PCI DSS v3.0: afrontando el nuevo reto

El pasado 7 de noviembre salió la versión 3.0 de PCI DSS. Desde que se publicara la primera de este estándar allá por el 2006, han pasado ya con esta nueva publicación 5 versiones en las que el estándar ha ido evolucionando, derivado de la necesidad de eliminar ciertas ambigüedades en aquellos requisitos que permitían interpretaciones diferentes, tanto en QSAs como en el personal de las organizaciones, cubrir carencias que se han ido detectando conforme se aplica el estándar en el día a día, e ir aumentando el nivel de seguridad de aquellos sistemas que procesan, transmiten o almacenan datos de tarjeta. En las siguientes líneas hace una revisión de aspectos importantes de esta nueva versión, al tiempo que se bridan algunos consejos útiles para afrontarlos.

Carmen de Alba Muñoz

Tras un análisis de la nueva versión de la norma se puede observar que aquellas empresas que ya han adaptado su negocio a PCI DSS versión 2.0 deberán orientar sus esfuerzos en complementar aspectos relativos a documentar y reforzar los procesos y procedimientos ya implantados, o lo que es lo mismo, en mejorar la eficacia de los mismos, siendo razonable y asumible para dichas empresas la inversión de tiempo y recursos que esto les supone.

El motivo por el que esta nueva versión hace más hincapié en documentar procesos, procedimientos de operativa diaria o instrucciones de trabajo, viene provocado por la madurez alcanzada por el estándar en los más de siete años de vida, donde ha pasado de focalizarse inicialmente en los aspectos más técnicos que se debían cubrir para proteger los datos de tarjeta, a perfeccionar los procesos relacionados con la gestión y mantenimiento de la seguridad de dichos datos. Esta evolución de la norma es fruto también de la retroalimentación que el PCI SSC recibe de todos los implicados en el ciclo de vida definido para las normas PCI.

Como empresa QSA uno de los problemas más habituales que nos encontramos cuando revisamos o asesoramos en el cumplimiento con PCI DSS es que departamentos como TI, Sistemas u Operaciones, no invierten el tiempo suficiente en documentar, bien porque no lo ven prioritario, o bien porque faltan recursos para poder realizar esta tarea. Pero tenemos que ser conscientes de que es difícil que el personal de una organización trabaje de la misma manera o de que se pueda retener el conocimiento cuando las personas dejan las empresas, si no existen procesos y procedimientos documentados que indiquen cómo se deben realizar las tareas. En este sentido, lo que como QSAs nos encontramos en muchas auditorías PCI DSS (y más aún si es la primera vez que la organización se certifica) es que o falta documentación por generar, o la documentación no cubre los requisitos solicitados por el estándar.

Figura 1.

Un fallo muy común que se encuentra en las auditorías cuando una empresa se certifica por primera vez, es en relación a los procesos y procedimientos de control de cambios. Durante la auditoría, es bastante normal que se encuentren sistemas que no están correctamente bastionados o les falte por instalar alguna actualización. En consecuencia, el administrador, de buena fe, ejecuta el cambio sin abrir petición alguna, incumpliendo el estándar. Este hecho es una señal de que la empresa no ha terminado de asimilar la necesidad y el motivo de implantar un procedimiento de control de cambios.

Otro ejemplo común sucede durante la revisión del correlador de *logs*. El auditor QSA identifica eventos que, de acuerdo a la configuración del correlador, generan una alerta, que en muchas ocasiones es un falso positivo (por ejemplo, que el IDS o el WAF detecten un XSS porque aparece la palabra "Alert" en algún *log* de una aplicación web y realmente se corresponde con un tráfico válido) y se descarta sin establecer un criterio, registro y justificación de por qué se descarta. En este sentido, la nueva versión incluye el nuevo requisito 10.6.3, en el que se deberá desarrollar un procedimiento de seguimiento de alertas del correlador, desde que éste lanza la alerta hasta que se cierra.

