



**Normas de Seguridad de Datos  
de la Industria de Tarjetas de Pago (PCI)  
Cuestionario de autoevaluación A  
y Declaración de cumplimiento**

---

**Sin almacenamiento, procesamiento o  
transmisión electrónica de los datos de los  
titulares de tarjetas**

**Versión 1.2**

Octubre de 2008

## Modificaciones realizadas a los documentos

---

Fecha	Versión	Descripción
1º de octubre de 2008	1.2	Alinear el contenido con las nuevas PCI DSS, versión 1.2 e implementar cambios menores observados desde la versión 1.1. original.

## Índice

---

<b>Modificaciones realizadas a los documentos</b> .....	<b>i</b>
<b>Normas de seguridad de datos de la PCI: documentos relacionados</b> .....	<b>ii</b>
<b>Antes de comenzar</b> .....	<b>iii</b>
<b>Cómo completar el Cuestionario de autoevaluación</b> .....	<b>iii</b>
<b>Cumplimiento de las PCI DSS: pasos de conclusión</b> .....	<b>iii</b>
<b>Guía para la no aplicabilidad de ciertos requisitos específicos</b> .....	<b>iii</b>
<b>Declaración de cumplimiento, SAQ A</b> .....	<b>1</b>
<b>Cuestionario de autoevaluación A</b> .....	<b>4</b>
<b>Implemente medidas sólidas de control de acceso</b> .....	<b>4</b>
<i>Requisito 9: Limite el acceso físico a los datos del titular de la tarjeta</i> .....	<b>4</b>
<b>Mantenga una política de seguridad de información</b> .....	<b>5</b>
<i>Requisito 12: Mantenga una política que aborde la seguridad de la información para empleados y contratistas</i> .....	<b>5</b>
<b>Anexo A: (no se usa)</b> .....	<b>6</b>
<b>Anexo B: Controles de compensación</b> .....	<b>7</b>
<b>Anexo C: Hoja de trabajo de controles de compensación</b> .....	<b>8</b>
<b>Hoja de trabajo de controles de compensación – Ejemplo completo</b> .....	<b>9</b>
<b>Anexo D: Explicación de no aplicabilidad</b> .....	<b>10</b>

## Normas de seguridad de datos de la PCI: documentos relacionados

Los siguientes documentos han sido creados para ayudar a los comerciantes y proveedores de servicios a entender las normas de seguridad de la PCI y el cuestionario de autoevaluación de las normas PCI DSS.

Documento	Destinatarios
<i>Requisitos de normas de seguridad de datos de la PCI y procedimientos de evaluación de seguridad</i>	Todos los comerciantes y proveedores de servicios
<i>Exploración de PCI DSS: Comprensión del objetivo de los requisitos</i>	Todos los comerciantes y proveedores de servicios
<i>Normas de seguridad de datos de la PCI: Instrucciones y directrices de autoevaluación</i>	Todos los comerciantes y proveedores de servicios
<i>Normas de seguridad de datos de la PCI: Declaración y cuestionario de autoevaluación A</i>	Comerciantes <sup>1</sup>
<i>Normas de seguridad de datos de la PCI: Declaración y cuestionario de autoevaluación B</i>	Comerciantes <sup>1</sup>
<i>Normas de seguridad de datos de la PCI: Declaración y cuestionario de autoevaluación C</i>	Comerciantes <sup>1</sup>
<i>Normas de seguridad de datos de la PCI: Declaración y cuestionario de autoevaluación D</i>	Comerciantes <sup>1</sup> y todos los proveedores de servicios
<i>Glosario de términos, abreviaturas y acrónimos de las Normas de seguridad de datos de la PCI y Normas de seguridad de datos para las aplicaciones de pago</i>	Todos los comerciantes y proveedores de servicios

<sup>1</sup> Para determinar el Cuestionario de Autoevaluación apropiado, consulte las *Normas de seguridad de datos de la PCI: Instrucciones y directrices de autoevaluación*, "Selección del SAC y de la declaración que mejor se adapta a su organización".

