Obligaciones de control de proveedores externos

Estándar de seguridad de datos del sector de las tarjetas de pago (PCI DSS)

Versión 13.0 Fecha Septiembre 2023

Obligación de PCI DSS	Descripción	Por qué es importante
1. Lograr el cumplimiento en materia de datos de tarjetas	El proveedor deberá cumplir con las distintas versiones de los estándares de seguridad de datos del sector de las tarjetas de pago publicadas por el Payment Security Standards Council, como PCI DSS, PA-DSS, PCI-P2PE, PCI-PTS y PCI Card Production.	Proteger los datos de los titulares de las tarjetas: El estándar reconocido para lograrlo es PCI DSS y se trata de un requisito normativo sectorial mundial. Los estándares de seguridad PCI son requisitos técnicos y operativos que establece el Payment Security Standards Council para proteger los datos de los titulares de las tarjetas.
2. Certificación de proveedores y vendedores	El proveedor deberá aportar una declaración de cumplimiento para evaluaciones *in situ* (AoC) o, en su caso, un cuestionario de autoevaluación (SAQ), aplicable al alcance de los servicios que preste a Barclays antes del contrato y con una periodicidad anual posteriormente. Esto debe hacerse de acuerdo con los requisitos PCI DSS - véase www.pcisecuritystandards.org/ Si la revisión del AoC plantea cuestiones relativas al alcance de los servicios, la descripción del entorno o el cumplimiento PCI del proveedor, podrá solicitarse y revisarse el informe sobre cumplimiento (RoC) subyacente para obtener más información. Podrá aceptarse un RoC editado si se confirma que el alcance de la certificación PCI se aplica al alcance de los servicios prestados, o si Barclays plantea otras cuestiones tras la revisión del AoC. El proveedor deberá notificar a Barclays los incumplimientos, es decir, en cuanto sea posible y	Pruebas de que un proveedor o vendedor ha alcanzado el cumplimiento en materia de datos de las tarjetas relevante para el alcance de los servicios prestados a Barclays y ha cumplido los requisitos. Pruebas de que la certificación AoC/RoC o SAQ del proveedor tiene que ver con el servicio prestado. Si Barclays se sirve de algún proveedor o vendedor que no cumple el PCI DSS, deberá contactar con el equipo de riesgos de terceros de Visa Europa (agentcompliance@visa.com) por correo electrónico para confirmar que está implementando PCI DSS y ha presentado a Visa Europa un plan de estado de PCI DSS (empleando la plantilla de Visa Europa) para la revisión y aprobación por parte de Visa Europa.

	no más tarde de 30 días después de la fecha en que expiren los documentos de validación.	
3. Reconocimiento del proveedor	El proveedor debe reconocer por escrito a Barclays antes del contrato que se hace responsable de la seguridad de los datos de los titulares de las tarjetas para los siguientes servicios que poseen/almacenan/tratan/ceden o que podrían afectar a la seguridad del entorno de datos de titulares de las tarjetas de Barclays, es decir, servicios de seguridad (como servidores de autenticación), alojamiento web, etc. Los cambios en los servicios prestados deberán reconocerse por escrito a Barclays antes de la implementación de cualquier cambio.	**Desde PCI DSS v3.2.1** **Procedimiento de pruebas para 12.8.2:** Observar los acuerdos escritos y confirmar que incluyen un reconocimiento por parte de los proveedores de servicios en el sentido de que se hacen responsables de la seguridad de los datos de los titulares de las tarjetas que poseen o almacenan, tratan o ceden de otra forma o en la medida en que podrían afectar a la seguridad del entorno de datos de los titulares de las tarjetas del titular. Nota: Junto con el requisito 12.9, este requisito relativo a los acuerdos escritos entre organizaciones y proveedores de servicios pretende promover un nivel uniforme de comprensión entre las partes en torno a las responsabilidades de PCI DSS aplicables. Por ejemplo, el acuerdo puede incluir los requisitos PCI DSS aplicables que deben mantenerse como parte del servicio prestado. **Orientación para 12.8.2:** El reconocimiento del proveedor de servicios evidencia su compromiso con el mantenimiento de una adecuada seguridad de los datos de los titulares de las tarjetas que obtiene de sus clientes. Las políticas y procedimientos internos de los proveedores de servicios vinculados al proceso de captación de sus clientes y las plantillas empleadas para los acuerdos escritos deben incluir una disposición relativa al reconocimiento de PCI DSS aplicable a sus clientes. El método por el cual el proveedor de servicios aporta el reconocimiento escrito debe ser acordado entre el proveedor y sus clientes.

Uso de proveedores terceros/externalización de servicios

Un proveedor de servicios o vendedor podrá utilizar a un proveedor de servicios tercero para almacenar, tratar o ceder datos de titulares de tarjetas en su nombre o para gestionar componentes como routers, firewalls, bases de datos, seguridad física y/o servidores. En ese caso, puede hacer un impacto sobre la seguridad del entorno de datos de los titulares de las tarjetas.

Las partes deben identificar claramente los componentes de los servicios y sistemas incluidos en el alcance de la evaluación de PCI DSS del proveedor de servicios, los requisitos de PCI DSS específicos cubiertos por el proveedor de servicios y cualquier requisito que sea responsabilidad de los clientes de los proveedores de servicios para incluirlos en sus propias revisiones de PCI DSS. Por ejemplo, un proveedor de alojamiento gestionado debería definir claramente cuál de sus direcciones IP se analiza como parte de su proceso trimestral de análisis de vulnerabilidades y qué direcciones IP su cliente tiene la responsabilidad de incluir en sus propios análisis trimestrales.

Los proveedores de servicios tienen la responsabilidad de demostrar su cumplimiento en materia de PCI DSS y pueden tener que hacerlo mediante las marcas de pago. Los proveedores de servicios deben ponerse en contacto con su comprador y/o marca de pago para determinar la validación de cumplimiento adecuada.

Existen dos opciones para que los proveedores de servicios terceros validen el cumplimiento:

1) **Evaluación anual**: Los proveedores de servicios pueden someterse a una evaluación de PCI DSS anual por su cuenta y aportar pruebas a sus clientes para demostrar su cumplimiento; o

2) **Evaluaciones múltiples a demanda**: Si no realizan sus propias evaluaciones de PCI DSS anuales, los proveedores de servicios deben someterse a evaluaciones previa solicitud de sus clientes y/o participar en cada una de las revisiones de PCI DSS de sus clientes, aportando los resultados de cada revisión a los respectivos clientes.

Si el tercero se somete a su propia evaluación de PCI DSS, debe aportar pruebas suficientes a sus clientes para verificar que el alcance de la evaluación de PCI DSS del proveedor de servicios incluyó los servicios aplicables al cliente y que los requisitos de PCI DSS relevantes se examinaron y se determinó su implementación. El tipo de servicio concreto prestado por el proveedor de servicios a sus clientes dependerá de los acuerdos/contratos existentes entre dichas partes. Por ejemplo, prestar la AoC y/o las secciones relevantes del RoC del proveedor de servicios (editado para proteger la información confidencial) podría ayudar a proporcionar la totalidad o parte de la información.

Además, los vendedores y proveedores de servicios deben gestionar y controlar el cumplimiento de PCI DSS de todos los proveedores de servicios terceros asociados con acceso a datos de los titulares de las tarjetas. *Consulte el requisito 12.8 del presente documento para obtener más información.*