EL CONTROL DE ACCESO LÓGICO

Otro de los procedimientos que más se refuerza en esta nueva versión es el vinculado con el *control de acceso lógico*. Con el nuevo estándar es necesario de acuerdo al requisito 7.1.1, identificar los roles y los recursos a los que cada rol (usuarios, administradores, etc.) puede acceder, y los privilegios que tiene asignados, teniendo en cuenta que se deben asignar el mínimo número de privilegios necesarios para desempeñar su trabajo. Relacionado con el control de acceso, el requisito 3.3 requiere elaborar un listado de roles, que por necesidades del negocio, necesitan visualizar el PAN completo (cualquier rol que no aparezca en este listado debe visualizar el PAN enmascarado). Esto afectaría a aplicaciones, ficheros, *logs*, etc.

Para cubrir los requisitos anteriores, junto con el nuevo requisito 2.4 que requiere un inventario de activos a nivel de hardware y software que componen el alcance de PCI DSS, y también el nuevo requisito 9.1.1 que requiere un inventario de todos los TPVs físicos (Point of Sale – POS en inglés); la solución que desde nuestra experiencia como QSA facilita este cumplimiento es lo que denominamos la **Cardholder Data Environment Matrix (CDEM).** Desde versiones anteriores de la norma esta herramienta ya facilita la gestión unificada de distintos requisitos y ahora se fortalece aún más su utilidad al aumentarse los requisitos de la norma 3.0 que solicitan mantener inventarios de distintos tipos.

La CDEM consiste en elaborar una serie de matrices organizadas por tipo de componente (hardware, software, comunicaciones, aplicaciones, etc.), que se relacionan entre ellas y que vinculan a cada componente los requisitos PCI DSS que les aplican. Elaborando una CDEM consistente, se cubren los requisitos anteriormente mencionados (7.1.1, 3.3, 2.4, 9.1.1), así como el requisito 3.1 que requiere una política de retención de datos de tarjeta, verificar que en el mapa de red no se ha olvidado incluir ningún componente, o pintar los flujos de datos de tarjetas, como exige el nuevo requisito 1.1.3.

La CDEM se puede construir con una hoja de cálculo, en el caso de entornos de datos de tarjeta pequeños, o mediante herramientas como bases de datos o CMDBs en entornos más complejos.

En resumen, se trata de una matriz que, aparte de ser una herramienta poderosa para controlar los componentes del entorno, permite tener un conocimiento importante de la función de cada uno de los sistemas y ubicaciones por donde pasan los datos de tarjeta.

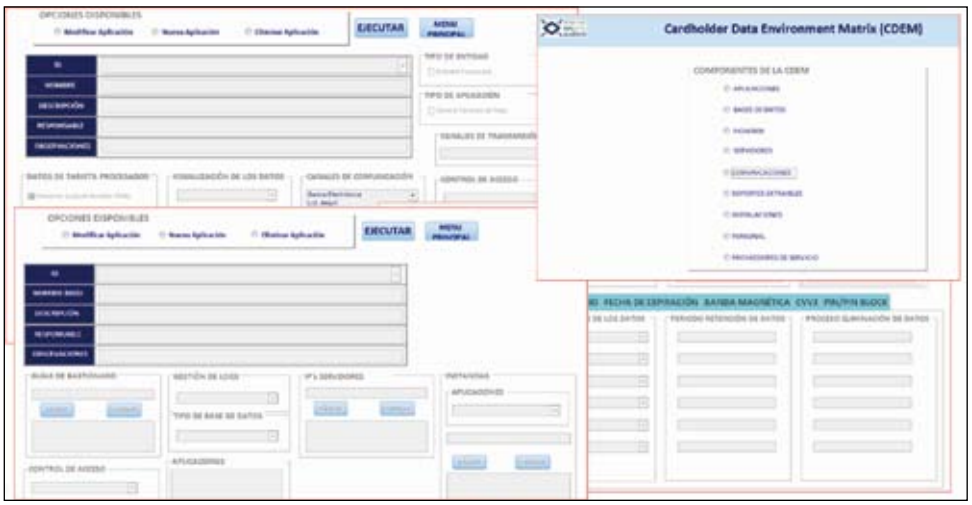

Figura 2.- CEDEM (Cardholder Data Environment Matrix).

