PCI Card Production, aspectos a destacar

El estándar PCI Card Production, vigente desde mayo del 2013, se ha creado para cubrir una necesidad patente desde tiempo atrás. Antes de su definición, los fabricantes de tarjetas de pago debían cumplir con el estándar PCI DSS [1], que no encajaba del todo con sus especificaciones funcionales. Por este motivo, las diferentes marcas de tarjetas de pago exigían a este tipo de empresas cumplir con su propia normativa, lo que les obligaba a seguir varios programas de seguridad para un mismo propósito, el de producir tarjetas. Hay que tener en cuenta que este tipo de empresas tienen un riesgo muy alto, ya que producen un material muy sensible (tarjetas de pago). De esta forma y con la inclusión de la PCI Card Production, se ha conseguido un único programa de seguridad, enfocado a las especificaciones requeridas por este tipo de empresas. En este artículo se procede a analizar las características más destacables de este nuevo estándar, haciendo énfasis en los puntos que pueden ser más problemáticos para las entidades afectadas en su cumplimiento, en base a la experiencia de Internet Security Auditors en la adecuación de las medidas de seguridad existentes a los nuevos requerimientos.

Guillem Fàbregas

Alcance

Antes de empezar con los requerimientos concretos del estándar, hay que definir muy bien los **sistemas, instalaciones y procedimientos bajo su alcance**. Este alcance variará entre el estándar de seguridad lógica ("*Card Production Logical Security Requirements v1.0*." [2]) y el de seguridad física ("*Card Production Physical Security Requirements v1.0*" [3]), como vemos a continuación.

Respecto al **alcance del estándar de seguridad lógica**, éste lo conformarán los sistemas y procedimientos de negocio relacionados con las actividades de producción de tarjetas de pago, siendo estos la Preparación de Datos, Pre-personalización y Personalización. Las actividades realizadas en estos procedimientos de negocio pueden incluir programación de tarjetas, generación de PIN, PIN *mailers* y distribución de los materiales generados.

Vemos a continuación una explicación de cada uno de estos procedimientos, que corresponderán con las diferentes redes del entorno de cumplimiento:

• **Preparación de datos:** en este procedimiento se engloban las actividades desde que los datos de tarjetas llegan al productor de tarjetas, a través de entidades bancarias o de centros de procesado autorizados, hasta que los datos son pasados a la red Personalización. En estas actividades se proporciona a los datos el formato adecuado para la personalización de tarjetas.

• **Pre-personalización:** procedimientos de inicialización de chips de las tarjetas con claves propias de la entidad productora o del fabricante del chip, pero sin la introducción de datos de clientes o de titulares.

• **Personalización:** procedimientos de introducción de los datos de titulares de las tarjetas en las mismas, incluyendo el estampado del CVV2 (o equivalente) y otros datos, grabación de la banda magnética y del chip EMV, generación de PIN, envío de PIN (PIN *mailers*), distribución de tarjetas, etc.

En cuanto al **alcance del estándar de seguridad física,** éste será mayor, y lo conformaran las instalaciones en las que se realicen los siguientes procedimientos:

- Fabricación de tarjetas.
- Estampado y codificación de tarjetas.
- Personalización.
- Iniciación de chip y pre-personalización.
- Incrustación de chip.
- Personalización de chip.
- Almacenamiento de tarjetas.
- Envíos de datos y tarjetas.

Seguridad lógica

En el documento "*Card Production Logical Security Requirements v1.0*." se describen los requerimientos de seguridad lógica del estándar PCI Card Production a aplicar en los sistemas e infraestructuras de los productores de tarjetas.

