PCI DSS v2.0, la maduración de un estándar

Actualmente nos encontramos en la primera etapa del ciclo de vida definido por el PCI SSC[1] para la gestión de los cambios en las normas PCI DSS y PA DSS. Esto implica que en octubre, tras los *community meetings* que realiza el PCI SSC anualmente en EEUU y Europa, y que este año ha sido acogido por la ciudad de Barcelona como lugar para el evento europeo, la nueva versión de la norma, la 2.0, ha sido publicada para que todos los implicados en su cumplimiento comiencen la adaptación a estos nuevos estándares. Con el objetivo de facilitar el alineamiento a PCI DSS v2.0, el presente artículo recoge los principales cambios que han sido introducidos en la norma y los aspectos a considerar por todos los implicados para adaptar sus procesos de transmisión, almacenamiento y procesamiento de datos de tarjetas de pago.

Miguel Ángel Domínguez Torres

Aunque las normas PCI han sido numeradas en esta nueva versión como 2.0, realmente puede decirse que la actualización desde la versión anterior 1.2.1 a la versión 2.0 no ha introducido cambios mayores que hagan peligrar el trabajo realizado para las implementaciones de PCI DSS que ya existen en la actualidad, aunque por descontado habrá que realizar ciertos ajustes.

Los cambios en la norma han sido organizados en tres tipos: **Aclaraciones**, **Guía Adicional** y **Evolución del Requisito**.

Las Aclaraciones son cambios principalmente del texto con el objetivo de explicar mejor el objetivo deseado con el requisito. En cambio, la Guía Adicional nos introduce ejemplos o definiciones que permitan aumentar el entendimiento o proporcionar mayor información en relación con algún aspecto recogido por el requisito.

Son los cambios de Evolución del Requisito los que introducen verdaderas modificaciones en cómo implementar cada uno de éstos.

La buena noticia es que la gran mayoría de cambios introducidos en la norma PCI DSS v2.0 corresponden a aclaraciones y a guías adicionales. Únicamente existen dos requisitos donde se ha realizado un cambio evolutivo y que luego veremos en detalle. No obstante, es importante prestar especial atención a algunas de las Aclaraciones y Guías Adicionales que ayudarán a implementar mejor la norma.

Uno de los cambios generales más importantes con respecto a las partes implicadas en el cumplimiento de PCI DSS es que la nueva versión de la norma nos habla de **entidades adquirientes y emisores**. Las marcas siempre han incluido a las entidades en la necesidad de cumplimiento de PCI DSS, pero no es hasta esta versión 2.0 donde aparecen reflejadas directamente en el texto de la propia norma como entidades implicadas en el cumplimiento de PCI DSS al almacenar, transmitir y procesar tarjetas de pago.

Adicionalmente, para las entidades emisoras implicadas en el cumplimiento de PCI DSS, siempre ha existido la necesidad de tratar con datos sensibles y almacenarlos como parte de las necesidades del negocio. Esta situación iba en contra de los requisitos de PCI DSS en cuanto a no almacenar datos sensibles (CVV2, PIN, PIN Block, Pista2, etc.) tras el proceso de autorización. Con la nueva versión de la norma las entidades emisoras y otras compañías que proporcionan servicios de emisión aparecen reflejadas en el requisito 3.2 mediante una aclaración donde se expone que estas entidades emisoras pueden almacenar información sensible de autenticación si existe la debida justificación por necesidad del negocio y, por descontado, si estos datos son almacenados de forma segura.

