



Vanesa Gil Laredo
 Manager del Departamento de Consultoría. Qualified Security Assessor

Grupo S21sec
 Gestión S.A.

Un paso más en la **seguridad** de las transacciones con tarjetas

El estándar Payment Card Industry Data Security Standard (PCI DSS), cuyo principal objetivo es garantizar la existencia de un marco global consistente para la protección de los datos de titulares de tarjetas, continúa progresivamente su difusión e implantación en el mercado tecnológico y financiero español. El número de comercios, proveedores de servicios y entidades financieras que han realizado una evaluación de cumplimiento del estándar y que se encuentran actualmente en proceso de implantación del mismo ha aumentado considerablemente durante estos últimos años.

La publicación, el pasado día 28 de octubre de 2010, de la versión 2.0 de PCI DSS surge como resultado de la necesaria evolución del estándar y de los requerimientos que lo constituyen, con objeto de adaptar sus exigencias a la evolución de la tecnología y de los riesgos a los que se encuentra expuesta la información y, ante todo, considerar todas aquellas recomendaciones y mejoras que han sido reportadas al PCI Security Standards Council durante el período de feedback por parte de los diferentes agentes implicados en el cumplimiento del estándar.

En el marco de esta continua evolución del estándar PCI DSS, gestionado por el PCI Security Standards Council, y en especial durante estos dos últimos años, se ha procedido a la creación de varios Grupos de Interés (Special Interest Groups), cuyo principal objetivo es realizar un estudio detallado de ciertos aspectos relacionados con el

cumplimiento del estándar, así como recomendar cambios, clarificaciones o mejoras en el mismo.

Los Special Interest Groups (SIGs) existentes en la actualidad son los de Preautorización, Definición del Alcance (Scoping), Virtualización y Wireless. Estos Grupos de Interés prestan un importante apoyo al Grupo Técnico de Trabajo del Security Standards Council en el análisis de los diferentes retos que surgen en relación con la seguridad de los datos de tarjetas, como resultado de las nuevas tecnologías emergentes y de la evolución de los riesgos a los que se encuentran expuestos este tipo de datos.

El Grupo de Preautorización, en primer lugar, se está centrando en aspectos tales como el almacenamiento de datos de autenticación sensibles antes de la autorización de la transacción y el establecimiento de una serie de recomendaciones técnicas a considerar para garantizar la protección de este tipo de datos, indicando cómo deben ser tratados en transacciones de diversa índole. Se está prestando especial atención, entre otros, al concepto de pre-autorización de la transacción y a la problemática específica del sector hotelero.

Los esfuerzos del Grupo de Interés de Definición del Alcance (Scoping), por otra parte, se están centrando en el estudio de las tecnologías de cifrado, *tokenización* y la relación entre PCI DSS y el estándar EMV, así como en ciertas consideraciones para la definición del

alcance al que afecta PCI DSS propiamente dichas. El objetivo de este Grupo de Interés, constituido por cuatro grupos de trabajo diferentes, es clarificar cómo debe ser definido el alcance al que afecta PCI DSS (sistemas que almacenan, procesan o transmiten datos de tarjetas) y cómo se puede reducir dicho alcance, con objeto de facilitar la implantación del estándar.

En relación al cifrado, uno de los requerimientos cuyo cumplimiento resulta en la actualidad más complejo y costoso, el grupo de trabajo se está centrando en la definición de los requisitos que deben cumplir las herramientas que pueden ser utilizadas para el mantenimiento ilegible de datos de tarjetas, así como en el establecimiento de las circunstancias en las que un PAN (Primary Account Number) cifrado podría dejar de ser considerado dato de tarjeta y quedaría, por tanto, fuera del alcance de PCI DSS.

Con respecto a la *tokenización*, el objetivo fundamental del grupo de trabajo es establecer directrices en relación a cómo determinar correctamente el alcance al que afecta PCI DSS en aquellos casos en los que se está empleando alguna solución de este tipo para la securización de datos de tarjetas y a cómo se debe implementar la solución de *tokenización* para garantizar la reducción del alcance.

Por otra parte, el grupo de trabajo referente a Consideraciones sobre el Alcance, tiene como principal objetivo establecer guías concretas sobre cómo definir de manera correcta el alcance al que afecta PCI DSS y

cómo segmentar el entorno de datos de tarjetas de forma que sea posible la reducción del mismo. La definición del alcance suele resultar complicada en entornos complejos debido a la inexistencia de criterios concretos y homogéneos en relación a aspectos tales como la segmentación, por ejemplo. La correcta definición del alcance, que constituye el primer paso a realizar en el marco de cualquier proyecto de adecuación al estándar PCI DSS, resulta imprescindible para garantizar el éxito de dicho proyecto.

En relación al Grupo de Interés EMV, su objetivo fundamental ha sido la revisión de la Guía publicada por el PCI Security Standards Council en relación a la aplicación de PCI DSS en entornos EMV, "*PCI DSS Applicability in an EMV Environment: A Guidance Document*", con objeto de sugerir mejoras en relación al contenido de la misma. Este documento compara los requerimientos de PCI DSS y EMV y señala las similitudes y diferencias existentes entre los mismos, facilitando su comprensión y destacando la necesaria consideración de PCI DSS y EMV como dos estándares complementarios.

Por último, en relación al Grupo de Trabajo de Virtualización, es necesario destacar que en junio de 2011 ha sido publicado el documento "*Information Supplement: PCI DSS Virtualization Guidelines*", en el que se resumen los resultados del trabajo realizado por este Grupo de Interés, destacando los principales escenarios de virtualización, los riesgos a los que se encuentran expuestos este tipo de entornos y una serie de

“
**La consecución del
objetivo último
perseguido con el
estándar PCI DSS es
garantizar la seguridad
de los datos de titulares
de tarjetas**
”

recomendaciones orientadas a garantizar el cumplimiento de los diferentes requerimientos establecidos por PCI DSS.

Resulta indudable el hecho de que estos Grupos de Interés han permitido incrementar la influencia de las organizaciones participantes en el Security Standard Council, considerando su experiencia técnica y de negocio y facilitando la implantación del estándar PCI DSS y su adecuación a la realidad de las organizaciones obligadas a su cumplimiento. El trabajo de estos Grupos de Interés se enmarca dentro de la necesaria evolución del estándar, y permitirá garantizar mayor consistencia en la forma de interpretar y aplicar el estándar por los diferentes Qualified Security Assessors, favoreciendo la consecución del objetivo último perseguido con el estándar PCI DSS: garantizar la seguridad de los datos de titulares de tarjetas. ●