OCHO NUEVOS REQUISITOS

Otra novedad importante a destacar en la versión 3.0 es que se han introducido 8 nuevos requisitos, que por el impacto que tiene su implantación, serán buenas prácticas hasta julio de 2015, fecha en la cual pasarán a ser requisitos de obligado cumplimiento. Estos requisitos se pueden agrupar en cuatro apartados:

1.- Desarrollo Seguro de Aplicaciones

Vuelve al *top ten* de vulnerabilidades la "pérdida de autenticación y gestión de sesiones" (esta vulnerabilidad aparecía en la v1.2.1 del estándar, y en la v2 desapareció) y también se incluye el "manejo inseguro de datos sensibles en memoria" como nueva vulnerabilidad a verificar en las aplicaciones que procesan los datos de tarjeta. Hay que tener en cuenta que cuando un atacante trata de robar datos de tarjeta, no se va a ir en primer lugar a robar los datos en aquellos repositorios en los que éstos se almacenan cifrados. Antes de atacar la base de datos, tratará de buscar aquellas ubicaciones donde el dato aparece en claro, en memoria (como puede ser este caso) o en ficheros temporales que se generan tras producirse un error en la aplicación o en el sistema, donde se suelen volcar los datos que en ese momento estaban en memoria.

El requisito al que no hay que esperar a julio de 2015, relacionado con el desarrollo seguro de aplicaciones, es el 6.5.c, que establece la obligación de impartir cursos de formación de técnicas seguras de desarrollo de aplicaciones para evitar las vulnerabilidades más comunes en dichos desarrollos y donde se explique cómo los datos sensibles son manejados en memoria; exigiéndose formalmente un registro de asistencia a estas formaciones. Apoyarse en empresas de seguridad especializadas en auditoría de aplicaciones para dar estos cursos es una opción muy recomendable ya que estas empresas tienen una visión más amplia de las vulnerabilidades que las aplicaciones suelen tener y su trabajo les exige estar al día de los nuevos riesgos y ataques que se producen en la actualidad. Contando con personal con amplia experiencia en revisión de código o subcontratando empresas especializadas y definiendo un buen programa de formación en desarrollo seguro de aplicaciones –que se actualice de acuerdo a las novedades de la industria y a las amenazas emergentes– el riesgo de pasar a producción aplicaciones con vulnerabilidades se reduce considerablemente.

Relacionado con la seguridad de las aplicaciones web públicas, el requisito 6.6 abre la opción a instalar una solución técnica que detecte y prevenga ataques web, como podría ser un IPS inspeccionando el tráfico por delante de los frontales web. Aunque la norma no especifica la solución tecnológica a implantar, lo que sí que debe cumplir la solución que se adopte es que monitorice constantemente el tráfico, detecte y prevenga ataques web.

2.- Test de Intrusión

Los tests de intrusión internos y externos a nivel de red y a nivel de aplicación son una herramienta muy valiosa a través de la cual una organización puede detectar los puntos débiles de sus sistemas. La nueva versión 3.0 introduce varios cambios en relación a los test de intrusión, añadiendo requisitos que pretenden homogeneizar la ejecución de estas pruebas técnicas en todas las organizaciones. Un test de intrusión no es sólo lanzar una herramienta. Sin una metodología que identifique cómo determinar el alcance de la auditoría, los criterios de auditoría, los aspectos a auditar, cómo hacerlo, los resultados que se deben generar, o las competencias profesionales que deben tener las personas que realizan estas tareas, las posibilidades de que los resultados no sean los esperados aumentan considerablemente. Es por este motivo que las modificaciones en el requisito 11.3 requieren que todos los test de intrusión que se ejecuten en entornos PCI DSS deberán seguir una metodología basada en las buenas prácticas de la industria (NIST SP800-115, Open Source Security Testing Methodology Manual (OSSTMM), OWASP (para aplicaciones web), etc.). Hasta julio de 2015 en que el requisito será de obligado cumplimiento, los requisitos de la versión 2.0 serán los que se deban seguir para realizar los test de intrusión.