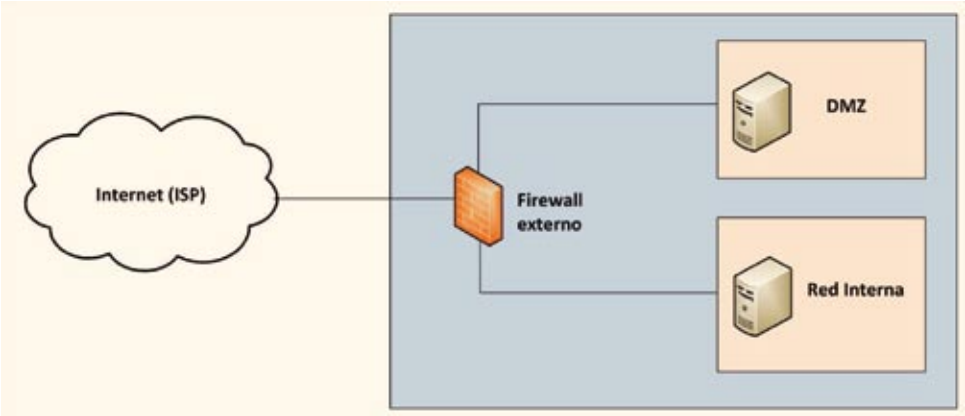

Figura 1

Distribución de Red

El primer punto a destacar es el tema de la segmentación de red. Mientras el estándar PCI DSS sólo requiere de la implementación de una DMZ para gestionar las conexiones des-

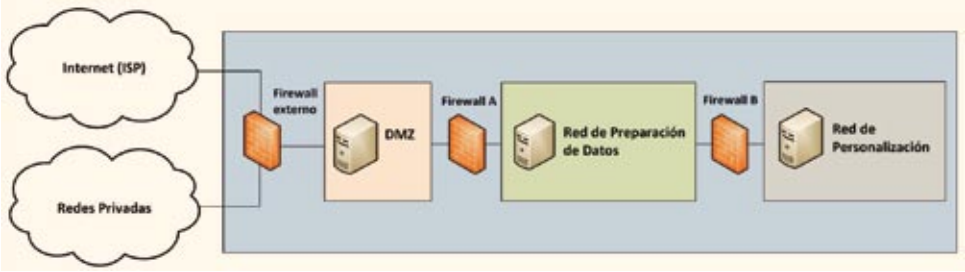

Figura 2

de el exterior, y la existencia de una correcta segmentación lógica entre la red interna con dicha DMZ a través de un cortafuegos (como se puede ver de manera simplificada en la **Figura 1**), **el nuevo estándar es más estricto en este sentido**.

Para empezar, el estándar PCI Card Production cuenta con dos redes internas diferenciadas dentro del entorno: la red de Preparación de Datos y la red de Personalización, como se puede ver en el diagrama de la **Figura 2**. Es importante recalcar que estas dos redes pueden estar en el mismo segmento de red, eliminándose la segmentación entre ellas, pero sólo si están situadas en la misma zona o red de alta seguridad.

Además, debe existir segmentación (lógica y física) entre todas estas redes**,** y un mismo *firewall* no puede realizar las dos funciones, por lo que se requiere un mínimo de dos cortafuegos, en la mayoría de los casos tres, para aplicar una correcta segmentación.

Hay que tener en cuenta que los requerimientos de distribución de red comentados aplican a entidades que realizan actividades de Preparación de Datos y/o Personalización. Por lo tanto, si una entidad se encarga solo de la inicialización de los chips de las tarjetas (Pre-Personalización) pero en ningún caso recibe los datos de los titulares o efectúa la personalización, la aplicación de estos requerimientos no será necesaria.

Entrada y preparación de datos

La recepción de datos se produce a través de entidades bancarias, con las que la entidad fabricante de tarjetas actúa con rol de proveedor. Es responsabilidad del fabricante de tarjetas el velar para que la recepción de datos se realice según los requerimientos del estándar, por lo cual se debe acordar con el banco las metodologías de envío/recepción de la información.

Este envío/recepción de información **se debe realizar con el cifrado de los datos**, y nunca con la información sensible en claro. Existen algunas herramientas comerciales que implementan el envío/recepción de este tipo de datos a partir de canales seguros en redes X.25, o en redes basadas en IP (como *frame relay* o MPLS), que la mayoría de bancos tienen implementadas. Hay que constatar que por el momento, la mayoría de entidades bancarias aún utilizan envíos seguros a través de redes tradicionales (como la X.25), aunque es de esperar que progresivamente se vaya migrando a soluciones basadas en redes de nueva generación a través de Internet, como MPLS.

Como lo más habitual es que cada entidad bancaria cuente con su propio método de envío de datos, será necesario acordar con cada una de ellas qué método de envío de datos puede asumir y bajo qué circunstancias.

Una vez recibidos los datos, será necesaria la preparación de los mismos según las necesidades de almacenamiento y producción. Para ello, se aplicará una conversión de datos según los formatos establecidos en cada caso.