Por desgracia, la frase "almacenados de forma segura" añade un nuevo aspecto de subjetividad a su interpretación práctica. Teniendo en cuenta que el resto de requisitos PCI DSS aplican a los emisores y que el problema real es no poder eliminar la información sensible, es decir, no

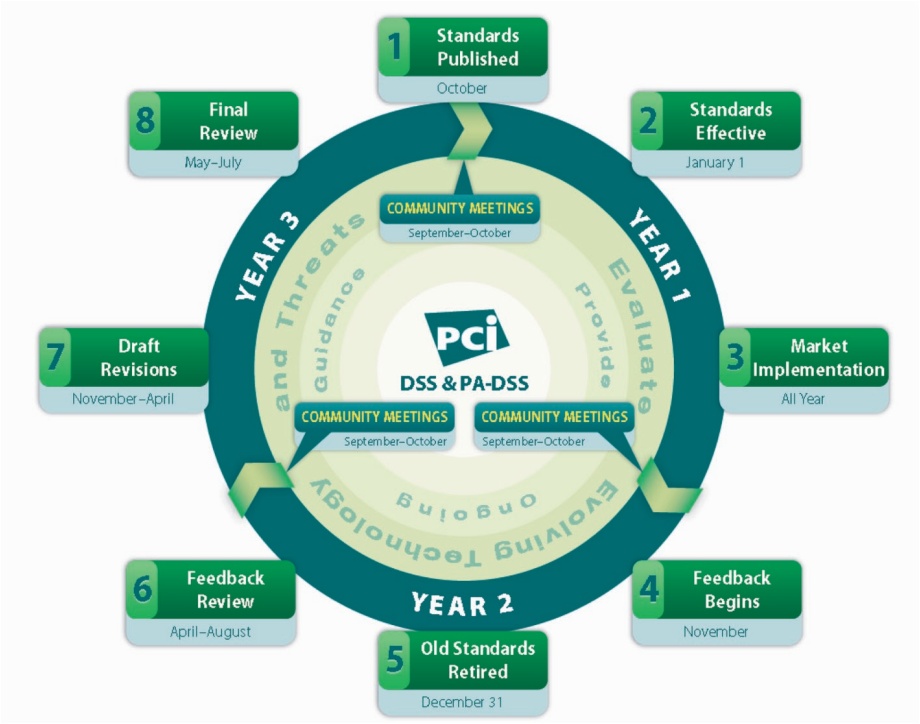

Figura 1.- Ciclo de Vida de los cambios de PCI DSS y PA DSS. [2]

Uno de los cambios generales más importantes con respecto a las partes implicadas en el cumplimiento de PCI DSS es que la nueva versión de la norma habla de entidades adquirientes y emisores. Las marcas siempre han incluido a las entidades en la necesidad de cumplimiento de PCI DSS, pero no es hasta esta versión 2.0 donde aparecen reflejadas directamente en el texto de la propia norma como entidades implicadas en el cumplimiento de PCI DSS al almacenar, transmitir y procesar tarjetas de pago.

poder implementar el requisito tal y como expresa la norma, el objetivo de la frase "almacenados de forma segura" deberá cubrirse mediante el mecanismo de controles compensatorios que la propia norma facilita.

Aún sin salirnos de la parte introductoria de la norma, encontramos otra aclaración importante y que a menudo aparece como duda de todas las empresas que deben implementar PCI DSS: **¿qué debemos proteger?**

En la nueva versión de la norma se introduce el término *Account Data* que substituye al término antes utilizado de *Cardholder data* en relación con la aplicabilidad de PCI DSS. Este cambio ha surgido como necesidad de alinearse con otras normas PCI permitiendo aclarar a su vez que PCI DSS aplica al PAN, la fecha de caducidad, el nombre del titular, el código de servicio, pero también a datos sensibles de autenticación que son la pista completa en la banda magnética, el código de validación CVV2/CVC2/CAV2/CID y el PIN/PIN Block.

Además, se puntualiza que **es el PAN el mínimo dato que define la necesidad de aplicar PCI DSS**. Pero si otros datos como la fecha de caducidad, el titular o el código de servicio están presentes en el entorno de cumplimiento PCI DSS (en inglés CDE – *CardHolder Data Environment*), éstos deberán ser protegidos también mediante los requisitos que define la norma, a excepción (y esto es otra aclaración importante) de los requisitos 3.3 y 3.4, que únicamente aplican al PAN. Por tanto, no es necesario que apliquemos cifrado a los datos que complementan el PAN.