Otro nuevo requisito, el 11.3.4, incluye la obligación de verificar la validez de la segmentación utilizada para reducir el entorno PCI DSS. La norma nos dice que la segmentación y el aislamiento del entorno PCI DSS es una recomendación, y hasta esta nueva versión no incluía ningún control que permitiera validar que dicha segmentación se había hecho adecuadamente. Realmente, la experiencia constata que la segmentación es siempre una de las medidas a implementar aunque sea una recomendación ya que ninguna empresa está interesada en incluir toda su organización dentro del alcance de PCI DSS, dado el esfuerzo considerable que conlleva su implantación. La manera más efectiva de verificar la validez y eficacia de esta segmentación es ejecutando un test de intrusión, ya que durante la ejecución de estos tests se van a identificar todas las máquinas dentro del alcance y se validarán las medidas de aislamiento implementadas para separar el ámbito PCI DSS de otros ámbitos considerados inseguros. Y esto precisamente es lo que nos pide el requisito 11.3.4. Puesto que validar la segmentación es un punto crítico para poder cerciorarnos de que el entorno PCI DSS está correctamente definido (si no está correctamente definido podemos caer en el error de implantar PCI DSS a medias, lo que invalidaría todo el esfuerzo realizado en caso de tener un incidente), es recomendable contar con empresas expertas en realizar este tipo de pruebas, ya que su conocimiento y pericia a la hora de ejecutar estos tests se basa en las metodologías, estándares y buenas prácticas de la industria. Sin dejar de lado que además aportan una visión independiente que en muchos casos es difícil de conseguir por personal interno de la organización.

3.- Terminales Punto de Venta (TPV) Físicos

La versión 3.0 viene con la incorporación de nuevos activos al entorno PCI DSS. Estos activos son los TPVs físicos que pueden encontrarse en cualquier comercio de cara al público y para los que se solicita implementar controles de seguridad como los que especifica el requisito 9.9 con el objetivo de evitar modificaciones físicas; por ejemplo, instalando *skimmers* o por sustitución física del terminal, y que permitan capturas de datos fraudulentas. De acuerdo al requisito 9.9.1, se deberá elaborar un inventario de todos los TPVs, incluyendo marca, modelo, ubicación y número de serie. Para gestionar este inventario, como ya se ha comentado anteriormente, se puede utilizar una CDEM.

Complementando el requisito anterior, el 9.9.2 requiere establecer un programa de revisiones periódicas (definiendo cómo, cuándo y quién), en las que se verifique que estos dispositivos no han sido sustituidos o manipulados.