## Antes de comenzar

---

### Cómo completar el Cuestionario de autoevaluación

El cuestionario SAQ A se desarrolló para responder a los requerimientos de comerciantes que retienen solamente informes o recibos en papel donde constan los datos de los titulares de tarjetas, pero que no almacenan esos datos en formato electrónico ni procesan o transfieren ningún dato de los titulares de tarjetas en sus instalaciones.

A fin de validar el cuestionario SAQ, estos comerciantes quedan definidos como tipo 1 tanto en este documento como en los *Lineamientos e instrucciones para completar el cuestionario de autoevaluación de las normas PCI DSS*. Según esta clasificación, no almacenan los datos de los titulares de tarjetas en formato electrónico ni procesan o transmiten cualquier tipo de dato de los titulares de tarjetas en sus instalaciones. Deben validar el cumplimiento completando el Cuestionario de autoevaluación A y la Declaración de cumplimiento relacionada con dicho cuestionario, a fin de confirmar que:

- Su empresa realiza solo transacciones donde la tarjeta no es visible (comercio electrónico u órdenes por mail o teléfono).
- Su empresa no almacena, procesa o transmite ningún tipo de datos de titulares de tarjetas en las instalaciones, sino que depende por completo en proveedores de servicios externos para ejercer esta función.
- Su compañía ha confirmado que el o los proveedores de servicios externos son responsables del almacenamiento, procesamiento y/o transferencia de los datos de los titulares de tarjetas cumplen con las normas PCI DSS.
- Su empresa conserva solamente informes o recibos en papel donde constan los datos de los titulares de tarjetas, y no recibe estos documentos por medios electrónicos.
- Su empresa no almacena ningún dato de los titulares de tarjetas en formato electrónico.

**Esta opción no se aplica nunca a los comerciantes con entornos de punto de venta (POS) cara a cara.**

### Cumplimiento de las PCI DSS: pasos de conclusión

1. Complete el Cuestionario de autoevaluación (SAQ A) según las instrucciones de las *Instrucciones y directrices del cuestionario de autoevaluación*.
2. Complete la Declaración de cumplimiento en su totalidad.
3. Presente al adquirente el cuestionario SAQ y la Declaración de cumplimiento junto con cualquier otro documento solicitado.

### Guía para la no aplicabilidad de ciertos requisitos específicos

**Non-Applicability:** Requirements deemed not applicable to your environment must be indicated with “N/A” in the “Special” column of the SAQ. Accordingly, complete the “Explanation of Non-Applicability” worksheet in the Appendix for each “N/A” entry.

## Declaración de cumplimiento, SAQ A

### Instrucciones para la presentación

El comerciante debe completar esta Declaración de cumplimiento para manifestar su estado de cumplimiento con los *Requisitos de las Normas de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI DSS)* y los *procedimientos de evaluación de seguridad*. Complete todas las secciones aplicables y consulte las instrucciones para presentar esta declaración en la sección "Cumplimiento con las normas PCI DSS: pasos para completar el proceso", incluida en este documento.

### Parte 1. Información sobre la empresa del Asesor de Seguridad Certificado (si corresponde)

Nombre de la empresa:				
Nombre de contacto del QSA principal:	Cargo:			
N.º de teléfono:	Dirección de correo electrónico:			
Dirección comercial:	Ciudad:			
Estado/Provincia:	País:	Código postal:		
URL:				

### Parte 2. Información sobre la organización del comerciante

Nombre de la empresa:	Nombre(s) comercial(es) (DBA):			
Nombre de contacto:	Cargo:			
N.º de teléfono:	Dirección de correo electrónico:			
Dirección comercial:	Ciudad:			
Estado/Provincia:	País:	Código postal:		
URL:				

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

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

Enumere las instalaciones y ubicaciones incluidas en la revisión de las normas PCI DSS:

## Parte 2b. Relaciones

¿Su empresa tiene relación con uno o más proveedores de servicios externos (por ejemplo, empresas de puertos de enlace y Web hosting, agentes de reservas aéreas, agentes de programas de lealtad, etc.)?  Sí  No

