PA-DSS: seguridad en aplicaciones de pago

El pasado 8 de noviembre, el PCI SSC[1] publicó una nota de empresa[2] en su página web, donde se expone que un nuevo estándar está siendo añadido a los ya gestionados por el Council: PCI DSS (PCI Data Security Standard) y PED (Pin Entry Device security requirements). Este nuevo estándar ha sido llamado PA-DSS (Payment Application Data Security Standard) y en este artículo se detalla cuál es su propósito, a quién afecta, su relación con PCI DSS y qué se debe hacer para afrontar sus requerimientos.

Miguel Ángel Domínguez Torres

PA-DSS no es un estándar que aparezca de la nada, sino que está basado en las buenas prácticas en aplicaciones de pago **PABP[3] (Payment Application Best Practices)** que VISA proporciona a los proveedores de aplicaciones para asegurar el cumplimiento de un conjunto de medidas de seguridad a la hora de procesar, almacenar o transmitir datos de tarjetas.

Desde 2005, VISA está intentando que los proveedores de aplicaciones de pago utilicen su guía de buenas prácticas PABP, la cual es voluntaria, para implementar medidas de seguridad que tienen como finalidad, por un lado, asegurar que las aplicaciones de pago no almacenan datos prohibidos (banda magnética completa, CVV2 o PINs), y por otro, ayudar al cumplimiento de PCI DSS, a fin de seguir colaborando en la reducción del fraude relacionado con las tarjetas de crédito.

De hecho, los requerimientos de PABP, y por tanto los de PA-DSS (ver **tabla 1**), se derivan de PCI DSS[4], tanto del estándar como de los procedimientos de auditoría[5]. La integración de este nuevo estándar por parte del PCI SSC, era por lógica cuestión de tiempo, lo que implica el soporte por parte de todas las marcas de tarjetas de crédito que integran el PCI SSC (**VISA**, **Mastercard**, **American Express**, **JCB** y **Discover**), el alineamiento con los requerimientos de PCI DSS[6] y además, con PA-DSS el carácter voluntario tenderá a desaparecer, como ya está haciendo VISA, aunque esto último es decisión de cada una de las marcas.

Los cambios entre PABP y PA-DSS se engloban en los siguientes aspectos:

- Eliminar menciones específicas a VISA y a su proceso de cumplimiento. Al igual que PCI DSS, este nuevo estándar define los requerimientos a cumplir, dejando a las marcas desarrollar sus programas de cumplimiento.
- Reorganizar algunas partes del texto, aunque esto es mínimo.
- Clarificar algunos puntos, extendiéndolos o bien adaptándolos a las explicaciones utilizadas en PCI DSS.
- Mejorar las pruebas a realizar de algunos requerimientos, ya que se pasa de un documento de buenas prácticas a un estándar que debe ser más robusto. En este sentido, se ha trabajado bastante el Requerimiento 5: Desarrollar aplicaciones seguras.

Ya en el artículo publicado en SIC[7] Nº 76 se exponía cómo PCI DSS permite reducir el fraude relacionado con tarjetas de crédito, incrementando la seguridad relacionada con estos datos. Esto nos hace pensar entonces sobre el por qué ahora aparece un nuevo estándar relacionado con aplicaciones de pago, cuando PCI DSS dedica el requerimiento 6 precisamente a aspectos de seguridad en el desarrollo de aplicaciones.

Cuando hablamos de PCI DSS, las organizaciones se catalogan en comercios, proveedores de servicios y entidades adquirientes. En función de esto, se determinan las obligaciones respecto a PCI DSS (aunque no debe olvidarse que todas deben cumplir el estándar si almacenan, transmiten o procesan números de tarjetas). No obstante, hay un participante adicional dentro de este juego, los **proveedores/creadores de aplicaciones de pago**. Estas organizaciones no tienen por qué trabajar con números de tarjetas, y de hecho si su función es desarrollar únicamente las aplicaciones de pago para empresas que realizan transacciones con tarjetas, no deberían tratar con datos reales. Por tanto, estrictamente hablando, PCI DSS no les afecta, ya que ni almacenan, ni transmiten, ni procesan datos de tarjetas. Aunque sí que es verdad que el software que venden a sus clientes puede realizar una o varias de estas acciones. Entonces, ¿qué hacer con ellos?