Nº	PCI DSS Requisito – Julio 2015	Explicación
6.5.10	Broken Authentication and Session Management.	Se debe verificar que las funciones relacionadas a autenticación y gestión de sesiones se implantan correctamente para evitar que terceros se puedan hacer con identificadores de sesión, contraseñas en claro, etc. con el objetivo de robar cuentas de usuarios.
8.5.1	Service providers with access to customer environments must use a unique authentication credential (such as a password/phrase) for each customer environment.	Se pretende aplicar la misma política de control de acceso de los usuarios internos a los proveedores otorgando cuentas individuales a cualquier proveedor que acceda al entorno PCI DSS. El proveedor debe ser consciente de que está prohibido el uso de cuentas genéricas y compartidas, independientemente que el acceso sea puntual o habitual.
9.9	Protect point-of-sale (POS) devices that capture payment card data via direct physical interaction with the card from tampering and substitution. **NOTE:** This includes card-reading devices used in card-present transactions (that is, card swipe or dip) at the point of sale. This requirement is not intended to apply to manual key-entry components such as computer keyboards and POS keypads.	Los comercios deben poner controles adicionales a los TPVs físicos que permitan gestionarlos de forma segura. Se trata de evitar que ladrones roben el TPV para estudiarlo y ver cómo acceder a él, cambiar partes del TPV (como lector de tarjetas, teclado, etc.) modificadas para capturar los datos, etc. También se recomienda utilizar las buenas prácticas antiskimming publicadas en la web del PCI SSC.
11.3	Develop and implement a methodology for penetration testing that: • Is based on industry-accepted penetration testing approaches (for example, NIST SP800-115). • Includes coverage for the entire CDE perimeter and critical systems. • Includes testing from both inside the network, and from outside of the network attempting to get in. • Includes testing to validate any segmentation and scope-reduction controls. • Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in Requirement 6.5. • Defines network-layer penetration tests to include components that support network functions as well as operating systems. • Includes review and consideration of threats and vulnerabilities experienced in the last 12 months. • Specifies retention of penetration testing results and remediation activities results.	Se debe desarrollar una metodología para la ejecución del test de intrusión. Esta metodología, debe basarse en las buenas prácticas de la industria como por ejemplo, NIST SP800-115, Open Source Security Testing Methodology Manual (OSSTMM), OWASP (para aplicaciones web), etc., tener en cuenta todo el entorno de datos de tarjeta, validar la segmentación, revisar las vulnerabilidades que hayan aparecido en los últimos 12 meses, especificar el periodo de retención de los resultados de los tests de intrusión y las actividades derivadas del plan de remediación, y al menos verificar que los sistemas no son vulnerables a las vulnerabilidades que aparecen en apartado 6.5.x (inyecciones SQL, buffer overflow, etc.).
12.9	Additional requirement for service providers: Service providers acknowledge in writing to customers that they will maintain all applicable PCI DSS requirements to the extent the service provider handles, has access to, or otherwise stores, processes, or transmits the customer's cardholder data or sensitive authentication data, or manages the customer's cardholder data environment on behalf of a customer.	Los proveedores de servicios deben comprometerse a firmar por contrato con sus clientes, a que son conscientes de que trabajan con datos de tarjeta, y que se comprometen a cumplir con todos los requisitos de PCI DSS que les aplique, para poder asegurar que los datos de tarjeta, son procesados, transmitidos y/o almacenados en un entorno seguro de acuerdo a lo establecido por PCI DSS.

Figura 3.- Buenas prácticas hasta 2015.

Y por último, para concluir este conjunto de requisitos, el 9.9.3 requiere diseñar cursos de formación y concienciación a aquellos empleados que trabajan con los TPVs, en los que se les enseñe a detectar comportamientos sospechosos de personas que intenten modificar los dispositivos, colocando elementos que permitan capturar los datos de tarjetas, o suplantarlos por completo; e incluso evitar que atacantes suplanten a las empresas de mantenimiento de este tipo de dispositivos. Es decir, los comercios deberán establecer una serie de protocolos en los que el personal que trabaja con los TPVs deberá tener conocimiento y autorización previa del reemplazo del TPV en su totalidad o de alguna pieza. Lo que se pretende evitar son ataques de ingeniería social.

Aunque no es un requisito específico de la norma, nuestra experiencia como empresa QSA y de seguridad nos hace aconsejar que para validar la efectividad de estos cursos de formaciones y de los procesos definidos se realicen pruebas de ingeniería social, de forma que una empresa especializada valide que el personal que trabaja a diario con los TPVs está correctamente formado y concienciado para detectar intentos de manipulación y sustitución de los dispositivos.

Todos estos requisitos ayudan a evitar incidentes como el sucedido por ejemplo en octubre de 2012, donde la cadena de librerías norteamericana "Barnes & Noble" detectó que al menos 63 PIN PADs en diferentes estados fueron manipulados para robar datos de tarjeta.