CAMBIOS DE ASPECTOS GENERALES

A la hora de plantearse la necesidad de implementar PCI DSS aparece la tarea inicial de identificar el entorno de cumplimiento sobre el cual se deben aplicar los requisitos de la norma. En este sentido, la nueva versión de ésta recoge algunos cambios dignos de mencionar:

• **Componentes de Sistema.** Ya desde la norma 1.2 se debatía sobre cómo aplicar PCI DSS en entornos virtualizados y, por supuesto, no se ha dejado de aplicar la norma en una de las tecnologías que más se ha implementado en los últimos años. No era sostenible el pasar a soluciones o entornos físicos sólo para cubrir la norma PCI DSS. Esta situación ya fue trasladada al PCI SSC para que lo recogiera en la nueva versión 2.0, apareciendo el concepto de componente virtualizado que implica máquinas virtuales, dispositivos de red virtuales e incluso aplicaciones, escritorios e hipervisores.

De igual forma, se incluye a las personas y procesos dentro de los componentes de sistema afectados por PCI DSS y no sólo a la tecnología.

• **Segmentación de Red.** El aislamiento de los componentes de sistemas que forman parte del entorno PCI DSS es algo que incluye la norma como una recomendación desde versiones anteriores. Este aspecto es algo que los auditores QSA hemos considerado y recomendado en todos los proyectos de implantación PCI DSS, puesto que supone en la mayoría de casos un beneficio por la disminución de coste y esfuerzo de implementación y mantenimiento del cumplimiento con PCI DSS.

El cambio introducido en la versión 2.0 y que ayuda en el diseño de la segmentación del entorno PCI DSS es el hecho de que segmentar no es un concepto que se admita únicamente en lo que se refiere a segmentación física, sino que también es aceptado como segmentación lógica de la red. Siempre desde la base de que la segmentación es correcta si aislamos aquellos componentes de sistema involucrados en el almacenamiento, procesamiento y transmisión de datos de tarjetas, de los que no lo están.

Aun realizando esta aclaración, la segmentación de red seguirá siendo un punto negro en la definición y aislamiento del entorno de cumplimiento PCI DSS, puesto que se deja abierto en la norma qué se considera una segmentación adecuada y se deja a discreción del QSA. Se echa en falta que todas las dudas y recomendaciones que las empresas QSA transmiten en este sentido al PCI SSC queden recogidas en un documento complementario de buenas prácticas en segmentación de red, tal y como se ha hecho con otras tecnologías y conceptos aplicados a PCI DSS.

• **Muestreo.** Las auditorías de PCI DSS se basan habitualmente en muestreo (aunque no es un requisito de la norma), de forma que se puede extraer una conclusión respecto al cumplimiento sin necesidad de revisar todos los componentes y localizaciones incluidos dentro del entorno de cumplimiento PCI DSS.

En este sentido, la versión 2.0 de la norma ha incluido una guía adicional con respecto a cómo se debe realizar dicho muestreo, incluyendo la necesidad de que la muestra sea determinada por el auditor de forma independiente, que primero se deben seleccionar las localizaciones a auditar, y en base a esto, seleccionar los componentes de sistemas dentro de dichas localizaciones y que no se puede seleccionar una muestra de los requisitos de la norma (como estaríamos acostumbrados en auditorías de normas ISO), es decir, que no se puede dejar de validar el cumplimiento de un requisito de la norma.

• **Validación del Entorno PCI DSS.** La tarea de identificar el entorno de cumplimiento PCI DSS no puede ser algo puntual que se realiza durante el proceso inicial de alineamiento con la norma. Debe ser un proceso periódico que identifique cambios en dicho entorno en base a la situación cambiante de las organizaciones. Este aspecto ha sido reflejado como Guía Adicional en la nueva versión de la norma, requiriendo que, como mínimo, anualmente y previo a la auditoría, en el caso de aquellas organizaciones que deban realizarlas, la empresa afectada por PCI DSS deberá confirmar que el entorno de cumplimiento no ha cambiado, o en caso contrario, adecuar la documentación (localizaciones, flujos de datos, etc.) que define dicho entorno a la situación actual. Esta documentación forma parte de la revisión que hará el auditor QSA durante el proceso de auditoría anual.