Se necesita alguna forma de garantizar que el software desarrollado por estos proveedores de aplicaciones de pago cumple los requerimientos de seguridad necesarios para que las organizaciones que las utilizan sigan cumpliendo PCI DSS. Es aquí donde PA-DSS entra en juego.

PA-DSS, al igual que PABP tampoco lo hace, no afecta a las aplicaciones propietarias (aplicaciones que no se revenden o distribuyen a terceros), ya sean desarrolladas por personal interno o bien subcontratado.

Si la aplicación desarrollada se utiliza *in-house* entonces los requerimientos a cumplir recaen en los especificados por PCI DSS.

La mayoría de comercios usa aplicaciones de pago comerciales para gestionar las transacciones realizadas con tarjetas de crédito. Estos comercios, y en especial los pequeños, no quieren ni pueden en su mayoría realizar revisiones de las aplicaciones que emplean para garantizar que cumplen los requerimientos de seguridad que PCI DSS exige. PA-DSS, viene a solventar este problema ya que supone poder reducir todo este trabajo a simplemente comprar software certificado por el PCI SSC, igual que puede comprarse un producto certificado Criterios Comunes, igual que exigimos a las empresas con las que trabajamos sellos de calidad ISO9001 o de seguridad ISO27001, o igual que debemos exigir el cumplimiento PCI DSS a empresas a las que se ceden nuestros datos de tarjetas.

Hay que entender que PA-DSS es un impulsor de PCI DSS, ya que exige el cumplimiento de requerimientos de seguridad en aplicaciones de pago que facilitan cumplir los requerimientos PCI DSS (ver **tabla 2**).

El ejemplo más claro es el requerimiento 1 de PA-DSS, el cual exige que las aplicaciones de pago no retengan datos prohibidos (banda magnética completa, CVV2, etc.). Si esto no fuese así, y la aplicación retuviera estos datos, el cumplimiento PCI DSS del comercio se complicaría. El proveedor tendría que adaptar la aplicación o bien el comer-

REQUERIMIENTOS PA-DSS v1.1	
Requerimiento 1	No retener la banda magnética completa, CAV2, CID, CVC2, CVV2 o PIN Block
Requerimiento 2	Proteger los datos de tarjetas almacenados
Requerimiento 3	Proporcionar capacidades de contraseñas seguras
Requerimiento 4	Guardar *logs* de la aplicación
Requerimiento 5	Desarrollar aplicaciones seguras
Requerimiento 6	Proteger las transmisiones inalámbricas
Requerimiento 7	Testear las aplicaciones en busca de vulnerabilidades
Requerimiento 8	Facilitar la implementación de redes seguras
Requerimiento 9	Los datos de tarjetas no deben almacenarse nunca en un servidor conectado a Internet
Requerimiento 10	Facilitar actualizaciones remotas del software de forma segura
Requerimiento 11	Facilitar el acceso a la aplicación de forma segura
Requerimiento 12	Cifrar el tráfico sensible en redes públicas
Requerimiento 13	Cifrar todo el acceso administrativo que no sea por consola
Requerimiento 14	Mantener manuales de instrucciones y planes de formación para clientes, revendedores e integradores.

Tabla 1: Requerimientos PA-DSS

cio debería optar por otro producto, implicando una migración que puede en algunos casos ser verdaderamente traumática.

Pero, ante todo, hay que tener claro que PA-DSS no es lo mismo que PCI DSS.