Algoritmo	TDES	RSA	Curva Elíptica	DSA/D-H	AES
Tamaño mínimo de la clave en bits	112	1024	160	1024/160	128

Figura 3

Algoritmo	TDES	RSA	Curva Elíptica	DSA/D-H	AES
Tamaño mínimo de la clave en bits	112	1024	160	1024/160	-
	168	2048	224	2048/224	-
	-	3072	256	3072/256	128
	-	7680	384	7680/384	192
	-	15360	512	15360/512	256

Figura 4

Almacenamiento y producción

Otro aspecto a destacar y que marca una gran diferencia con el estándar PCI DSS es la necesidad, por parte de los productores de tarjetas, de almacenar datos sensibles durante cierta cantidad de tiempo (el estándar PCI DSS prohíbe el almacenamiento de dichos datos salvo justificación demostrable de negocio), y todas las medidas de seguridad específicas para su almacenamiento que eso conlleva. En el caso de los productores de tarjetas, ya se asume que en todos ellos existe una necesidad de negocio para el almacenamiento de dichos datos, por lo que el estándar incluye los requerimientos de seguridad necesarios.

El tiempo de conservación de los datos de los titulares de las tarjetas es de 30 días a partir de la fecha de personalización, y dicha retención deberá efectuarse siempre en una zona de alta seguridad (HSA). Esta fecha de inicio de retención puede variar respecto a la fecha de recepción, ya que el tiempo de preparación de los datos antes de la personalización de tarjetas no está incluido en estos 30 días. Además, en caso de tener una justificación por escrito del banco responsable de los datos, éstos se pueden retener durante un máximo de seis meses. Esta justificación tendrá vigencia sólo durante dos años, por lo que será necesaria su renovación periódica.

Lo que se debe tener en cuenta es que **los datos se deben eliminar de las máquinas personalizadoras en el momento en el que la tarjeta se acaba de producir**. Esta medida es necesaria debido a que las máquinas personalizadoras pueden ser "básicas" a nivel de software, por lo que pueden no disponer de las medidas de seguridad para el almacenamiento en forma segura de dichos datos (opciones de cifrado, parches de seguridad, etc.). Además, recordemos que estos equipos tienen un coste de adquisición muy elevado y un periodo de amortización largo, y es por ello que es posible que tecnológicamente puedan tener un riesgo elevado a las vulnerabilidades en el largo plazo.

En este punto hay que ser muy cuidadoso a la hora de adecuarse con el estándar, ya que existen máquinas de personalización que funcionan a través de ficheros TXT en texto plano como entrada de datos, que son almacenados en su *back office* mientras dura la personalización de tarjetas, y que posteriormente hay que eliminar. Así pues, para lograr una correcta adecuación al estándar, se debe asegurar que dichos ficheros son eliminados:

- De manera manual por los empleados encargados de la personalización en el caso de que la máquina no permita el borrado automático (opción poco recomendable, ya que debido a descuidos lo normal es que algunos ficheros con datos permanezcan en ellas, creando serias inconformidades respecto al estándar).
- Mediante procedimientos automáticos independientes del *firmware* de la máquina como *scripts* de borrado, que nos faciliten la tarea y nos ahorren descuidos innecesarios.

Volviendo a los sistemas y equipos que pueden tratar datos durante su preparación y almacenarlos durante 30 días o más a partir de la fecha de personalización, estos deben aplicar en todo momento métodos de cifrado, salvo cuando los datos deban procesarse en claro para la personalización de tarjetas.

Los tamaños mínimos de los algoritmos de cifrado que se deben implementar tanto para el almacenamiento de datos confidenciales como para su transporte deben coincidir con los de la tabla de la **Figura 3**.

Para los profesionales de la seguridad, estos requerimientos mínimos pueden parecer insuficientes para proteger datos de alta sensibilidad, por lo que parece obvio que a medida que el estándar avance y se desarrollen nuevas versiones del mismo, estos se irán endureciendo, aunque de momento éstos son los tamaños aceptados.

Por último, y para evitar la recuperación de datos sensibles mediante técnicas forenses en los dispositivos que la han contenido, **se deben implementar metodologías de borrado seguro de la información, como desmagnetización, sobre-escritura o destrucción física de los dispositivos**.

