Payment Card Industry

Estándar de Seguridad de Datos

Atestación de Cumplimiento para el Informe de Cumplimiento - Comerciantes

Versión 4.0.1

Fecha de Publicación: Agosto de 2024

PCI DSS v4.0.1 Atestación de Cumplimiento para el Informe de Cumplimiento - Comerciantes

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 considerar se, 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*) debe ser completado como una declaración de los resultados de la evaluación del comerciante 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 comerciante 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 ningún 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. Canales de Pago del Comerciante (seleccione todos los que apliquen): (*ROC* Secciones 2.1 y 3.1)

Indique todos los canales de pago utilizados por la empresa que se incluyen en esta Evaluación.

☐ Pedido por correo / por teléfono *(MOTO)*

☐ Comercio electrónico

☐ Presencial

¿Hay algún canal de pago que no esté incluido en esta Evaluación? En caso afirmativo, indique qué canal(les) no están incluidos en la evaluación y explique brevemente por qué se han excluido.	☐ Sí ☐ No

Nota: *Si el comerciante tiene un canal de pago no cubierto por esta Evaluación, consulte con la(s) entidad(es) a la(s) que se presentará esta AOC acerca de la validación para los otros canales.*

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

Para cada canal de pago incluido en esta Evaluación seleccionado en la Parte 2a previa, describa cómo la empresa almacena, procesa y/o transmite los datos del titular de la tarjeta.

Canal	Cómo la Empresa Almacena, Procesa y/o Transmite los Datos del Titular de la Tarjeta

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. Consulte la sección "Segmentación" de PCI DSS para obtener orientación sobre la segmentación.	☐ Sí ☐ No

Parte 2. Resumen Ejecutivo (continuación)

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

Enumere todos los tipos de ubicaciones físicas/instalaciones (por ejemplo, locales de venta al por menor, 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)
Ejemplo: Ubicación de Locales de Venta al por Menor	*3*	*Boston, MA, EUA*

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)

Tiene la entidad relaciones con uno o más proveedores de servicios externos que:	
• 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*) y almacenamiento externo)	☐ Sí ☐ No
• Gestionar los componentes del sistema incluidos en el ámbito de la Evaluación (por ejemplo, a través de servicios de control de seguridad de la red, servicios *anti-malware*, 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)	☐ Sí ☐ No
• 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).	☐ Sí ☐ 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.

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:	☐	☐	☐	☐	☐
Requisito 2:	☐	☐	☐	☐	☐
Requisito 3:	☐	☐	☐	☐	☐
Requisito 4:	☐	☐	☐	☐	☐
Requisito 5:	☐	☐	☐	☐	☐
Requisito 6:	☐	☐	☐	☐	☐
Requisito 7:	☐	☐	☐	☐	☐
Requisito 8:	☐	☐	☐	☐	☐
Requisito 9:	☐	☐	☐	☐	☐
Requisito 10:	☐	☐	☐	☐	☐
Requisito 11:	☐	☐	☐	☐	☐
Requisito 12:	☐	☐	☐	☐	☐
Anexo A2:	☐	☐	☐	☐	☐

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 recopilaron pruebas o se hicieron observaciones.*	DD-MM-AAAA
¿No se pudo cumplir con algún requisito del ROC debido a restricciones legales?	☐ Sí ☐ No
¿Se realizaron algunas actividades de prueba a distancia?	☐ Sí ☐ 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)*:

☐	**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, (Nombre del Comerciante) ha demostrado que cumple con todos los requisitos de PCI DSS con la excepción de aquellos señalados anteriormente como No Probado.
☐	**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, (Nombre del Comerciante) no ha demostrado estar en conformidad con los requisitos de PCI DSS. **Fecha Límite** para estar en Conformidad: DD-MM-AAAA 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.
☐	**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, *(Nombre del Comerciante)* 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. Esta opción requiere una revisión adicional por parte de la entidad a la que se presentará este AOC. *Si la selecciona, complete lo siguiente:*

Requisito Concerniente	Detalles de cómo la restricción legal impide que se cumpla con el requisito

Parte 3. Validación PCI DSS (continuación)

Parte 3a. Reconocimiento del Comerciante

El signatario confirma:
(Seleccione todos lo que aplican)

☐	El *ROC* se completó de acuerdo con el PCI DSS, versión 4.0, y según las instrucciones de la misma.
☐	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.
☐	Los controles PCI DSS se mantendrán en todo momento, según sea aplicable al entorno de la entidad.

Parte 3b. Declaración del Comerciante

Firma del Ejecutivo del Comerciante ↗	Fecha: DD-MM-AAAA
Nombre del Ejecutivo del Comerciante:	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:	☐ El *QSA* realizó los procedimientos de prueba.
	☐ 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:	☐ El ISA(s) realizó procedimientos de prueba.
	☐ 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)		**Rehabilitación Fecha y Acciones** (Si selecciona "NO" para cualquier Requisito)
		SÍ	**NO**	
1	Instalar y mantener los controles de seguridad de la red	☐	☐	
2	Aplicar configuraciones seguras a todos los componentes del sistema	☐	☐	
3	Proteger los datos del titular de la tarjeta almacenados	☐	☐	
4	Proteger los datos de tarjetahabiente con criptografía robusta durante la transmisión a través de redes abiertas y públicas	☐	☐	
5	Proteger todos los sistemas y redes de software malicioso	☐	☐	
6	Desarrollar y mantener sistemas y softwares seguros	☐	☐	
7	Restringir el acceso a los componentes del sistema y a los datos de tarjetahabiente según la necesidad de conocimiento de la empresa	☐	☐	
8	Identificar a los usuarios y autenticar el acceso a los componentes del sistema	☐	☐	
9	Restringir el acceso físico a los datos de tarjetahabiente	☐	☐	
10	Registrar y supervisar todos los accesos a los componentes del sistema y a los datos de tarjetahabiente	☐	☐	
11	Poner a prueba regularmente la seguridad de los sistemas y de las redes	☐	☐	
12	Respaldar la seguridad de la información con políticas y programas organizacionales	☐	☐	
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	☐	☐	

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/