Si un comercio compra una aplicación de pago que está certificada con PA-DSS, no quiere decir que ya esté hecho todo el trabajo. El comercio aún deberá asegurar que esta aplicación se instala en un entorno que cumple los requerimientos PCI DSS y por supuesto la configuración de la aplicación deberá realizarse de acuerdo a la **Guía de implementación PA-DSS** que debe proporcionar el proveedor para asegurar el cumplimiento PCI DSS en su funcionamiento.

Requerimiento PA-DSS	Requerimientos PCI DSS
Requerimiento 1	PCI DSS 3.2
Requerimiento 2	PCI DSS 3.3, 3.4, 3.5, 3.6
Requerimiento 3	PCI DSS 8.1, 8.2, 8.4
Requerimiento 4	PCI DSS 10.1, 10.2, 10.3
Requerimiento 5	PCI DSS 2.2.2, 6.3, 6.4, 6.5
Requerimiento 6	PCI DSS 1.3.8, 2.1.1, 4.1.1
Requerimiento 7	PCI DSS 6.2
Requerimiento 8	PCI DSS 1, 3, 4, 5, 6.6
Requerimiento 9	PCI DSS 1.3.4
Requerimiento 10	PCI DSS 1.3.9, 12.3.9
Requerimiento 11	PCI DSS 8.3
Requerimiento 12	PCI DSS 4.1, 4.2
Requerimiento 13	PCI DSS 2.3
Requerimiento 14	-

Tabla 2: Mapeo PA-DSS/PCI DSS

¿Y cómo afecta PA-DSS a los distribuidores, integradores o proveedores de servicio de aplicaciones de pago?

Estas empresas no desarrollan la aplicación, pero sí que son responsables de garantizar o proporcionar soporte al comercio, proveedor de servicio o entidad adquiriente en cómo instalar la aplicación en un entorno que cumpla PCI DSS y configurar la aplicación de acuerdo con lo estipulado en la citada Guía de Implementación PA-DSS del proveedor de la aplicación.

Actualmente el estándar se encuentra en estado de borrador y ha sido distribuido a los miembros del PCI SSC, incluyendo empresas QSA y ASV, con el objetivo de recoger los comentarios de todas las partes y poder acabar el proceso de aprobación y publicación, durante el primer trimestre del 2008.

Las empresas que proveen aplicaciones de pago, tendrán que certificar sus productos en este nuevo estándar a través de empresas homologadas como PA QSA[8] por el PCI SSC. El funcionamiento de los PA QSA es el mismo que para el estándar PCI DSS, de manera que en base al procedimiento de auditoría definido por el PCI SSC, se validará el cumplimiento de los requerimientos PA-DSS y se reflejará a través del informe de cumplimiento (ROC – Report On Compliance).

Las empresas que actualmente ya han validado sus aplicaciones con PABP, tendrán que migrar a PA-DSS, aunque esto será fácil dado que PA-DSS se basa en PABP y el propio PCI SSC ha expuesto su voluntad en que esta migración sea poco traumática para los proveedores que ya están cumpliendo PABP.

Tal y como sucede con el PABP de VISA, el PCI SSC publicará sus listas de aplicaciones certificadas[9], lo cual será el punto de partida para que las empresas que requieren estos productos para ejecutar sus procesos de pago con tarjeta, tengan como referencia los productos aceptados por el PCI SSC.

Y mientras tanto, ¿hay que cruzarse de brazos?

La respuesta, como es de suponer, es ***no***. Las organizaciones responsables de cumplir PCI DSS deben asegurar que todos los componentes del entorno que afecta al tratamiento, almacenamiento o transmisión de datos de tarjetas cumplen los requerimientos de seguridad necesarios, y entre ellos está la aplicación de pago. Por tanto, se debe hablar con los proveedores y solicitarles cuáles son sus planes para adaptar el software que utiliza nuestra empresa a los requerimientos establecidos por PA-DSS y acabar siendo una aplicación certificada.