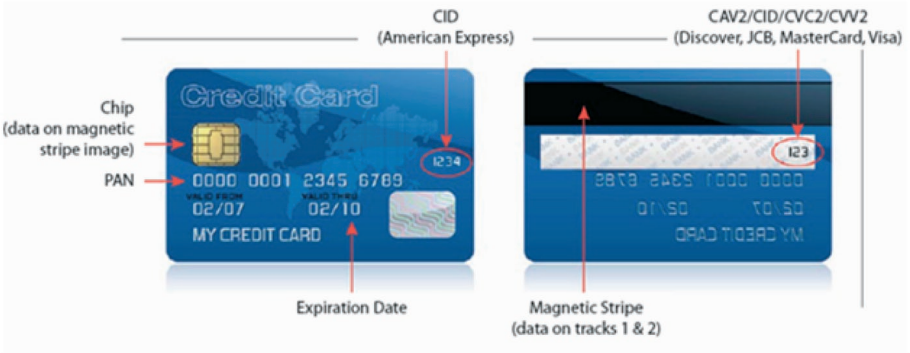

Figura 2.- Datos a proteger por PCI DSS.

En la v2 las entidades emisoras y otras compañías que proporcionan servicios de emisión aparecen reflejadas mediante una aclaración donde se expone que estas entidades emisoras pueden almacenar información sensible de autenticación si existe la debida justificación por necesidad del negocio y, por descontado, si estos datos son almacenados de forma segura. Por desgracia, la frase "almacenados de forma segura" añade un nuevo aspecto de subjetividad a su interpretación práctica.

CAMBIOS POR REQUISITO

Una vez revisados los cambios introducidos en los aspectos generales de la nueva versión de

la norma, si nos adentramos en los cambios que se han realizado en la escala de los distintos requisitos, encontramos que la organización sigue manteniendo los 12 requisitos globales, pero se han realizado una serie de reestructuraciones a nivel de subrequisitos que se dividen o contraen con el objetivo de reorganizar aspectos que quedaban confusos o que aparecían repetidos en distintos lugares de la norma. También se ha hecho una labor importante para alinear los procedimientos de auditoría con los requisitos de la norma a que hacen referencia. Los siguientes puntos resumen por cada requisito global los cambios más destacables:

Requisito 1. Instalar y mantener cortafuegos y su configuración para proteger la información de tarjetas. En general, es un requisito donde se han realizado bastantes aclaraciones, pero cabe destacar que se proporciona una guía adicional en cuanto a no considerar únicamente dispositivos catalogados como cortafuegos o **routers** dentro de la aplicación de las medidas de seguridad recogidas en este requisito, sino que debemos considerar otros componentes de sistema que implementen controles del tráfico desde o hacia redes inseguras.

Otro aspecto importante a remarcar es la aclaración con respecto al requisito 1.3.7 donde en la versión 1.2.1 de la norma se hablaba de ubicar la base de datos en la red interna separada de la DMZ, mientras que en la nueva versión 2.0 se matiza que el requisito aplica a cualquier tipo de almacenamiento de datos de tarjetas y no sólo a bases de datos. Curiosamente este cambio se cataloga como una aclaración cuando el impacto que puede tener sobre las implantaciones de PCI DSS actuales puede ser alto en según qué casos donde se estén guardando datos de tarjetas (siguiendo las medidas que PCI DSS establece en el requisito 3) en servidores de la DMZ que no sean propiamente bases de datos estructuradas.

Requisito 2. No emplear parámetros de seguridad y usuarios del sistema por defecto. El requisito 2.2.1 siempre ha generado dudas al referirse a la implementación de una única función primaria por servidor. Con la nueva versión de la norma se aclara que el objetivo de este requisito es la no coexistencia de funcionalidades que requieran diferentes niveles de seguridad. Y se ponen ejemplos como es el caso de no compartir servidor entre un webserver, DNSs o bases de datos. Además, introduce el concepto de virtualización para remarcar que si los sistemas están virtualizados, cada uno de ellos debe implementar una única función primaria.