¿Su empresa tiene relación con más de un adquiriente?  Sí  No

## Parte 2c. Elegibilidad para completar el cuestionario SAQ A

El comerciante certifica la elegibilidad para completar esta versión abreviada del Cuestionario de Autoevaluación porque:

- |                          |   |
|--------------------------|---|
| <input type="checkbox"/> | El comerciante no almacena, procesa o transmite ningún tipo de datos de titulares de tarjetas en las instalaciones, sino que depende por completo en proveedores de servicios externos para ejercer esta función. |
| <input type="checkbox"/> | Los proveedores de servicios externos responsables del almacenamiento, el procesamiento y/o la transferencia de los datos de los titulares de tarjetas cumplen con las normas PCI DSS.                            |
| <input type="checkbox"/> | El comerciante no almacena ningún tipo de dato de los titulares de tarjetas en formato electrónico.   |
| <input type="checkbox"/> | Debido a que el comerciante no almacena los datos de los titulares de tarjetas, esos datos se conservan solamente como informes en papel o copias de recibos, y no se los recibe por medios electrónicos.         |

## Parte 3. Validación de las PCI DSS

Según los resultados observados en el cuestionario SAQ A de fecha (*fecha de compleción*), (*Nombre de la empresa del comerciante*) declara que su estado de cumplimiento es el siguiente (marque una opción):

- Conforme:** Se han completado todas las secciones del cuestionario SAQ de la PCI y la respuesta a todas las preguntas es "Sí," lo que da como resultado una clasificación general de **CUMPLIMIENTO**. Por tanto, (*Nombre de la empresa del comerciante*) ha demostrado un total cumplimiento con las PCI DSS.
- No conforme:** Se han completado todas las secciones del cuestionario SAQ de la PCI y algunas respuestas obtuvieron "No" como respuesta, lo que da como resultado una clasificación general de **NO CONFORME**. Por tanto, (*Nombre de la empresa del comerciante*) no ha demostrado un total cumplimiento con las PCI DSS.
- **Fecha objetivo** para el cumplimiento:
  - Una entidad que envía el presente formulario con el estado No conforme posiblemente deba completar el Plan de acción de la Parte 4 de este documento. *Consulte con su adquiriente o la(s) marca(s) de pago antes de completar la Parte 4, ya que no todas las marcas de pago necesitan esta sección.*

## Parte 3a. Confirmación del estado de cumplimiento

El comerciante confirma que:

- |                          |  |
|--------------------------|--|
| <input type="checkbox"/> | El Cuestionario de autoevaluación A de las normas PCI DSS, versión (SAQ version #), se completó según las instrucciones dadas.                           |
| <input type="checkbox"/> | Toda la información que aparece en el cuestionario antes mencionado y en esta declaración muestran los resultados de la evaluación de manera equitativa. |
| <input type="checkbox"/> | He leído las normas PCI DSS y reconozco que debo cumplirlas en todo momento.   |

### Parte 3b. Confirmación del comerciante

<i>Firma del Oficial ejecutivo del comerciante</i> ↑	<i>Fecha</i> ↑
<i>Nombre del Oficial Ejecutivo del comerciante</i> ↑	<i>Cargo</i> ↑
<i>Nombre del comercio representado</i> ↑	

### Parte 4. Plan de acción para el estado de no conformidad

Seleccione el “Estado de cumplimiento” adecuado para cada requisito. Si la respuesta a cualquier requisito es “NO”, debe proporcionar la fecha en la que la empresa cumplirá 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, ya que no todas las marcas de pago necesitan esta sección.*

Requisitos de las PCI DSS	Descripción del requisito	Estado de cumplimiento (Seleccione uno)		Fecha de la reparación y acciones (si el estado de cumplimiento es “NO”)
		SÍ	NO	
9	Limite el acceso físico a los datos del titular de la tarjeta	<input type="checkbox"/>	<input type="checkbox"/>	
12	Mantenga una política que aborde la seguridad de la información	<input type="checkbox"/>	<input type="checkbox"/>	