Si nuestro proveedor no nos presenta un plan aceptable conforme ya está realizando acciones en este sentido o existe un plan de acción satisfactorio, nuestra empresa deberá plantearse la opción de sustituir el software por el de un proveedor que sí cumpla PA-DSS (o PABP en la actualidad).

Cualquier empresa (comercio, proveedor de servicio, entidad adquiriente, distribuidor, integrador, etc.) que necesita integrar una aplicación de pago dentro de sus procesos de negocio, lo que tendrá que hacer es consultar la lista de productos certificados (teniendo en cuenta la versión del producto, ya que los cambios de versión implican tener que re-certificar la aplicación a no ser que estos cambios no afecten a los requerimientos establecidos por PA-DSS) y determinar cual de todos se adecua más a sus necesidades.

Pero ya se ha dicho que PA-DSS aún no ha sido publicado. ¿Cómo se puede exigir a los proveedores algo de lo que no disponen? La respuesta está en PABP. Tal y como se ha señalado al inicio del artículo, PA-DSS está basado en PABP. Por tanto, el punto inicial es solicitar a nuestros proveedores qué grado de cumplimiento tienen con PABP.

Por su parte, a los proveedores de aplicaciones de pago, les interesa comenzar a trabajar en el cumplimiento de PA-DSS, por lo que también hacer un *gap analysis* contra PABP, es una forma de adelantar acontecimientos y estar preparados para esta nueva carrera por alcanzar el sello de calidad PA-DSS en sus productos, adquiriendo la ventaja competitiva que todos buscamos.

Para finalizar, hagamos un resumen de los aspectos más importantes de PA-DSS:

- Facilita el cumplimiento PCI DSS a comercios, proveedores de servicio y entidades adquirientes, al intentar garantizar que las aplicaciones de pago no ponen impedimentos para cubrir los requerimientos PCI DSS.
- Quiere seguir impulsando la reducción del fraude relacionado con el proceso de pago con tarjetas mediante requerimientos de seguridad que incorporan los proveedores en sus aplicaciones de pago.
- Implica a los proveedores de aplicaciones de pago, los cuales no tienen por qué estar obligados a cumplir PCI DSS, en el proceso de aseguramiento de todo el ciclo de vida de las transacciones con tarjetas.
- Técnicamente, los requerimientos se derivan de PCI DSS y engloban aspectos de seguridad relacionados con el desarrollo seguro de aplicaciones como son las buenas prácticas establecidas por la OWASP[10] (Open Web Application Security Project), control de acceso, seguridad en comunicaciones, registro de eventos y configuraciones seguras. ■

Miguel Ángel Domínguez Torres
Director de Consultoría
CISSP, CISA, PCI QSA, ISO27001 L.A.
INTERNET SECURITY AUDITORS
mdominguez@isecauditors.com

REFERENCIAS

[1] PCI SSC – https://www.pcisecuritystandards.org/
[2] PCI SSC Strengthens Data Security - https://www.pcisecuritystandards.org/pdfs/11-07-07.pdf
[3] PABP - http://www.visaeurope.com/documents/ais/payment_applications_best_practices.pdf
[4] Estándar PCI DSS - https://www.pcisecuritystandards.org/tech/download_the_pci_dss.htm
[5] Procedimientos de Auditoría PCI DSS - https://www.pcisecuritystandards.org/pdfs/pci_audit_procedures_v1-1.pdf
[6] PA-DSS FAQs – https://www.pcisecuritystandards.org/about/faqs.htm#pa-dss
[7] PCI DSS: ¿Cómo cumplir? – SIC Nº 76
[8] QSA Español – Internet Security Auditors – http://www.isecauditors.com/es/noticias.html#qsa_asv
[9] Lista de aplicaciones de pago validadas PABP - http://www.visaeurope.com/documents/ais/list_of_visa_europe_payment_applications_30112007.pdf
[10] OWASP – http://www.owasp.org