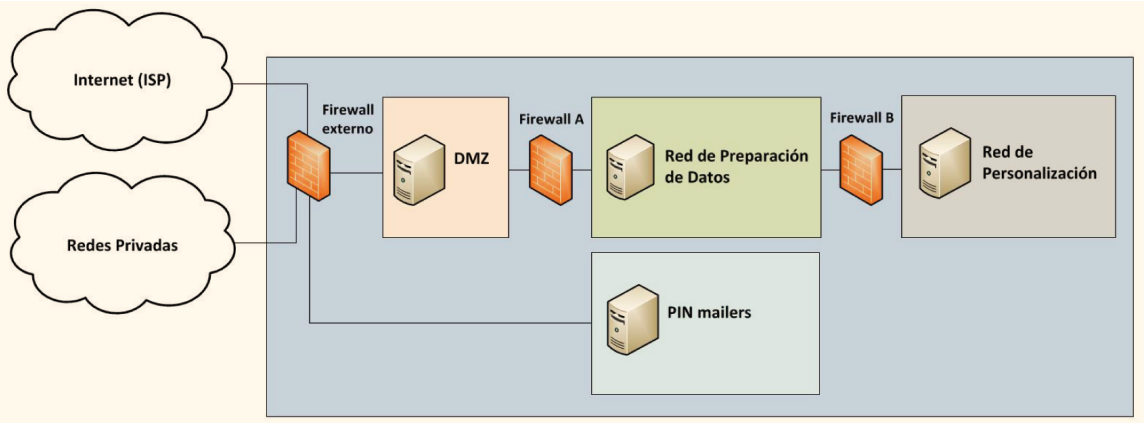

Figura 5

La gestión de claves

El siguiente aspecto a destacar por su complejidad es el que hace referencia a la gestión de las claves de cifrado. El estándar hace especial énfasis en este punto, por lo que dedica 2 apartados enteros a hablar sobre el tema.

La primera consideración a tener en cuenta es la necesidad de **conocimiento dividido para todas las claves de cifrado (*split knowledge*)**, con la única excepción de los criptogramas (fragmento de mensaje cifrado cuyo significado resulta ininteligible hasta que se descifra con el conocimiento de un patrón determinado).

Los requerimientos mínimos de los algoritmos de cifrado para el almacenamiento o transmisión de dichas llaves deben ser como mínimo de la misma robustez que las llaves protegidas. Las equivalencias entre la robustez de las diferentes llaves para cumplir con este requerimiento se pueden comprobar en la tabla de la **Figura 4**.

Además, los equipos encargados de gestionar dichas claves deben permanecer en áreas de alta seguridad (HSA), con fuertes controles de acceso y vigilancia: uso de cámaras de seguridad, aisladas de otros segmentos de red, etc.

Se debe **nombrar oficialmente a un *Key Manager***, que será el responsable de las operaciones de gestión de las mismas. Este responsable deberá llevar un control de todas las claves generadas, guardar registros de todas las acciones realizadas, gestionar todos los procedimientos de carga, etc.

Deberán existir para cada clave sus correspondientes custodios, los cuales deben ser oficialmente designados y conscientes de sus responsabilidades. Estos custodios deben ser siempre empleados con contrato vigente con la organización, ya que su responsabilidad es muy elevada. Como custodios, deben ser poseedores de una parte de cada clave de cifrado, y asegurarse que los otros custodios no puedan acceder a su parte (almacenándolas bajo caja fuerte, realizando periódicamente auditorías de control sobre sus claves, etc.). Además, es necesario que los custodios de una clave estén formados por empleados de diferentes departamentos, para reducir la posibilidad de actos fraudulentos.

La generación de dichas claves debe realizarse en un dispositivo de hardware HSM conforme al estándar PCI PTS, o en su defecto a la FIPS 140-2. Una vez generadas, la parte correspondiente a cada custodio se debe distribuir de manera segura, bajo cifrado si se transmiten electrónicamente, o bajo sobres cerrados y confidenciales si se transmiten en soportes físicos.

En el momento en que cada custodio cuenta con su correspondiente parte de la llave, éstas se deben cargar en los dispositivos HSM encargados de efectuar las operaciones criptográficas entre la empresa de producción de tarjetas y la entidad bancaria correspondiente. Para este procedimiento es vital asegurarse que ninguno de los demás custodios pueda llegar a conocer la clave completa. Para ello, las instalaciones de dicho HSM deben ser inspeccionadas por el *Key Manager*, para asegurarse que las cámaras de vigilancia funcionan pero no pueden registrar la llave en su introducción en el HSM, que no existan dispositivos espías en los equipos, que todo esté debidamente configurado, etc.

Cuando el *Key Manager* ha comprobado que las medidas de seguridad en la sala del HSM son correctas, cada uno de los custodios debe introducir su parte de la llave en el equipo de manera individual, sin que ninguna otra persona pueda llegar a ver parte de dicha llave. Para ello, lo más recomendable es que cada custodio entre en la sala del HSM solo y por turnos, y efectúe las operaciones necesarias en el equipo.