4.- Gestión de Proveedores de Servicio

Si se busca en Internet, se pueden encontrar numerosos robos de datos personales y de datos de tarjeta, entre muchos otros, a organizaciones, cuyo origen se produjo en sus proveedores. Uno de los puntos débiles y más peligrosos de cualquier organización es el modo de gestionar la seguridad en los contratos con sus proveedores. No tiene ningún sentido que una organización haga el gran esfuerzo en cumplir con PCI DSS y que sus proveedores no cumplan, o su nivel de seguridad sea menor. En este sentido, la nueva versión 3.0 añade el requisito 12.9 para proveedores de servicio, también como buena práctica hasta julio de 2015, en el que éstos se corresponsabilizan por contrato a procesar, almacenar o transmitir los datos de tarjeta de acuerdo a PCI DSS, estando obligados a proporcionar las evidencias suficientes que permitan verificar el cumplimiento de los requisitos que les afecten. Además, los proveedores deberán hacer un esfuerzo adicional en la gestión de cuentas de usuario y contraseñas de sus clientes, teniendo prohibido poner la misma contraseña para distintos clientes.

Para gestionar esto, recomendamos en primer lugar identificar los requisitos que afectan a cada proveedor (req. 12.8.5) y definir las responsabilidades del proveedor y las de la organización. En paralelo, se deben definir los tipos de proveedores que pueden dar servicio a la organización (acceso lógico a los datos, acceso físico al entorno pero no a los datos, etc.). Y en base al tipo de proveedor y a los requisitos que le apliquen, redactar una serie de cláusulas adicionales que se anexarán al contrato. Estas cláusulas deben especificar, de la forma más clara posible, las responsabilidades PCI DSS que el proveedor se compromete a cumplir. Incluir una cláusula genérica del tipo "y me comprometo a cumplir con PCI DSS" puede desencadenar en malos entendidos y futuros litigios. Por ejemplo, para un proveedor de software le quedarán más claros los requisitos de seguridad que tiene que cumplir la aplicación si se incluyen en el contrato que si se incluye que "la aplicación debe ser segura". Con esto, se asegura que el proveedor se corresponsabiliza a dar el servicio de acuerdo a PCI DSS (req. 12.8.2 y req. 12.9).

CONCLUSIONES

Como hemos ido viendo en esta pequeña introducción a los cambios en la nueva versión 3.0, la revisión cubre diversos frentes: 1) reforzar los requisitos de la versión 2.0, 2) aclarar el significado de requisitos que han dado lugar a interpretaciones distintas y a veces opuestas, entre los propios QSAs y entre las organizaciones, 3) proteger los datos de tarjeta de nuevos riesgos que van surgiendo. Y en definitiva, seguir con la mejora continua que permita reducir los incidentes de seguridad que puedan provocar robos masivos de datos de tarjetas.

Pensar que PCI DSS es un estándar exclusivamente técnico es el primer error en el que se suele caer. Evidentemente es una norma técnica que aplica a unos sistemas, aplicaciones y componentes de red, y que son implementados y mantenidos por el departamento de TI. Pero todo esto es una pieza más del conjunto, y los cambios que PCI DSS requiere vienen dados por la necesidad de definir e implementar un proceso continuo de seguridad que proteja los datos de tarjetas de pago, lo cual afecta a toda la organización.

Es por esto que ahora el reto que nos pone la versión 3.0 no se encuentra tanto en la parte técnica como si lo hace en la parte documental y la administrativa, tratando de aumentar la seguridad en los procesos de gestión del cumplimiento. Muchas veces el robo de la información no sucede por la falta de controles técnicos sino por deficiencias en la aplicación y gestión de los mismos. ■

Carmen de Alba Muñoz
Responsable Consultoría Madrid
CISM, CISA, PCI QSA, PCI PA-QSA
INTERNET SECURITY AUDITORS

REFERENCIAS

- PCI DSS v3.0
  https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf
- PCI DSS Summary of Changes v2.0 to v3.0
  https://www.pcisecuritystandards.org/documents/PCI_DSS_v3_Summary_of_Changes.pdf