## Cuestionario de autoevaluación A

Fecha de cumplimiento:

### Implemente medidas sólidas de control de acceso

#### Requisito 9: *Limite el acceso físico a los datos del titular de la tarjeta*

Pregunta	Respuesta	Sí	No	Especial*
9.6 ¿Están todos los papeles y dispositivos electrónicos que contienen datos de los titulares de tarjetas resguardados de forma física?		<input type="checkbox"/>	<input type="checkbox"/>	
9.7 (a) ¿Lleva un control estricto sobre la distribución interna o externa de cualquier tipo de medios que contengan datos de los titulares de tarjetas?		<input type="checkbox"/>	<input type="checkbox"/>	
(b) ¿Incluyen los controles lo siguiente?				
9.7.1 ¿Se encuentran los medios clasificados de manera que se puedan identificar como confidenciales?		<input type="checkbox"/>	<input type="checkbox"/>	
9.7.2 ¿Se envía medios por correo seguro u otro método de envío que se pueda rastrear con precisión?		<input type="checkbox"/>	<input type="checkbox"/>	
9.8 ¿Existen procesos y procedimientos establecidos para asegurar que se obtenga aprobación de la administración antes de trasladar cualquier medio con los datos de titulares de tarjetas desde un área segura (especialmente cuando se los distribuye a personas)?		<input type="checkbox"/>	<input type="checkbox"/>	
9.9 ¿Se mantiene un control estricto sobre el almacenamiento y accesibilidad de los medios que contienen datos de los titulares de tarjetas?		<input type="checkbox"/>	<input type="checkbox"/>	
9.10 ¿Se destruyen los medios que contengan datos de titulares de tarjetas cuando ya no sean necesarios para la empresa o por motivos legales? La destrucción debe realizarse de la siguiente manera:		<input type="checkbox"/>	<input type="checkbox"/>	
9.10.1 ¿Se pasan los materiales de copias en papel por una trituradora que corte en zig zag, se incineran o se hacen pasta de modo que sea imposible reconstruirlos?		<input type="checkbox"/>	<input type="checkbox"/>	

\* "No aplicable" (N/A) o "Se utilizaron Controles de compensación". Las organizaciones que utilicen esta sección deben completar la Hoja de trabajo para controles de compensación o la Hoja de trabajo de explicaciones de no aplicabilidad, según corresponda. Ambos formularios se encuentran en el Anexo.

## Mantenga una política de seguridad de información

### **Requisito 12: Mantenga una política que aborde la seguridad de la información para empleados y contratistas**

Pregunta		Respuesta	Sí	No	Especial*
12.8	Si se comparten los datos de titulares de tarjetas con proveedores de servicios, ¿se mantienen e implementan políticas y procedimientos para administrar proveedores de servicios? ¿las políticas y los procedimientos incluyen lo siguiente?		<input type="checkbox"/>	<input type="checkbox"/>	
12.8.1	Se mantiene una lista de proveedores de servicios.		<input type="checkbox"/>	<input type="checkbox"/>	
12.8.2	Un acuerdo escrito que incluya una mención de que los proveedores de servicios son responsables de la seguridad de los datos de los titulares de tarjetas que ellos tienen en su poder.		<input type="checkbox"/>	<input type="checkbox"/>	
12.8.3	Existe un proceso para comprometer a los proveedores de servicios que incluye una auditoría de compra adecuada previa al compromiso.		<input type="checkbox"/>	<input type="checkbox"/>	
12.8.4	Se mantiene un programa para supervisar el estado de cumplimiento de las PCI DSS de los proveedores de servicios.		<input type="checkbox"/>	<input type="checkbox"/>	

\* “No aplicable” (N/A) o “Se utilizaron Controles de compensación”. Las organizaciones que utilicen esta sección deben completar la Hoja de trabajo para controles de compensación o la Hoja de trabajo de explicaciones de no aplicabilidad, según corresponda. Ambos formularios se encuentran en el Anexo.