Hay que recordar que para entornos de este tipo, se debe utilizar una clave de cifrado diferente para cada cliente con el que se intercambien datos de tarjetas de pago (entidades bancarias). Por lo que cada vez que se debe realizar un cambio de claves para alguno de los bancos (porque la clave ha caducado, se ha corrompido, etc.), se deberán repetir los procedimientos comentados.

Como se ha podido observar, los requerimientos de gestión de claves de cifrado del estándar son muy estrictos y requieren de la participación de diferente personal, por lo que es necesario que el *Key Manager* actúe de líder y gestione correctamente todos los empleados implicados en el proceso. Además, hay que recordar que los custodios no siempre serán técnicos de IT o empleados con altos conocimientos informáticos, por lo que se les debe simplificar y detallar el procedimiento y su participación para la correcta efectividad y agilidad de éste.

PIN *mailers*

Otro aspecto a destacar es la distribución de PIN de las tarjetas de pago a las correspondientes entidades bancarias para que éstas las hagan llegar a sus respectivos clientes. Si el productor decide realizar este procedimiento, hay que sumar unos cuantos requerimientos a los comentados hasta el momento.

Esta distribución se podrá realizar de manera física, bajo sobres cerrados y con una gestión conforme a la normativa (proveedores de distribución fiables, con fuertes medidas de control y protección del material, etc.) o de manera electrónica.

Si se efectúan procedimientos de distribución electrónica de PIN y por tanto existe una red de PIN *mailers*, ésta debe ser **una red segmentada de las demás redes descritas** a través de un cortafuegos dedicado, de una forma similar a la vista en el diagrama de la **Figura 5**.

Desde el equipo de distribución electrónica de PIN sólo debe realizarse esta tarea, y su almacenamiento y distribución debe seguir los mismos procedimientos y algoritmos de cifra-

do que los otros datos sensibles del entorno (ya comentados en la tabla anterior). En esta red de distribución no deben existir en ningún caso otros datos relativos a las tarjetas producidas (PAN, fechas de caducidad, nombre del cliente, etc.).

Además, la sala donde se encuentre el sistema de distribución de PIN, ya sea para impresión de sobres con los PIN para su distribución física como para los equipos de distribución electrónica, también debe ser una zona de alta seguridad (HSA), con todas las medidas de seguridad que esto conlleva, y que son resumidas a continuación.

Seguridad física

Además de los requerimientos de seguridad lógica, el estándar destaca por sus **fuertes medidas de seguridad física**, que se recogen en un documento aparte, el "*Card Production Physical Security Requirements v1.0*".

Los requerimientos de seguridad física recogidos son muy estrictos, mucho más que en la PCI DSS, y su correcta aplicación puede resultar en fuertes inversiones por parte de las empresas productoras. Hay que tener en cuenta que la pérdida o robo de tarjetas u otro material sensible en las instalaciones del productor ocurren bajo su propia responsabilidad, por lo que es imprescindible llevar un fuerte control de las existencias, así como introducir procedimientos de control para evitar robos, tanto de origen interno como externo.

A continuación se muestra una pincelada de los requerimientos de seguridad física más destacables de dicho estándar:

- Las instalaciones donde se produzcan tarjetas deberán tener implementadas fuertes medidas de seguridad y control en todas las posibles entradas. Además, se deben incluir puertas con contactos magnéticos o eléctricos conectados a alarmas de seguridad para todas las entradas.
- Las zonas de alta seguridad (HSA) deberán tener las entradas controladas por cabinas de acceso individuales o *mantrap doors*, gestionadas por un sistema central de acceso, siendo responsabilidad del Responsable de Seguridad el aprobar los permisos de acceso de cada empleado. Además, deberán existir sensores de presencia con contadores de personas para dichas zonas, de manera que si el contador de personas está a cero (nadie en la sala) y se detecta movimiento, salten las alarmas.
- Deben existir procedimientos de control estrictos sobre el material y los dispositivos introducidos en estas áreas de alta seguridad, estando prohibida la entrada de cualquiera que no sea necesario para la personalización de tarjetas (*pendrives*, móviles, PDA, etc.). La introducción de equipos o material en estas áreas deberá realizarse a través de accesos diferentes a los del personal.
- Se debe llevar control de cada uno de los empleados que tengan acceso a áreas sensibles, siendo necesario que estos lleven tarjetas de identificación visibles en todo momento. Además, se deberán controlar las tarjetas asignadas y los accesos permitidos para cada empleado. En caso de que un visitante o empleado de terceros deba tener acceso a las zonas de alta seguridad, habrá de existir una aprobación explícita del Responsable de Seguridad, y se deberán guardar registros de sus visitas a dichas zonas. Lo más recomendable es facilitar en estos casos una tarjeta de visitante, aprobar los permisos temporales a las áreas concretas a las que necesite acceder, y almacenar de manera electrónica los accesos a dichas áreas.
- Deberán existir guardias de seguridad, que no tengan acceso a las áreas sensibles, y que controlen a partir de cámaras de vigilancia todas las áreas sensibles y entradas a la entidad.
- Se debe llevar un estricto control sobre las tarjetas fabricadas y las personalizadas, de manera que quede muy bien definido el empleado responsable de las tarjetas en cada momento, y el número concreto de tarjetas de una determinada marca que quedan bajo su responsabilidad.
- Para la producción de tarjetas con la tecnología *Contactless*, utilizadas en pagos sin contacto a través de ondas de radio-frecuencia, la entidad debe asegurar que fuera de la zona de alta seguridad no se detecten ondas de este tipo de tarjetas. Para ello, es necesario aislar la HSA, así como efectuar escaneos de radio-frecuencias periódicos en el exterior de estas zonas, para comprobar que realmente no se detecta ningún tipo de señal de este tipo. La recomendación principal es efectuar los escáneres WiFi también requeridos por el estándar junto con estos escaneos de radio-frecuencia, de manera que se ahorre tiempo y recursos.

Conclusiones

Como se ha podido comprobar a lo largo de este artículo, en el que se han introducido las consideraciones prácticas más relevantes sobre el nuevo estándar PCI Card Production, éste es muy estricto y de laborioso cumplimiento, incluso más que la PCI DSS, ya de por sí muy estricta. Además, **representa una inversión considerablemente elevada** para las empresas que decidan emprender el negocio de la producción de tarjetas.

Para las empresas que ya llevan tiempo dentro del sector, y que hasta hace poco debían cumplir con las normativas de las diferentes marcas, la inversión es obviamente menor, aunque también deben emplear una serie de recursos para adecuarse al nuevo estándar. Esto es debido a que hasta hace poco existían matices y diferencias entre los requerimientos de los programas a aplicar, que se han modificado/ajustado en la redacción del nuevo estándar, y por lo tanto, esto supone una revisión de los requerimientos por parte de las empresas. En estos casos, lo más recomendable es **efectuar un análisis de brechas sobre la PCI Card Production**, localizando los aspectos a abordar para conseguir la completa adecuación con el estándar.

A pesar de las inversiones necesarias para adecuarse con el estándar, **el nivel de seguridad resultante de su aplicación es muy elevado**, e intenta minimizar los flancos de seguridad tanto externos como internos, para evitar el robo o sustracción tanto de datos sensibles como de las mismas tarjetas de pago y materiales asociados. Además, hay que tener en cuenta que **las marcas de tarjetas requieren de su cumplimiento**, y exigen **auditorías anuales** sobre dicho estándar para dar su aprobación a la entidad productora para la utilización de sus tarjetas. En caso de no superar dichas auditorías, **las marcas pueden retirar la certificación a las entidades para la producción de sus tarjetas** hasta que se arreglen las no conformidades detectadas. Esta prohibición puede ser temporal o permanente, y es obvio que puede resultar catastrófica en términos económicos para dichas entidades.

Por tanto, es muy importante que las entidades afectadas por su cumplimiento estén familiarizadas con sus requerimientos, los interpreten correctamente y se propongan cumplirla lo antes posible, de manera que se eviten graves problemas en un futuro. ■

Guillem Fàbregas Margenats
Consultor en Seguridad
INTERNET SECURITY AUDITORS
CISA, CISM, PCIP

REFERENCIAS

[1] Payment Card Industry Data Security Standard v2.0
https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf

[2] Card Production Logical Security Requirements v1.0
https://www.pcisecuritystandards.org/documents/PCI_Card_Production_Logical_Security_Requirements_2013.pdf

[3] Card Production Physical Security Requirements v1.0
https://www.pcisecuritystandards.org/documents/PCI_Card_Production_Physical_Security_Requirements_2013.pdf