Otros cambios menores hacen referencia a tecnologías que se han eliminado, como WPA, al no considerarse seguras, o a la introducción del estándar ISO dentro de las buenas prácticas a seguir para los estándares de *hardening*.

Requisito 3. Proteger los datos almacenados de tarjetas. Es, quizás, el requisito más importante, dado que se centra exclusivamente en los datos de tarjetas, e introduce los aspectos comentados anteriormente en cuanto a la aplicación del cifrado únicamente al PAN y a las excepciones para las entidades emisoras o compañías que soportan procesos de emisión.

En el requisito 3.4 se introduce una nota sobre el uso combinado de técnicas de *hash* y de truncado del PAN. Esta nota alerta sobre el hecho de que es bastante trivial reconstruir un PAN a partir de su *hash* y de su versión truncada. Por tanto se requiere implementar medidas de seguridad adicionales para que no se pueda hacer una correlación entre el *hash* y el dato truncado que permita obtener el PAN completo. Además, se prohíbe utilizar el *hashing* como técnica para substituir la parte truncada del PAN.

Dentro de los requisitos para la gestión de claves, se elimina la necesidad de cambiar las claves criptográficas anualmente y se introduce la necesidad de definir un criptoperíodo (del inglés *cryptoperiod*) que puede ser, por ejemplo, un período de tiempo o una cantidad total de texto cifrado generado por la clave a cambiar. Por tanto, existen más opciones para cumplir este requisito pero siempre dentro de las buenas prácticas definidas por la industria.

Otras aclaraciones importantes, y que facilitan la implementación de los procesos y procedimientos de gestión de claves son las recogidas en el requisito 3.6.6 y 3.6.8. El primero limita la necesidad del *split knowledge* y el control dual a aquellas operaciones de gestión de claves que se hagan en claro y que se realicen manualmente. Y el segundo requisito elimina la necesidad de obtener un formulario firmado por parte de los custodios de las claves, y en su lugar requiere una aceptación formal ya sea electrónica o por escrito.

Requisito 4. Cifrar las transmisiones de datos de tarjetas en redes abiertas o públicas. Se introducen pocos cambios en este requisito. Únicamente es de destacar que deja de ser válida la utilización de protocolo WEP, tal y como se especificaba en la versión 1.2.1, con la fecha límite del 30 de junio de 2010.

Requisito 5. Usar y actualizar regularmente software antivirus. Este requisito introduce únicamente un cambio aclarando, aún más si cabe, que el antivirus debe generar registros de auditoría.

Requisito 6. Desarrollar y mantener de forma segura sistemas y aplicaciones. Es el único punto en la versión 2.0 de la norma donde

REQUISITO	DESCRIPCIÓN
1.3.7	*Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.*
2.2.1	*Implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server.*
3.2	*Do not store sensitive authentication data after authorization (even if encrypted).*
3.3	*Mask PAN when displayed.*
3.4	*Render PAN unreadable anywhere it is stored.*
3.6.6	*If manual clear-text cryptographic key management operations are used, these operations must be managed using split knowledge and dual control.*
3.6.8	*Requirement for cryptographic key custodians to formally acknowledge that they understand and accept their key-custodian responsibilities.*
6.2	*Establish a process to identify and assign a risk ranking to newly discovered security vulnerabilities.*
6.3	*Develop software applications in accordance with PCI DSS, and based on industry best practices, and incorporate information security throughout the software development life cycle*
6.4	*Follow change control processes and procedures for all changes to system components.*
6.5	*Develop applications based on secure coding guidelines. Prevent common coding vulnerabilities in software development processes*
7.1.3	*Requirement for a documented approval by authorized parties specifying required privileges.*
11.4	*Use intrusion-detection systems, and/or intrusion-prevention systems to monitor all traffic at the perimeter of the cardholder data environment as well as at critical points inside of the cardholder data environment, and alert personnel to suspected compromises.*
12.3.10	*For personnel accessing cardholder data via remote-access technologies, prohibit copy, move, and storage of cardholder data onto local hard drives and removable electronic media, unless explicitly authorized for a defined business need.*

Figura 3.- Requisitos referenciados en el artículo.