## **Anexo A: (no se usa)**

*Esta página se dejó en blanco de manera intencional*

## Anexo B: Controles de compensación

Los controles de compensación se pueden tener en cuenta para la mayoría de los requisitos de las PCI DSS cuando una entidad no puede cumplir con un requisito explícitamente establecido, debido a los límites comerciales legítimos técnicos o documentados, pero pudo mitigar el riesgo asociado con el requisito de forma suficiente, mediante la implementación de otros controles, o controles de compensación.

Los controles de compensación deben cumplir con los siguientes criterios:

1. Cumplir con el propósito y el rigor del requisito original de las PCI DSS.
2. Proporcionar un nivel similar de defensa, tal como el requisito original de PCI DSS, de manera que el control de compensación compense el riesgo para el cual se diseñó el requisito original de las PCI DSS. (Consulte Exploración de PCI DSS para obtener el propósito de cada requisito de PCI DSS).
3. Conozca en profundidad otros requisitos de las PCI DSS. (El simple cumplimiento con otros requisitos de las PCI DSS no constituye un control de compensación).

Al evaluar exhaustivamente los controles de compensación, considere lo siguiente:

**Nota: los puntos a) a c) que aparecen a continuación son sólo ejemplos. El asesor que realiza la revisión de las PCI DSS debe revisar y validar si los controles de compensación son suficientes. La eficacia de un control de compensación depende de los aspectos específicos del entorno en el que se implementa el control, los controles de seguridad circundantes y la configuración del control. Las empresas deben saber que un control de compensación en particular no resulta eficaz en todos los entornos.**

- a) Los requisitos de las PCI DSS NO SE PUEDEN considerar controles de compensación si ya fueron requisito para el elemento en revisión. Por ejemplo, las contraseñas para el acceso administrativo sin consola se deben enviar cifradas para mitigar el riesgo de que se intercepten contraseñas administrativas de texto claro. Una entidad no puede utilizar otros requisitos de contraseña de las PCI DSS (bloqueo de intrusos, contraseñas complejas, etc.) para compensar la falta de contraseñas cifradas, puesto que esos otros requisitos de contraseña no mitigan el riesgo de que se intercepten las contraseñas de texto claro. Además, los demás controles de contraseña ya son requisitos de las PCI DSS para el elemento en revisión (contraseñas).
  - b) Los requisitos de las PCI DSS SE PUEDEN considerar controles de compensación si se requieren para otra área, pero no son requisito para el elemento en revisión. Por ejemplo, la autenticación de dos factores es un requisito de las PCI DSS para el acceso remoto. La autenticación de dos factores *desde la red interna* también se puede considerar un control de compensación para el acceso administrativo sin consola cuando no se puede admitir la transmisión de contraseñas cifradas. La autenticación de dos factores posiblemente sea un control de compensación aceptable si; (1) cumple con el propósito del requisito original al abordar el riesgo de que se intercepten las contraseñas administrativa de texto claro y (2) está adecuadamente configurada y en un entorno seguro.
  - c) Los requisitos existentes de la PCI DSS se pueden combinar con nuevos controles para convertirse en un control de compensación. Por ejemplo, si una empresa no puede dejar ilegibles los datos de los titulares de tarjetas según el requisito 3.4 (por ejemplo, mediante cifrado), un control de compensación podría constar de un dispositivo o combinación de dispositivos, aplicaciones y controles que aborden lo siguiente: (1) segmentación interna de la red; (2) filtrado de dirección IP o MAC y (3) autenticación de dos factores desde la red interna.
4. Sea cuidadoso con el riesgo adicional que impone la no adhesión al requisito de las PCI DSS

El asesor debe evaluar por completo los controles de compensación durante cada evaluación anual de PCI DSS para validar que cada control de compensación aborde de forma correcta el riesgo para el cual se diseñó el requisito original de PCI DSS, según los puntos 1 a 4 anteriores. Para mantener el cumplimiento, se deben aplicar procesos y controles para garantizar que los controles de compensación permanezcan vigentes después de completarse la evaluación.

