supervisar todos los accesos a los componentes del sistema y a los datos de tarjetahabiente	<input type="checkbox"/>	<input type="checkbox"/>	
11	Poner a prueba regularmente la seguridad de los sistemas y de las redes	<input type="checkbox"/>	<input type="checkbox"/>	
12	Respalidar la seguridad de la información con políticas y programas organizacionales	<input type="checkbox"/>	<input type="checkbox"/>	
Anexo A1	Requisitos adicionales de PCI DSS para Proveedores de Servicios Multiusuario	<input type="checkbox"/>	<input type="checkbox"/>	
Anexo A2	Requisitos adicionales de PCI DSS para entidades que utilizan SSL/primeras versiones de TLS para conexiones de terminal POS POI presencial con tarjetas	<input type="checkbox"/>	<input type="checkbox"/>	

Nota: El PCI Security Standards Council es un organismo de normas global que proporciona recursos para profesionales de la seguridad de los pagos que son desarrollados en colaboración con nuestra comunidad de partes interesadas. Nuestros materiales son aceptados en numerosos programas de cumplimiento en todo el mundo. Consulte con su organización de cumplimiento individual para asegurarse de que este formulario sea aceptado en su programa. Para obtener más información sobre PCI SSC y nuestra comunidad de partes interesadas, visite:

https://www.pcisecuritystandards.org/about_us/