Dentro de los requisitos para la gestión de claves criptográficas, se elimina la necesidad de cambiarlas anualmente y se introduce la de definir un criptoperíodo que puede ser, por ejemplo, un período de tiempo o una cantidad total de texto cifrado generado por la clave a cambiar. Por tanto, existen más opciones para cumplir este requisito pero siempre dentro de las buenas prácticas definidas por la industria.

aparecen cambios de tipo Evolución del Requisito. Concretamente, el cambio se introduce en el requisito 6.2 donde se requiere que las vulnerabilidades identificadas durante el proceso de identificación de nuevas vulnerabilidades deben ser clasificadas según el riesgo que introducen y basándose en las buenas prácticas definidas por la industria, como por ejemplo CVSS[3], y/o siguiendo las clasificaciones que proporcionan los proveedores del software afectado por la vulnerabilidad.

Esta nueva medida se ha definido como opcional hasta el 30 de junio de 2012 en que pasará a ser obligatoria.

Además, se han realizado cambios importantes en la estructura de los requisitos para facilitar su entendimiento, eliminando redundancias y agrupando conceptos principalmente en lo que se refiere a aplicaciones internas, aplicaciones externas, aplicaciones web y aplicaciones no web. Esta reestructuración se centra en la inclusión de la seguridad en el ciclo de vida del desarrollo recogido en el requisito 6.3, el control de cambios recogido en el requisito 6.4 y el desarrollo en base a guías de codificación segura recogido en el requisito 6.5.

Requisito 7. Restringir el acceso a la información de tarjetas según "need-to-know". El cambio que se ha producido en este requisito es en relación con relajar la exigencia del requisito 7.1.3, ya que en lugar de requerir un formulario firmado por dirección, se requiere la aprobación por escrito o electrónicamente de las partes autorizadas. Este tipo de cambio se ha realizado en otros requisitos de la norma con la finalidad de eliminar, por un lado la necesidad de la firma por escrito cuando hoy día se realiza la mayoría de autorizaciones a nivel electrónico, y por otro, no limitar las autorizaciones a personal directivo sino al personal debidamente.

Requisito 8. Asignar un único ID a cada persona con acceso a computadores. Una aclaración curiosa que se realiza en este requisito es con respecto a la autenticación de dos factores donde se añade una nota explicando el concepto de autenticación de doble factor con el objetivo de que no sea incorrectamente implementado y se adopten soluciones en las que en lugar de aplicar autenticación de dos factores se aplica autenticación de un factor dos veces, como es el caso de utilizar dos contraseñas.

Requisito 9. Restringir el acceso físico a la información de tarjetas. Es un requisito donde se han realizado aclaraciones menores en relación a términos como "*onsite personnel*", "*visitor*" y "*media*".

Requisito 10. Auditar y monitorizar todos los accesos a los recursos de red y datos de tarjetas. Se ha echado de menos en esta nueva versión una revisión y definición a fondo de los tipos de eventos que deben quedar registrados en las trazas de auditoría para facilitar su implementación, puesto que es, junto con la protección de los datos de tarjetas almacenadas, uno de los requisitos más complejos de abordar en cualquier implantación de PCI DSS.

Los cambios se han concentrado en aclarar los requisitos relacionados con la sincronización de tiempo, no centrándose en NTP como tecnología de sincronización (aunque realmente sea el protocolo más extendido para realizar estas tareas) y concretando cómo debe ser y estar protegida la arquitectura de sincronización.

Requisito 11. Testear de forma regular la seguridad de los sistemas y procesos. Los escaneos Wi-fi han sido ampliados para remarcar la necesidad de disponer de un proceso documentado que defina cómo se realizarán estos escaneos trimestralmente, añadiendo otros métodos además del escáner Wi-fi o IDS/IPS Wi-fi que incluyen la inspección física o tecnologías NAC.

