Amazon y PCI DSS: guía práctica para alinear AWS en un entorno de datos de tarjeta de pago

Cuando por consideraciones técnicas o administrativas se opta por delegar la gestión de ciertos componentes o de la totalidad de la infraestructura informática de la organización a un tercero, es imprescindible garantizar que los niveles de seguridad que dicho tercero aplicará serán iguales o mejores a los que la propia organización mantiene. Adicionalmente, si el entorno delegado debe cumplir con requerimientos legales o estándares de la industria, la responsabilidad de parte y parte debe quedar claramente estipulada en términos contractuales. Este es el caso de los servicios de Amazon en la nube (Amazon AWS) y el cumplimiento de PCI DSS. A pesar que el proveedor (CSP) ofrece una gran cantidad de servicios para configurar la infraestructura de forma segura, es finalmente el cliente el responsable de la seguridad de los datos y de la configuración de los servicios que se ejecutan sobre la capa provista por Amazon. Por otro lado, la complejidad en el despliegue de una solución de estas características implica un alto conocimiento tanto de la plataforma del CSP como de la aplicación de los controles de PCI DSS. Finalmente, en este artículo se ha plasmado el despliegue técnico de controles empleando las funcionalidades provistas por un CSP como Amazon.

David E. Acosta Rodríguez

Con el auge actual de los servicios en la nube (*cloud computing*), muchas empresas se están planteando migrar total o parcialmente su arquitectura informática a proveedores de *cloud* (CSP–Cloud Service Provider) para aprovechar las ventajas particulares de este modelo en su negocio, dentro de las que se encuentran –por sólo nombrar algunas– la optimización de los tiempos de despliegue de nuevos servicios, mejoras en el rendimiento y la disponibilidad, independencia del hardware, virtualización, almacenamiento y desempeño escalable, etc.

No obstante, una de las variables que puede afectar la decisión de migración a este modelo es el nivel de **seguridad** que ofrecerá el entorno en la nube respecto al entorno original desplegado en el cliente. En función del proveedor del servicio y del modelo a implementar (IaaS, PaaS, SaaS, etc.) son muchos los interrogantes que deben ser analizados antes de proceder: ¿la plataforma escogida garantiza la privacidad de los datos de los clientes? ¿Hasta qué punto el entorno en *cloud* contratado se puede adaptar a los requerimientos de cumplimiento? ¿Cuáles serán las responsabilidades del proveedor y de la empresa en la implementación y la gestión de los controles de seguridad? ¿En el caso de un incidente de seguridad, quién será el responsable de la gestión?

Y si –adicional a los controles de seguridad propios– la empresa que busca un proveedor de servicios en la nube almacena, procesa y/o transmite datos de tarjetas de pago, deberá garantizar el cumplimiento del estándar de seguridad de datos de tarjetas de pago (*Payment Card Industry Data Security Standard* o PCI DSS) en el entorno de *cloud,* labor para nada fácil que requiere de la asignación específica de responsabilidades entre el cliente y el proveedor del servicio.

Para gestionar este último punto, en febrero de 2013 el PCI SSC (*Payment Card Industry Security Standards Council*, que es la organización que desarrolla los estándares de seguridad de datos de tarjetas de pago [1]) publicó el documento "*Information Supplement: PCI DSS Cloud Computing Guidelines*" [2]) en el cual se ofrecen una serie de consideraciones prácticas a la hora de escoger, implementar y gestionar un entorno de cumplimiento parcial o totalmente desplegado en la nube, incluyendo controles de seguridad física, documental, lógica y administrativos, en donde el CSP debe ser capaz de proveer a sus clientes de:

– Documentación de cumplimiento de PCI DSS de su entorno (como el **Attestation of Compliance** – AoC o secciones relacionadas del Report on Compliance – RoC) incluyendo la fecha de la revisión.

– Evidencia documentada de componentes de sistemas y servicios incluidos dentro de la validación de PCI DSS.

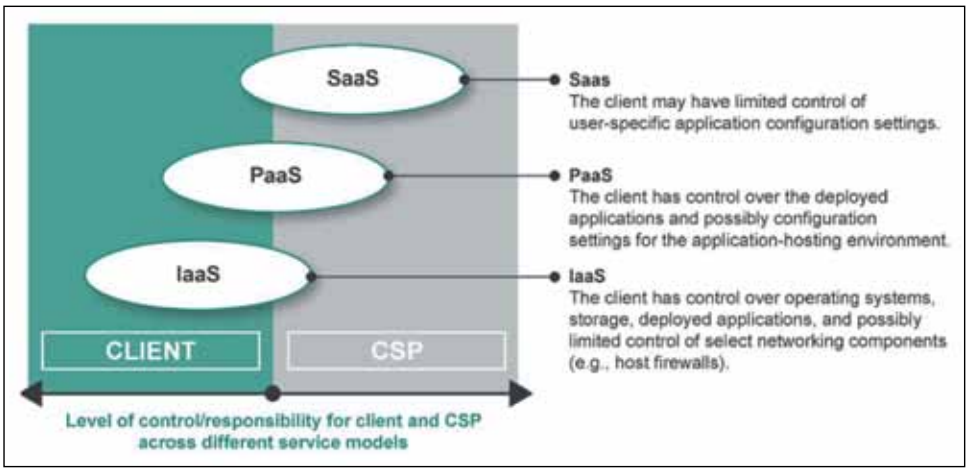

Figura 1.- Asignación de responsabilidades en un entorno de cloud. (Fuente: PCI SSC)

– Evidencia documentada de componentes de sistemas y servicios excluidos de la validación de PCI DSS.

– Contrato descriptivo en donde se describan de forma explícita las responsabilidades cubiertas por el CSP y el cliente.

Si los puntos anteriores no pueden ser provistos por el CSP, el entorno físico y lógico asociado deberá ser validado dentro de la auditoría PCI DSS del propio cliente, con los costes asociados que esto implica.

SERVICIO	DESCRIPCIÓN
Auto Scaling	Escalamiento automático de instancias Amazon EC2
AWS CloudFormation	Organización e implementación de recursos de AWS
Amazon CloudFront	Servicio de red de entrega de contenido (CDN)
AWS CloudHSM	Módulos de seguridad de hardware (HSM) dedicados en la nube de AWS
AWS CloudTrail	Almacenamiento y gestión de registro de eventos (logs)
AWS Direct Connect	Conectividad privada entre AWS y el centro de datos del cliente
Amazon DynamoDB	Servicio de base de datos NoSQL
AWS Elastic Beanstalk	Despliegue de aplicaciones
Amazon Elastic Block Store (EBS)	Gestión de volúmenes de almacenamiento persistente para instancias EC2
Amazon Elastic Compute Cloud (EC2)	Provisión de escalabilidad de servidores privados virtuales empleando Xen
Elastic Load Balancing (ELB)	Balanceo de carga entre instancias de Amazon EC2
Amazon Elastic MapReduce (EMR)	Procesamiento de big data empleando Hadoop
Amazon Glacier	Servicio de almacenamiento para archivar datos y backups
AWS Key Management Service (KMS)	Control centralizado de claves de cifrado
AWS Identity and Access Management (IAM)	Gestión de acceso de usuarios a servicios y recursos de AWS
Amazon Redshift	Almacén de datos para análisis empleando inteligencia empresarial
Amazon Relational Database Service (RDS)	Despliegue y gestión de bases de datos relacionales
Amazon Route 53	Servicio de DNS escalable y con alta disponibilidad
Amazon SimpleDB	Gestión de datastores NoSQL de alta disponibilidad
Amazon Simple Storage Service (S3)	Almacenamiento simple de objetos en cloud
Amazon Simple Queue Service (SQS)	Servicio de cola de mensajes
Amazon Simple Workflow Service (SWF)	Administración de flujos de trabajo
Amazon Virtual Private Cloud (VPC)	Aislamiento lógico de recursos de AWS

Tabla 1. Listado a junio de 2016

Igualmente –y con el fin de evitar confusiones provenientes de estrategias de marketing engañosas– es muy importante tener presentes los siguientes criterios básicos a la hora de escoger un CSP para desplegar un entorno que cumpla con PCI DSS:

a) Si un CSP cumple con PCI DSS no implica que por extensión sus clientes cumplen.

b) Si los clientes de un CSP cumplen con PCI DSS no implica que el CSP cumple.

c) Si un CSP y uno de sus clientes cumple con PCI DSS no implica que los otros clientes cumplen.

Para aclarar todos estos conceptos con un ejemplo práctico, este artículo se focalizará en el despliegue de una infraestructura en el *cloud* haciendo uso de Amazon Web Services (AWS [3]) y alineando los servicios provistos por ese proveedor con PCI DSS.

Amazon Web Services (AWS) y PCI DSS

Uno de los pioneros en los servicios de computación en la nube es Amazon con su servicio Amazon Web Services (AWS). Se trata de un modelo de responsabilidad compartida de *Infrastructure as a Service* (IaaS) en el cual AWS es el responsable de la seguridad de la infraestructura que soporta el servicio, mientras que el cliente es el responsable de la seguridad de los servicios y datos desplegados sobre este entorno [4].

Bajo estas premisas, Amazon tiene certificados una serie de servicios dentro de su certificación PCI DSS Level 1 como Proveedor de Servicios [5] dentro de los cuales se encuentran. (Ver **Tabla 1**).

Tal como se comentaba anteriormente, Amazon como CSP ofrece a sus clientes una serie de documentación en la cual se establece su nivel de cumplimiento (a través del *Attestation of Compliance* – AoC) y un documento de asignación de responsabilidades. Esta documentación puede ser solicitada directamente a Amazon a través de un representante comercial [6].

La infraestructura física subyacente (GovCloud incluido) y el entorno de gestión de AWS

Al margen de la certificación de los servicios de infraestructura provistos por Amazon, el cliente es responsable de las siguientes actividades para garantizar el cumplimiento de su propio entorno de datos de tarjetas de pago (entre otras):

– Configuración y administración de las instancias virtuales de EC2 (*Guest Operating System*).

– Configuración de las reglas de filtrado y segmentación de su entorno.

– Autenticación y autorización del sistema operativo y de cualquier servicio o aplicación ejecutado sobre una instancia de EC2.

– Actualización de sistemas operativos, aplicaciones y servicios.

– Despliegue de controles anti*malware*, monitorización de integridad y detección/prevención de intrusiones.

– Cifrado de datos de tarjetas de pago almacenados en las instancias EC2.

– Coordinación de actividades de respuesta a incidentes.

– Uso y configuración de otros servicios de Amazon que no se encuentran explícitamente certificados como PCI DSS.

Con base en estas responsabilidades, a continuación se describirá cómo se pueden utilizar los servicios provistos y certificados por Amazon para lograr el cumplimiento del entorno del cliente por cada uno de los requisitos de PCI DSS.

Requisito 1: Instale y mantenga una configuración de *firewalls* para proteger los datos de los titulares de las tarjetas

Es importante tener presente que bajo el modelo de AWS desaparecen las capas/zonas clásicas de la red tradicional. Los elementos de filtrado perimetral (*firewalls*) se convierten en filtros a nivel de instancia, como se explicará más adelante.

Para el despliegue de una arquitectura de red en AWS conforme lo indica PCI DSS, se pueden emplear las siguientes estrategias:

– Distribuir el entorno en varias **Virtual Private Cloud (VPC)**. Cada VPC es una red privada con su propio rango de direcciones IP (CIDR), tablas de enrutamiento y puertas de enlace. Se puede pensar en una VPC como si se tratase de una VLAN. Empleando este criterio, se puede definir

una VPC "interna" (en donde se ubicarán los componentes que almacenen datos de tarjetas de pago) y una VPC DMZ, en donde se ubicarán los componentes que proveen servicios públicos. La comunicación entre las VPC se realiza mediante **VPC Peering**, que actúa como un enrutador virtual entre estos elementos.

Este mismo modelo también se puede implementar en una única VPC con diferentes segmentos de red, que se encontrarán aislados hasta que no se defina enrutamiento entre ellos.

– Para el establecimiento de políticas de filtrado conforme con PCI DSS se pueden emplear los VPC **Security Groups** (componentes que permiten trazabilidad de conexiones establecidas (*stateful*) que actúan como *firewalls* virtuales a nivel de instancia). Mediante listas de control de acceso (ACL) de Security Groups se puede aceptar (*allow*) el tráfico entrante y saliente requerido entre instancias a nivel de dirección IP, puerto y protocolo. El tráfico que no es explícitamente permitido es denegado.

– De forma complementaria se pueden emplear las **Network ACL**. A diferencia de los Security Groups, las Network ACL funcionan a nivel de subred y son *stateless*. Por esto último, esta funcionalidad no cumpliría con PCI DSS pero sí puede ser usada como una segunda capa de defensa complementaria.

Adicionalmente, se pueden desplegar **Amazon Machine Images** (AMIs) desde el AWS Marketplace [7] que ofrezcan servicios de filtrado *stateful* de paquetes, como los provistos por Palo Alto Networks, Fortinet y Check Point.

Como soporte a las características de filtrado provistas por Amazon, siempre se puede hacer uso de una solución de cortafuegos directamente en la propia instancia EC2 dependiendo del sistema operativo (iptables, nftables, pf o soluciones comerciales).

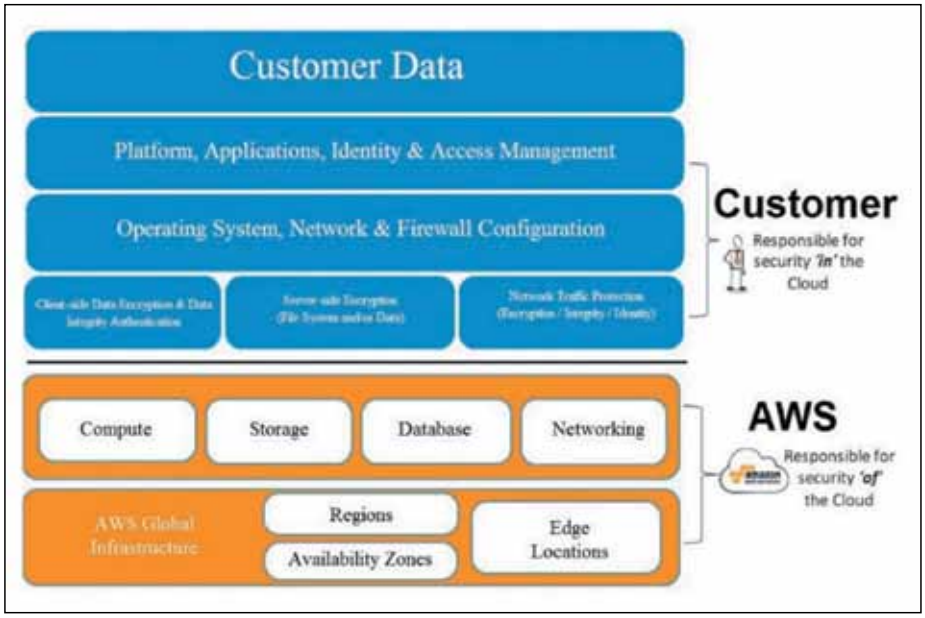

Figura 2.- Responsabilidades en el entorno AWS. (Fuente: Amazon)

Para proteger el direccionamiento interno, es necesario configurar NAT (*Network Address Translation*) en las VPC a través de **NATSG Security Groups** y/o desplegar una solución de proxy (como por ejemplo Squid), bajo responsabilidad del cliente [8].

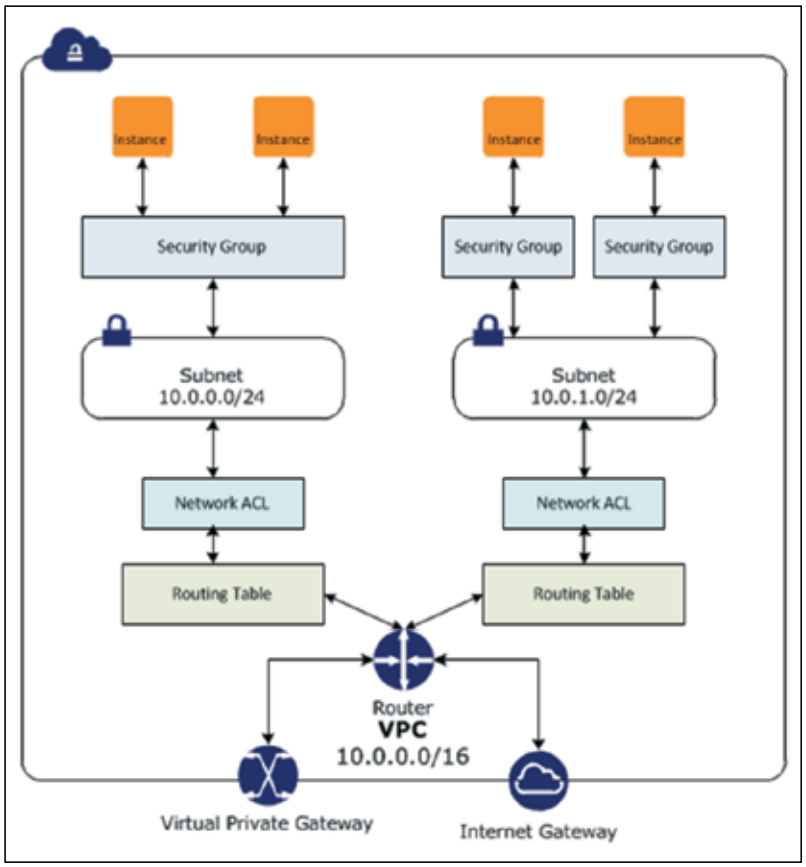

Figura 3.- Arquitectura de red y capas de filtrado en AWS. (Fuente: Amazon)

Requisito 2: No utilizar contraseñas de sistemas y otros parámetros de seguridad provistos por los proveedores

En este caso, el cliente es el responsable del aseguramiento (*hardening*) de sistemas operativos, bases de datos, aplicaciones y cualquier otro servicio que se ejecute sobre la infraestructura de Amazon. No obstante, Amazon publica de forma periódica una serie de documentos y guías de configuración que pueden ser muy útiles durante el proceso de despliegue de controles en AWS [9].

En el caso de sistemas operativos, Amazon provee AMIs para el despliegue de instancias EC2 (como por ejemplo Amazon Linux [10]) que viene con una serie de configuraciones de seguridad que pueden servir para el cumplimiento de PCI DSS (como por ejemplo contraseñas únicas para las cuentas, acceso remoto basado en claves SSH, minimización de servicios y notificación de actualizaciones), pero es responsabilidad del cliente documentar, configurar y asegurar todos los demás componentes

y cambiar los valores por defecto como lo indica PCI DSS.

Adicionalmente, se puede hacer uso de herramientas de automatización de despliegue de configuración como **Chef** [11], **Puppet** [12], **Ansible** [13] y/o **AWS OpsWorks** [14], que proveen de plantillas de configuración para tecnologías comunes y servicios de Amazon que se pueden tomar como base para la configuración de parámetros de seguridad basados en PCI DSS.

Para el aseguramiento de los propios componentes de AWS en el entorno PCI DSS desde el punto de vista de configuración se puede emplear como referencia la guía del *Center for Internet Security* "*CIS Amazon Web Services Foundations*" [15].

Por otro lado, para validar la implementación de controles de seguridad se puede emplear la herramienta "**Trusted Advisor**" que cuenta en su versión "free" con 4 revisiones en la categoría de "Seguridad" (Grupos de seguridad – Puertos específicos sin limitaciones, Uso de IAM y MFA en la cuenta raíz) o más de 50 comprobaciones adicionales en la versión "Premium" [16]. Por otro lado, el servicio **AWS Config** (del que se hablará en el requisito 6) permite la ejecución de reglas para la validación del estado de configuración de un activo, particularmente útil para garantizar el cumplimiento de PCI DSS [17].

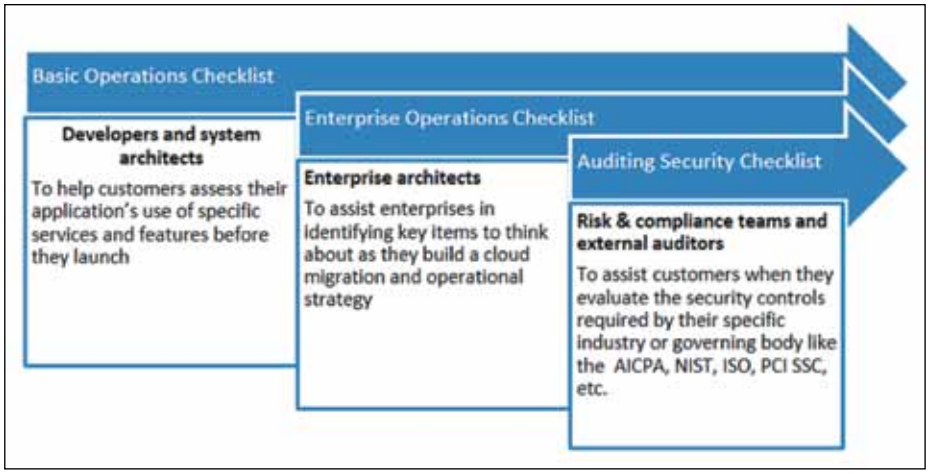

Figura 4.- Listas de comprobación disponibles para AWS. (Fuente: Amazon)

Finalmente, Amazon ha desarrollado varias listas de validación (checklist) que pueden ser empleadas como guías durante el despliegue e implementación de servicios:

– Operational & Enterprise Operations Checklist [18].

– Auditing Security Checklist [19].

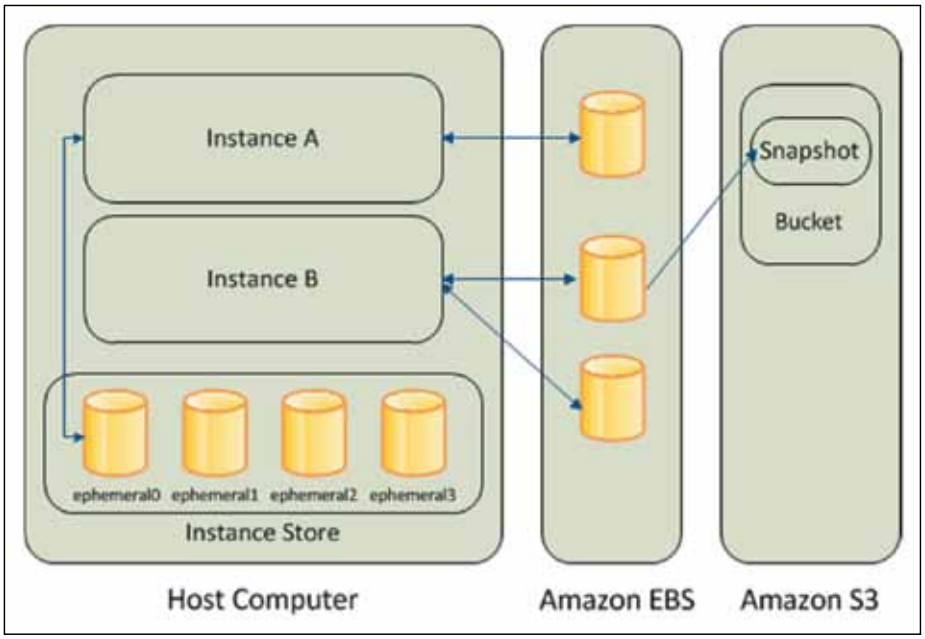

Figura 5.- Comparativo entre Amazon EBS y S3. (Fuente: Amazon)

Requisito 3: Proteja los datos del titular de la tarjeta que fueron almacenados

Probablemente uno de los requisitos en los cuales hay mayores dudas respecto a responsabilidades es el requisito 3 relacionado con la protección de datos almacenados usando cifrado en la infraestructura de Amazon.

De acuerdo con el PCI SSC, **la responsabilidad de los datos cifrados recae en quien controla y/o tiene acceso a los datos cifrafos y a las claves de cifrado**. Bajo este escenario, si en Amazon se almacenan datos cifrados en sus servicios de almacenamiento (EBS, S3, RDS) y adicionalmente se almacenan las claves de cifrado en dicho entorno, directamente los activos involucrados en ese proceso se encontrarán dentro del ámbito de cumplimiento de PCI DSS.

Siendo así, a continuación se describen algunas alternativas para 'securizar' los datos almacenados siguiendo los criterios de PCI DSS:

– Si los datos son almacenados en una estructura diferente a una base de datos (ficheros XML, por ejemplo), se puede emplear cifrado a nivel de disco o de volumen empleando **EncFS** [20], **DM-Crypt / LUKS** [21] o alguna de las alternativas de cifrado disponibles en el AWS MarketPlace. No obstante, toda la gestión de claves quedará bajo responsabilidad del cliente.

– Si se emplea **Amazon EBS** (que funciona como un volumen (disco) para una instancia de EC2) se puede emplear el cifrado disponible en dicha plataforma (AES-256) y su gestión de claves (que cumple con FIPS-140-2), que genera una única clave maestra que se almacena separada de los datos [22].

– Si se emplean *buckets* de **Amazon S3** (que funciona como un almacenamiento de red) se tienen varias opciones dependiendo de la gestión de las claves desplegada:

• Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3), en el cual cada objeto que se almacena en los *buckets* de S3 se cifra con una clave única, que a su vez es cifrada con una clave maestra gestionada por S3.

• Server-Side Encryption with AWS KMS-Managed Keys (SSE-KMS). En este

caso, las claves de cifrado son gestionadas empleando **AWS Key Management Service (KMS)**, que almacena las claves en dispositivos HSM (Hardware Security Modules).

• Server-Side Encryption with Customer-Provided Keys (SSE-C). Bajo este modelo, el cliente gestiona su propia clave de cifrado sin que S3 la almacene.

Si los datos se almacenan en bases de datos provistas por Amazon RDS, se puede emplear cifrado mediante **Amazon KMS** o **TDE** (Cifrado Transparente de datos - Transparent Data Encryption) disponibles para Oracle [23] y Microsoft SQL Server [24]. Otras bases de datos que pueden emplear cifrado en el almacenamiento de datos son MySQL, PostgreSQL, Aurora DB y MariaDB [25].

Con base en lo anterior, la gestión de claves de cifrado se puede llevar a cabo desde tres perspectivas diferentes:

– Por el propio usuario.

– Usando **AWS KMS** (*Key Management Service*) (HSM compartido).

– Usando **AWS CloudHSM** (HSM exclusivo) [26]

Los servicios de gestión de claves de Amazon permiten implementar de forma nativa los procesos de rotación/cambio de claves, así como la asignación de privilegios para acceso a las claves (custodios) a través de Amazon IAM (descrito más adelante).

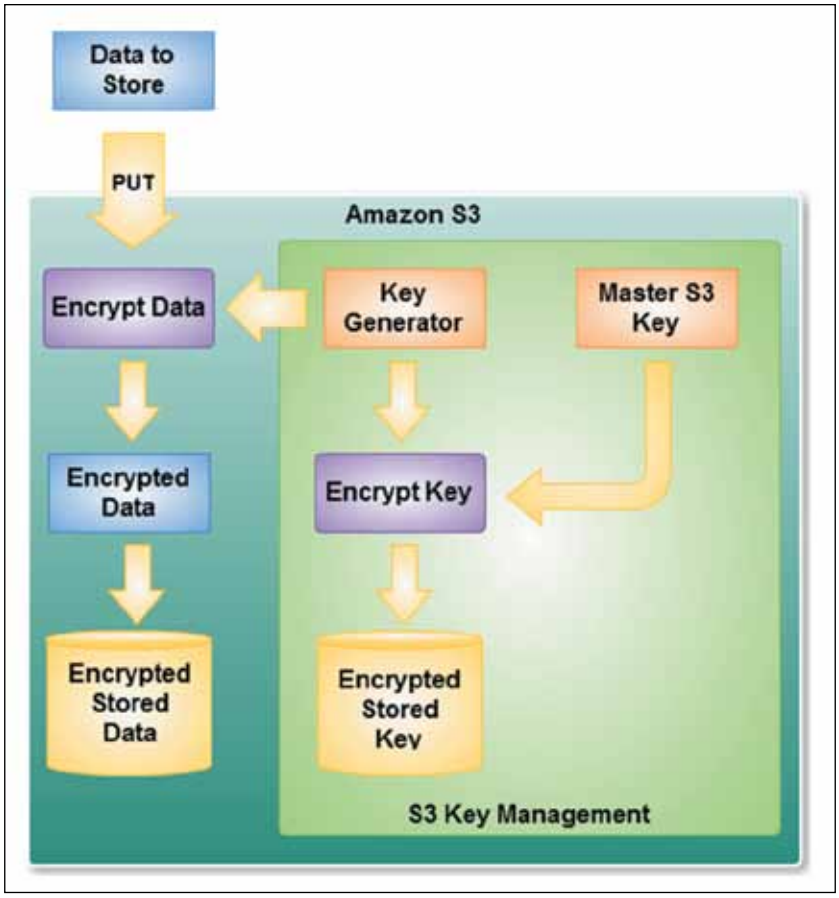

Figura 6.- Almacenamiento de datos en Amazon empleando SSE-S3. (Fuente: Amazon)

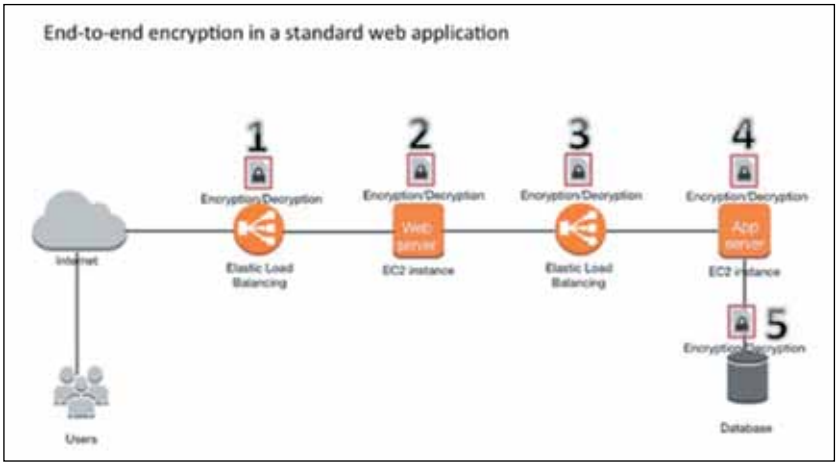

Figura 7.- Balanceo de carga empleando AWS ELB. (Fuente: Amazon)

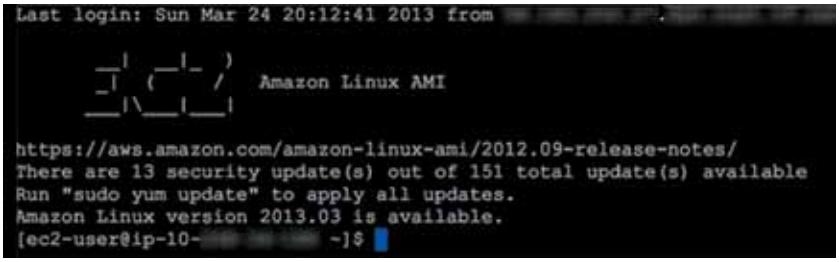

Figura 8.- Amazon Linux MOTD indicando actualizaciones disponibles. (Fuente: Amazon)

Requisito 4: Cifrar la transmisión de los datos del titular de la tarjeta en las redes públicas abiertas.

Para la protección de datos de tarjetas de pago en redes públicas abiertas, se pueden emplear varias estrategias:

– Si se trata de tráfico HTTPS, se puede finalizar el túnel de HTTPS en los propios servidores EC2. En este caso, la responsabilidad de configuración recae enteramente en el cliente. Si se despliega esta opción, todo el tráfico estará cifrado desde el navegador del usuario hasta el servidor web, lo cual puede afectar otros controles de seguridad como IDS o WAF.

– Amazon provee una infraestructura de balanceo de carga denominada **AWS Elastic Load Balancing** (ELB). ELB puede ser empleada como terminador de conexiones HTTPS y cuenta con una serie de plantillas predeterminadas para la configuración de negociación de protocolos y algoritmos de cifrado conforme con los requerimientos de PCI DSS [27].

Para la gestión de certificados, se puede hacer uso de **AWS Certificate Manager** (ACM), que se integra de forma transparente con ELB o se puede instalar un certificado propio. Y para conexiones VPN, de forma nativa las VPC soportan conexiones VPN IPSEC con claves previamente compartidas en formato estático o dinámico y

LAN-to-LAN o user-to-LAN.

Por otro lado, si se establecen canales de comunicación de alta velocidad entre Amazon y el cliente empleando **AWS Direct Connect** [28], es el cliente el responsable del cifrado de datos dependiendo del despliegue de este modelo.

Requisito 5: Proteger todos los sistemas contra malware y actualizar los programas o software antivirus regularmente

Para el cumplimiento del requerimiento 5 es importante aclarar que Amazon no provee de protección antimalware para las instancias EC2. En este caso, la responsabilidad de la instalación, configuración y monitorización de una solución antimalware recae enteramente en el cliente.

Para cubrir el requerimiento se puede instalar una solución antivirus licenciada por el propio cliente (bajo el modelo "Bring Your Own License") o instalar una del AWS Marketplace (McAfee, Trend Micro, Sophos, Bitdefender, etc.).

Requisito 6: Desarrolle y mantenga sistemas y aplicaciones seguras

Al igual que en el requisito 5, Amazon no provee de ninguna solución de despliegue de actualizaciones, por lo que la monitorización de vulnerabilidades y despliegue de actualizaciones de las instancias EC2 estarán bajo la responsabilidad del cliente.

Si se emplea Amazon Linux AMI, se recomienda consultar periódicamente el sitio web **Amazon Linux AMI Security Center** [29], que contiene el listado de vulnerabilidades y actualizaciones disponibles para esta plataforma.

Para la gestión de cambios, se puede hacer uso del servicio **AWS Config** [30], que permite obtener un inventario de los recursos de AWS con todos sus detalles de configuración, obtener un histórico de modificaciones y recibir notificaciones cuando se detecte un cambio en la infraestructura.

Finalmente, para cumplir con el requerimiento 6.6 se pueden emplear dos alternativas:

– Utilizar una herramienta de análisis de vulnerabilidades a nivel de aplicación, bajo responsabilidad del propio cliente.

– Emplear un WAF. Para la opción del WAF, Amazon cuenta con el servicio **Amazon AWS WAF** – Web Application Firewall [31]. AWS WAF cubre con los requerimientos de PCI DSS para la protección de aplicaciones web (incluyendo OWASP Top Ten) y puede desplegarse de manera transparente para analizar el tráfico web. Al respecto, hay que tener en cuenta dos cosas:

– En el momento de la redacción de este artículo (junio 2016), AWS WAF no se encontraba dentro de los servicios certificados por PCI DSS de Amazon, por lo cual su seguridad debería ser validada por un QSA dentro de la auditoría de cliente.

– Si se despliega esta solución, la finalización de los túneles HTTPS debe estar antes del WAF, de tal forma que el tráfico que reciba esté en texto claro.

Adicionalmente, se pueden emplear otras soluciones de WAF disponibles en el AWS MarketPlace (Imperva, Barracuda, entre otros) o desplegarlo directamente en la propia instancia del servidor web (empleando mod_security, por ejemplo).

Requisito 7: Restrinja el acceso a los datos del titular de la tarjeta según la necesidad de saber que tenga la empresa

Para el cumplimiento del requerimiento 7 es importante dividir el acceso en dos niveles:

– Acceso a la infraestructura AWS.

– Acceso a los servidores EC2.

Para la implementación de controles de PCI DSS en el acceso a la infraestructura AWS se puede emplear **AWS Identity and Access Management** (IAM). Este servicio permite la gestión de usuarios, roles y permisos dentro del entorno AWS, incluyendo acceso a claves de cifrado.

Para la implementación de acceso a los servidores EC2 y servicios sobre estas instancias (aplicaciones, bases de datos, etc.), la responsabilidad es completamente del usuario, aunque se pueden emplear servicios de directorio de Microsoft con **AWS Directory Service** [32], que permiten integrar la autenticación con instalaciones existentes de Microsoft Active Directory (AD Connector) o usar un servicio simple de directorio totalmente en la nube (Simple AD).

Requisito 8: Identificar y autenticar el acceso a los componentes del sistema

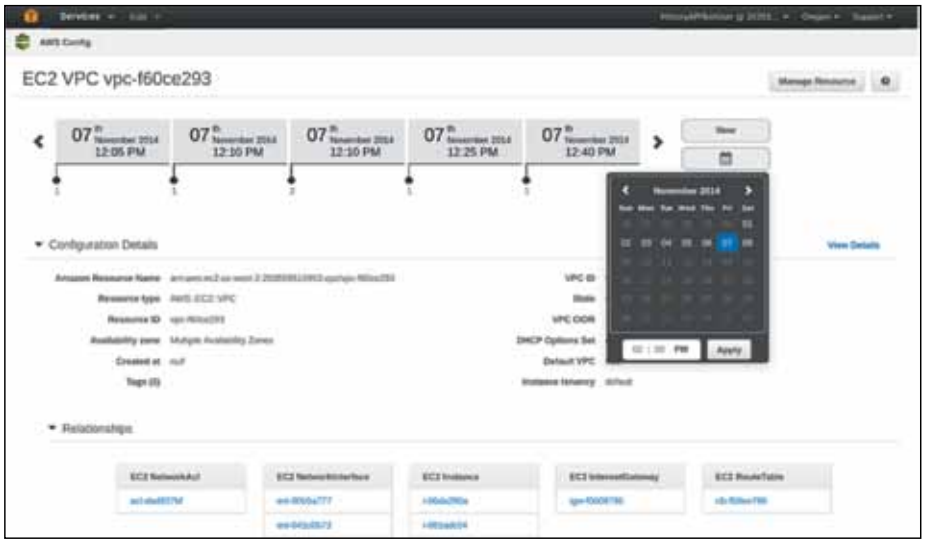

Figura 9.- Consola de AWS Config con un histórico de cambios de un host EC2. (Fuente: Amazon)

El cumplimiento de este requerimiento depende en gran parte de la estrategia empleada para cubrir el requisito 7, ya sea a través de la implementación de la autenticación de instancias EC2 por parte del cliente o haciendo uso de servicios de directorio de Amazon. En cualquier caso, la configuración de las políticas de contraseñas corre enteramente bajo responsabilidad del usuario.

Adicionalmente, se requiere configurar el servicio de multi-factor authentication (MFA) para accesos desde fuera del CDE (Cardholder Data Environment), que se puede implementar haciendo uso de **AWS Multifactor Authentication (MFA)** [33].

Requisito 9: Restringir el acceso físico a los datos del titular de la tarjeta

El cumplimiento de este requerimiento está cubierto en su totalidad por Amazon. Dicho cumplimiento se puede extrapolar

al cliente siempre y cuando toda la infraestructura del CDE (*Cardholder Data Environment*) esté ubicada en Amazon. De lo contrario, la seguridad física de los activos fuera de este entorno debe ser analizada por un QSA.

Requisito 10: Rastree y supervise todos los accesos a los recursos de red y a los datos de los titulares de las tarjetas

Para la gestión de registros de eventos (*logs*) es importante tener presente los siguientes criterios:

– Amazon a través del servicio **Amazon CloudTrail** registra los eventos provenientes de IAM y de la consola de AWS de acuerdo con PCI DSS [34] y a través de **Amazon CloudWatch** se pueden definir métricas y gestionar alarmas como complemento a la recolección de los *logs* [35].

– El cliente es el responsable de la configuración e implementación de controles de registro de eventos en todas las instancias EC2, RDS, EMR, SimpleDB, DynamoDB y de cualquier otro servicio dentro del alcance, así como de la sincronización horaria de dichos componentes.

Para cumplir con este requisito, se puede hacer uso de cualquier solución de SIEM disponible en el AWS MarketPlace (Splunk, AlienVault, etc.).

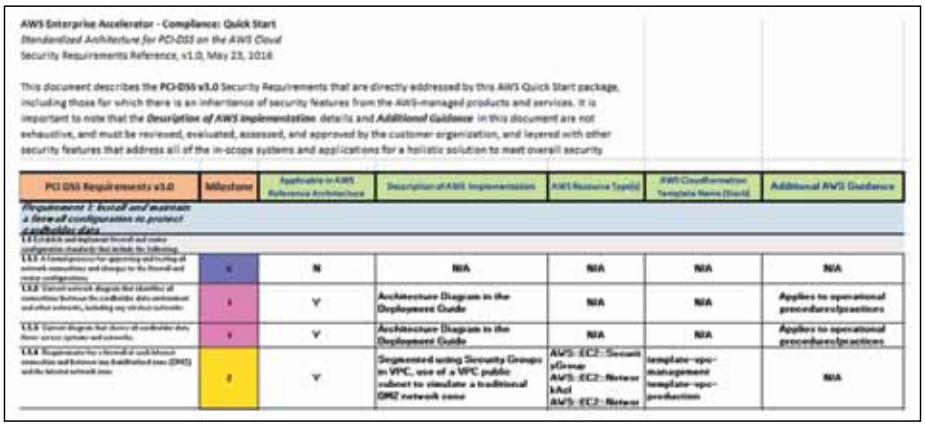

Figura 11.- Detalle del documento AWS Enterprise Accelerator – Compliance for PCI DSS.

Requisito 11: Pruebe con regularidad los sistemas y procesos de seguridad

Para el cumplimiento de este requisito, los escaneos de redes inalámbricas son cubiertos por Amazon dentro de sus procesos de certificación.

Para los escaneos de vulnerabilidades internos, es el cliente el responsable de la ejecución de estas pruebas. Para ello, se puede hacer uso de alguna de las soluciones del MarketPlace (Qualys, Tenable Nessus, Rapid 7, etc.) o hacer uso del servicio **AWS Inspector** [36].

Para los escaneos de vulnerabilidades externos, el cliente debe contratar a un proveedor cualificado ASV (Approved Scanning Vendor) [37].

El cliente es el responsable de la ejecución de pruebas de penetración, teniendo presente las limitaciones existentes de acceso a la capa de red, conforme con lo descrito en el Requisito 1.

Para la ejecución tanto de escaneos de vulnerabilidades como de pruebas de penetración, Amazon ha estipulado un protocolo de actuación para solicitar permiso *antes* de la ejecución de cualquier prueba de seguridad que pueda afectar la protección del entorno [38].

El despliegue de soluciones de IDS/IPS y FIM (*File Integrity Monitoring*) es responsabilidad del cliente. Al igual que sucediera en los requisitos anteriores, se puede hacer uso de soluciones disponibles en el AWS MarketPlace para IDS/IPS o FIM.

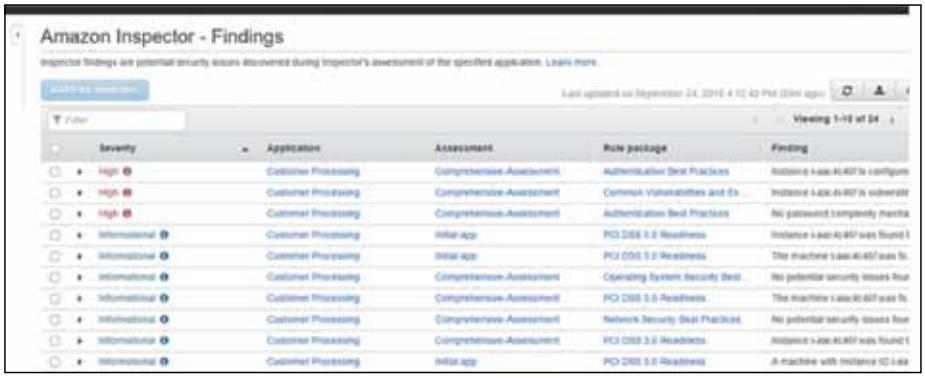

Figura 10.- Detalle de resultados de análisis de vulnerabilidades de Amazon Inspector. (Fuente: Amazon).

Requisito 12: Mantener una política que aborde la seguridad de la información de todo el personal

Para este requisito, la responsabilidad de mantenimiento de una política de seguridad, gestión de formación, gestión de proveedores, análisis de riesgos, etc. corren bajo responsabilidad del cliente.

Amazon se encuentra listado como Proveedor de Servicios Nivel 1 de PCI DSS para las diferentes marcas de pago y cuenta con un documento de definición de responsabilidades para el cubrimiento del req. 12.8.

Para la coordinación de acciones en caso de incidentes, Amazon mantiene un tablero de mando del estado de sus servicios [39] e internamente gestiona y coordina la gestión de incidentes a través de su servicio de soporte [40].

Siguientes pasos: Amazon AWS Enterprise Accelerator for PCI DSS Compliance Quick Start

Con el objetivo de simplificar el despliegue y configuración inicial de componentes modulares dentro de la infraestructura de AWS bajo las directrices de un estándar o de mejores prácticas, Amazon publica de forma periódica una serie de documentos de inicio rápido de referencia para implementaciones denominados *AWS Quick Start Reference Deployments* [41]. Estas guías están orientadas hacia la automatización de la configuración inicial con base en el servicio **AWS CloudFormation** [42]. CloudFormation está compuesta de dos elementos principales:

– Plantillas (*templates*): Ficheros de configuración con formato JSON que definen cómo se crearán los recursos empleando la API de AWS

– Pilas (*stacks*): Recopilación de

recursos creados como resultado de la ejecución de una plantilla.

Aprovechando las ventajas de este modelo, Amazon publicó en mayo de 2016 *AWS Enterprise Accelerator – Compliance: Standardized Architecture for PCI DSS on the AWS Cloud* [43], en donde se realiza un despliegue de un entorno PCI DSS básico contemplando AWS IAM, VPC con subredes para DMZ y *backend*, Security Groups y ACL para EC2, balanceo de carga con ELB y políticas TLS, *buckets* S3 para almacenamiento de contenido, acceso administrativo a través de SSH, bases de datos MySQL bajo RDS y gestión de *logs* con CloudTrail, CloudWatch y AWS Config rules, componentes descritos en su totalidad en este documento.

Para soportar la validación del estándar en comparación con los servicios provistos por AWS, se proporciona una lista de validación (checklist) con los controles de PCI DSS v3.0 de acuerdo con el documento *Prioritized Approach for PCI DSS Compliance* del PCI SSC [44] y las funcionalidades de CloudFormation por cada control [45]. Es de recibo anotar que en el momento de la redacción de este artículo la versión de PCI DSS era la v3.2 mientras que el documento de referencia de CloudFormation estaba basado en PCI DSS v3.0.

Conclusión

Cuando por consideraciones técnicas o administrativas se opta por delegar la gestión de ciertos componentes o de la totalidad de la infraestructura informática de la organización a un tercero, es imprescindible garantizar que los niveles de seguridad que dicho tercero aplicará serán iguales o mejores a los que la propia organización mantiene. Adicionalmente, si el entorno delegado debe cumplir con requerimientos legales o estándares de la industria, la responsabilidad de parte y parte debe quedar claramente estipulada en términos contractuales. Este es el caso de los servicios de Amazon en la nube (Amazon AWS) y el cumplimiento de PCI DSS. A pesar que el proveedor (CSP) ofrece una gran cantidad de servicios para configurar la infraestructura de forma segura, es finalmente el cliente el responsable de la seguridad de los datos y de la configuración de los servicios que se ejecutan sobre la capa provista por Amazon.

Por otro lado, la complejidad en el despliegue de una solución de estas características implica un alto conocimiento tanto de la plataforma del CSP (en este caso, Amazon) como de la aplicación de los controles de PCI DSS. Es por ello que es recomendable (si no indispensable) el acompañamiento de un asesor QSA, quien podrá guiar en todo momento a la organización en la implementación y configuración de controles para evitar incongruencias con el estándar.

Finalmente, en este artículo se ha plasmado el despliegue técnico de controles empleando las funcionalidades provistas por un CSP como Amazon. No obstante, muchos de los conceptos pueden ser extrapolados a otros proveedores de servicio empleando como premisa la descripción clara en términos contractuales de las responsabilidades tanto del cliente como del proveedor. ■

David E. Acosta Rodríguez
Consultor en Seguridad de la Información
PCI QSA, CISSP Instructor, CISM, CISA, CRISC, BS25999 LA, CCNA Security, CHFI Trainer, OPST
INTERNET SECURITY AUDITORS

REFERENCIAS

[1] https://www.pcisecuritystandards.org
[2] https://www.pcisecuritystandards.org/pdfs/PCI_DSS_v2_Cloud_Guidelines.pdf
[3] https://aws.amazon.com/es/
[4] https://aws.amazon.com/es/compliance/shared-responsibility-model/
[5] https://aws.amazon.com/es/compliance/pci-dss-level-1-faqs/
[6] https://aws.amazon.com/es/compliance/contact
[7] https://aws.amazon.com/marketplace
[8] http://blogs.aws.amazon.com/security/post/TxFRX7UFUIT2GD/How-to-Add-DNS-Filtering-to-Your-NAT-Instance-with-Squid
[9] https://aws.amazon.com/es/security/security-resources/
[10] https://aws.amazon.com/es/amazon-linux-ami/
[11] https://www.chef.io y http://docs.aws.amazon.com/quickstart/latest/chef-server/
[12] https://puppetlabs.com/ y http://docs.aws.amazon.com/quickstart/latest/puppet/
[13] https://www.ansible.com/aws
[14] http://aws.amazon.com/es/opsworks/
[15] https://benchmarks.cisecurity.org/downloads/show-single/?file=awsfoundations.100
[16] https://aws.amazon.com/es/premiumsupport/trustedadvisor/best-practices/
[17] https://github.com/awslabs/aws-config-rules/blob/master/RULES.md
[18] http://media.amazonwebservices.com/AWS_Operational_Checklists.pdf
[19] http://d0.awsstatic.com/whitepapers/compliance/AWS_Auditing_Security_Checklist.pdf
[20] http://www.arg0.net/encfs
[21] http://silvexis.com/2011/11/26/encrypting-your-data-on-amazon-ec2/
[22] http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html
[23] http://aws.amazon.com/es/blogs/aws/amazon-rds-for-oracle-database-data-and-network-encryption/
[24] https://aws.amazon.com/es/blogs/aws/amazon-rds-for-microsoft-sql-server-transparent-data-encryption-tde/
[25] http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Overview.Encryption.html
[26] https://aws.amazon.com/es/cloudhsm/
[27] http://docs.aws.amazon.com/ElasticLoadBalancing/latest/DeveloperGuide/elb-security-policy-table.html
[28] https://aws.amazon.com/es/directconnect/
[29] https://alas.aws.amazon.com/
[30] http://aws.amazon.com/es/config/
[31] https://aws.amazon.com/es/waf
[32] https://aws.amazon.com/es/directoryservice/
[33] http://aws.amazon.com/es/iam/details/mfa/
[34] http://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-supported-services.html
[35] http://aws.amazon.com/es/documentation/cloudwatch/
[36] https://aws.amazon.com/es/inspector/details/
[37] https://es.pcisecuritystandards.org/assessors_and_solutions/approved_scanning_vendors
[38] http://aws.amazon.com/es/security/penetration-testing/
[39] http://status.aws.amazon.com/
[40] http://aws.amazon.com/support y https://aws.amazon.com/es/security/vulnerability-reporting/
[41] http://aws.amazon.com/es/quickstart/
[42] https://aws.amazon.com/es/cloudformation/
[43] http://docs.aws.amazon.com/quickstart/latest/accelerator-pci/
[44] https://www.pcisecuritystandards.org/documents/Prioritized_Approach_for_PCI_DSS_v3_.pdf
[45] https://s3.amazonaws.com/quickstart-reference/enterprise-accelerator/pci/latest/docs/PCI-DSS-Security-Controls-Mapping.xlsx