## Anexo C: Hoja de trabajo de controles de compensación

Utilice esta hoja de trabajo para definir los controles de compensación para cualquier requisito en el que se marcó “Sí” y se mencionaron controles de compensación en la columna “Especial”.

**Nota:** Sólo las empresas que han llevado a cabo un análisis de riesgos y que tienen limitaciones legítimas tecnológicas o documentadas pueden considerar el uso de controles de compensación para lograr el cumplimiento.

### Número de requisito y definición:

	Información requerida	Explicación
1. <b>Limitaciones</b>	Enumere las limitaciones que impiden el cumplimiento con el requisito original.	
2. <b>Objetivo</b>	Defina el objetivo del control original; identifique el objetivo con el que cumple el control de compensación.	
3. <b>Riesgo identificado</b>	Identifique cualquier riesgo adicional que imponga la falta del control original.	
4. <b>Definición de controles de compensación</b>	Defina controles de compensación y explique de qué manera identifican los objetivos del control original y el riesgo elevado, si es que existe alguno.	
5. <b>Validación de controles de compensación</b>	Defina de qué forma se validaron y se probaron los controles de compensación.	
6. <b>Mantenimiento</b>	Defina los procesos y controles que se aplican para mantener los controles de compensación.	

## Hoja de trabajo de controles de compensación – Ejemplo completo

Utilice esta hoja de trabajo para definir los controles de compensación para cualquier requisito en el que se marcó “Sí” y se mencionaron controles de compensación en la columna “Especial”.

**Número de requisito:** 8.1 *¿Todos los usuarios se identifican con un nombre de usuario único antes de permitirles tener acceso a componentes del sistema y a datos de titulares de tarjetas?*

	Información requerida	Explicación
<b>1. Limitaciones</b>	Enumere las limitaciones que impiden el cumplimiento con el requisito original.	<i>La empresa XYZ emplea servidores Unix independientes sin LDAP. Como tales, requieren un inicio de sesión “raíz”. Para la empresa XYZ no es posible gestionar el inicio de sesión “raíz” ni es factible registrar toda la actividad “raíz” de cada usuario.</i>
<b>2. Objetivo</b>	Defina el objetivo del control original; identifique el objetivo con el que cumple el control de compensación.	<i>El objetivo del requisito de inicios de sesión únicos es doble. En primer lugar, desde el punto de vista de la seguridad, no se considera aceptable compartir las credenciales de inicio de sesión. En segundo lugar, el tener inicios de sesión compartidos hace imposible establecer de forma definitiva a la persona responsable de una acción en particular.</i>
<b>3. Riesgo identificado</b>	Identifique cualquier riesgo adicional que imponga la falta del control original.	<i>Al no garantizar que todos los usuarios cuenten con una ID única y se puedan rastrear, se introduce un riesgo adicional en el acceso al sistema de control.</i>
<b>4. Definición de controles de compensación</b>	Defina controles de compensación y explique de qué manera identifican los objetivos del control original y el riesgo elevado, si es que existe alguno.	<i>La empresa XYZ requerirá que todos los usuarios inicien sesión en servidores desde sus escritorios mediante el comando SU. SU permite que el usuario obtenga acceso a la cuenta “raíz” y realice acciones dentro de la cuenta “raíz”, aunque puede iniciar sesión en el directorio de registros SU. De esta forma, las acciones de cada usuario se pueden rastrear mediante la cuenta SU.</i>
<b>7. Validación de controles de compensación</b>	Defina de qué forma se validaron y se probaron los controles de compensación.	<i>La empresa XYZ demuestra al asesor que el comando SU que se ejecuta y las personas que utilizan el comando se encuentran conectados e identifica que la persona realiza acciones con privilegios raíz.</i>
<b>8. Mantenimiento</b>	Defina los procesos y controles que se aplican para mantener los controles de compensación.	<i>La empresa XYZ documenta procesos y procedimientos, y garantiza que no se cambie, se modifique, ni se elimine la configuración de SU y se permita que usuarios ejecuten comandos raíz sin que se los pueda rastrear o registrar.</i>