En el caso de los escaneos internos hay una aclaración importante en relación a cuándo se considera que un escaneo interno ha sido superado con éxito. En este sentido, la nueva versión de la norma dice que se puede dar como válido el escaneo interno si se han corregido todas las vulnerabilidades catalogadas como "altas" cumpliendo con el requisito 6.2, es decir, según la clasificación de riesgo que se introduce en esta nueva versión de la norma. Esto supone una ventaja, puesto que uno de los problemas que nos encontramos habitualmente con los escaneos internos es el alto volumen de vulnerabilidades que aparecen cuando realizamos este tipo de escaneos sobre la red interna. Por tanto, esto supone un incentivo para implementar el proceso de clasificación de vulnerabilidades antes de la fecha límite del 30 de junio de 2012 marcada por la norma PCI DSS v2.0.

La aclaración más significativa en cuanto a facilitar la implementación de sistemas IDS/IPS en el entorno PCI DSS es el hecho de que el requisito 11.4 pasa de hablarnos de monitorizar todo el tráfico dentro del entorno de cumplimiento PCI DSS a concretar la necesidad de monitorizar únicamente el tráfico a nivel de perímetro y en puntos considerados críticos.

Requisito 12. Mantener una política que gestione la seguridad de la información para todo el personal. Con la finalidad de aclarar qué se considera un análisis de riesgos formal se han introducido ejemplos que hacen referencia a metodologías como OCTAVE[4], ISO 27005[5] o NIST SP 800-30[6], quedando más claro que es necesario un proceso documentado que genere resultados comparables y reproducibles.

Además, se ha suavizado el requisito 12.3.10 donde se prohibía en el acceso remoto a datos de tarjetas el hecho de poder copiar, mover o almacenar en local y medios removibles esta información. Ahora se permite siempre que esté justificado por una necesidad de negocio y debidamente autorizado, protegiendo la información en base a los requisitos de PCI DSS.

Conclusiones

La nueva versión de la norma da un paso más en la madurez del estándar PCI DSS, proporcionando más detalle y mayor claridad y precisión en muchos aspectos de su implementación y auditoría, suavizando algunos requisitos e incorporando la necesidad de clasificar las vulnerabilidades en base al riesgo. Sin embargo, seguimos sin tener documentación oficial por parte del PCI SSC en relación con temas tan importantes como las prácticas aceptadas para la segmentación de red que permita el aislamiento del entorno PCI DSS. De nuevo, se inicia un ciclo de mejora en que todas las partes implicadas en el almacenamiento, transmisión y procesamiento de datos de tarjetas de pago deberán alinearse a los cambios introducidos por la nueva versión PCI DSS 2.0. ■

La aclaración más significativa en cuanto a facilitar la implementación de sistemas IDS/IPS en el entorno PCI DSS es el hecho de que el requisito 11.4 pasa de hablarnos de monitorizar todo el tráfico dentro del entorno de cumplimiento PCI DSS a concretar la necesidad de monitorizar únicamente el tráfico a nivel de perímetro y en puntos considerados críticos.

Miguel Ángel Domínguez Torres
PCI QSA, PA QSA, CISA, CGEIT, CISSP
ISO 27001 L.A., SBCI, BS 25999 L.A.
Director del Departamento de Consultoría
INTERNET SECURITY AUDITORS
mdominguez@isecauditors.com

REFERENCIAS

[1] **PCI Security Standards Council (PCI SSC)** http://www.pcisecuritystandardscouncil.org
[2] **Ciclo de Vida de los Cambios en PCI DSS y PA DSS** https://www.pcisecuritystandards.org/pdfs/3_at-a-glance_lifecycle_for_changes_to_pcidss_andpa-dss.PDF
[3] **Common Vulnerability Scoring System (CVSS)** http://www.first.org/cvss/
[4] **OCTAVE** http://www.cert.org/octave/
[5] **ISO 27005** http://www.27000.org/iso-27005.htm
[6] **NIST SP 800-30** http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf