Universitat Oberta de Catalunya
uoc.edu

Cifrado de datos en sistemas de Cloud Público

Rubén González Cobo
Máster universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones
Seguridad empresarial

Jordi Guijarro Olivares
Víctor García Font

2 de junio de 2020

FICHA DEL TRABAJO FINAL

Título del trabajo:	*Cifrado de datos en sistemas de Cloud Público*
Nombre del autor:	*Rubén González Cobo*
Nombre del consultor/a:	*Jordi Guijarro Olivares*
Nombre del PRA:	*Víctor García Font*
Fecha de entrega (mm/aaaa):	06/2020
Titulación:	*Máster universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones*
Área del Trabajo Final:	*Seguridad empresarial*
Idioma del trabajo:	Castellano
Palabras clave	*Cloud - nube* *Cifrado* *AWS*

Resumen del Trabajo:

La finalidad de este trabajo es revisar qué opciones tiene una entidad financiera para migrar su infraestructura a sistemas de proveedores en la nube, pero siempre manteniendo o aumentando la seguridad del almacenamiento y del tratamiento de los datos.

Actualmente el sector bancario está inmerso en un proceso de transformación digital que implica en algunos casos la migración de la infraestructura a sistemas en la nube debido, entre otras cosas, a las bondades de los sistemas en la nube y a la llegada de nuevos competidores al sector financiero proporcionado por directivas como PSD2 que obliga a la apertura de algunos servicios de pago de las entidades financieras a terceras empresas, los denominados TPP.

Los TPP suelen ser empresas 100% digitales y apoyan toda su infraestructura en la nube, lo que les está proporcionando ventajas como la escalabilidad, el pago por uso de los recursos que deriva en menos costes de IT, así como el reducido time to market, es decir, el tiempo que tardan desde que detectan una oportunidad de negocio hasta que la ponen a disposición de los clientes.

Por lo tanto, se ha realizado un estudio de los servicios ofrecidos por AWS, de PCI-DSS, del RGPD y de la PSD2. Además, se han revisado algunos CASB.

Finalmente se han dado una serie de buenas prácticas y ejemplos de arquitecturas para cumplir con PCI-DSS, PSD2 y una solución para disponibilizar aplicaciones internas a cualquier ubicación en entornos de teletrabajo, lo que ha evidenciado que cualquier organización, financiera o no, puede migrar sus sistemas a la nube sin tener que penalizar la seguridad en materia de protección de datos.

Abstract:

The purpose of this study is to review what options have a financial institutions to migrate their infrastructure to cloud provider systems, but always maintaining or enhancing the security of data storage and processing.

The financial industry is currently undergoing on a digital transformation process that in some cases involves the migration of infrastructure to cloud systems due, among other things, to the benefits of cloud systems and the arrival of new competitors in the financial sector provided by directives such as PSD2 that require some payment services from financial institutions to be opened up to third parties, known as TPP.

TPPs are usually 100% digital companies and support their entire infrastructure in the cloud, which is providing them advantages such as scalability, pay-per-use of resources which results in lower IT costs, as well as reduced time to market, i.e., the time it takes when they detect a business opportunity until they make it available to customers.

Therefore, a study has been carried out of the services offered by AWS, PCI-DSS, GDPR and PSD2. In addition, some CASBs have been reviewed.

Finally, a series of good practices and examples of architectures have given for complying with PCI-DSS, PSD2 and a solution for making internal applications available at any location in teleworking environments. It has shown that any organization, financial or otherwise, can migrate their systems to the cloud without having to penalize data protection security.

Índice

Lista de imágenes

Lista de tablas

1. Introducción

1.1 Contexto y justificación del Trabajo

El sector bancario se está viendo empujado a ofrecer servicios de valor para los clientes ante la llegada de nuevos competidores al sector financiero proporcionado por directivas como PSD2 que, entre otras cosas, busca la apertura por parte de los bancos de sus servicios de pagos a terceras empresas, los denominados TPPs (Third Party Payment Service Providers).

Estos TPP suelen nacer como empresas 100% digitales, que apoyan toda o gran parte de su infraestructura en la nube, lo que les está proporcionando ventajas como la escalabilidad, el pago por uso de los recursos (computación, almacenamiento, etc.), así como el reducido time to market, es decir, el tiempo que tardan estas empresas desde que detectan una oportunidad de negocio hasta que la ponen a disposición de los clientes en el mercado.

Debido a estos nuevos actores (Fintech, Neobancos, etc.), directivas como PSD2, y los beneficios que ofrecen los cloud públicos, hay una gran necesidad en el sector financiero de migrar parte de los centros de procesamiento de datos (CPD) tradicionales a la nube junto con los datos almacenados en los mismos para poder competir de tú a tú.

Ahora bien, en la nube, los datos residen físicamente en el proveedor de servicios cloud (Cloud Service Provider) lo que supone todo un reto en cuanto a cómo almacenar los datos. Disponer de un buen gobierno del dato, cifrado incluído, es esencial al tratar con información muy sensible, tanto interna como de los clientes.

Por lo tanto, con este trabajo se pretende revisar qué ofrecen los proveedores cloud poniendo el foco en Amazon Web Services (AWS), ya que en este momento es el proveedor más utilizado a nivel mundial, los organismos y regulaciones que aplican a la banca como, por ejemplo, RGPD, PCI-DSS, etc. y qué impacto tiene en la migración a un entorno cloud. Además, se hará una breve introducción a productos de terceros que pueden ayudar a mitigar los riesgos de la migración a un entorno cloud.

Por último, se ofrecerán una serie de buenas prácticas para el sector financiero que serán extrapolables a otras empresas de diferentes sectores que quieran implantar su CPD en la nube, así cómo almacenar de manera correcta los datos de sus clientes, empleados, proveedores, etc. en la nube.

1.2 Objetivos del Trabajo

Los objetivos de este trabajo son los siguientes:

- Qué ofrecen las cloud públicas para la migración y almacenamiento de los datos a su infraestructura:
    - Servicios de migración y comunicaciones
    - Tipos de almacenamiento
    - Cifrado en la cloud pública
        - Cifrado en AWS
    - Servicios de seguridad que ofrecen para autenticación, auditoría, monitorización, etc.
- Organismos, estándares, directivas y regulaciones que afectan a la banca y a cómo almacenan sus datos:
    - Banco de España (BdE) / Autoridad Bancaria Europea (ABE)
    - PCI
    - PSD2
    - RGPD
- Agentes de seguridad de acceso a la nube - CASB:
    - Introducción a los CASB
    - Ejemplos de CASB

1.3 Enfoque y método seguido

El enfoque y método seguido para este trabajo de fin de máster (TFM) va a ser realizar un estudio y un análisis de los puntos que se pretenden abordar como objetivos del trabajo.

1.4 Planificación del Trabajo

En las imágenes 1 y 2 se muestran los hitos parciales de cada una de las PEC.

Planificación Trabajo fin de máster			
Tarea	**Inicio**	**Fin**	**Días**
Trabajo final de máster	**19/2/2020**	**19/6/2020**	**122**
Plan de trabajo	**19/2/2020**	**3/3/2020**	**14**
Documentación previa	19/2/2020	21/2/2020	3
Contexto y justificación	22/2/2020	23/2/2020	2
Definición de objetivos	24/2/2020	25/2/2020	2
Definición de tareas	26/2/2020	28/2/2020	3
Planificación	29/2/2020	2/2/2020	3
Revisión y entrega Plan de trabajo - PEC 1	3/3/2020	3/3/2020	1
Estudio y redacción servicios Cloud pública	**4/3/2020**	**31/3/2020**	**28**
Introducción a AWS	4/3/2020	6/3/2020	3
Servicios de migración y comunicaciones en AWS	7/3/2020	10/3/2020	4
Almacenamiento: Disco y BBDD en AWS	11/3/2020	18/3/2020	8
Cifrado en cloud públicas - AWS	19/3/2020	25/3/2020	7
Servicios más importantes de seguridad en AWS	26/3/2020	29/3/2020	4
Revisión y entrega PEC 2	30/3/2020	31/3/2020	2
Estudio y redacción de reguladores y normativas que afectan a la banca	**1/4/2020**	**28/4/2020**	**28**
Banco de España (BdE) y Autoridad Bancaria Europea (ABE)	1/4/2020	7/7/2020	7
Payment Card Industry (PCI)	8/4/2020	11/4/2020	4
Directiva de Servicios de Pago (PSD2)	12/4/2020	15/4/2020	4
Reglamento General de Protección de Datos (RGPD)	16/4/2020	26/4/2020	11
Revisión y entrega PEC 3	27/4/2020	28/4/2020	2
CASB y guía de buenas prácticas - Memoria final	**29/4/2020**	**2/6/2020**	**35**
Introducción a los CASB	29/4/2020	30/4/2020	2
Principales CASB	1/5/2020	2/5/2020	2
Guía de buenas prácticas	3/5/2020	17/5/2020	15
Maquetación memoria TFM	18/5/2020	27/5/2020	10
Revisión y entrega memoria final - PEC 4	28/5/2020	2/6/2020	6
Grabación y revisión video presentación TFM	**3/6/2020**	**9/6/2020**	**7**
Grabación video presentación	3/6/2020	8/6/2020	6
Revisión y entrega video presentación	9/6/2020	9/6/2020	1
Defensa del TFM	**15/6/2020**	**19/6/2020**	**5**

Imagen 1. Planificación TFM

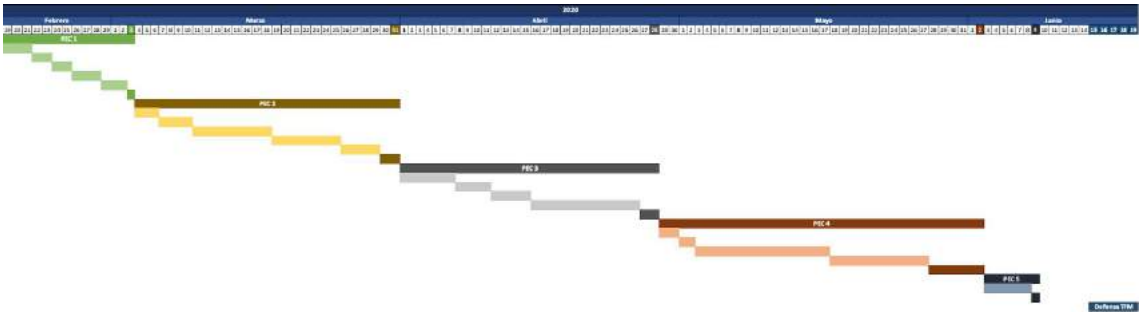

Imagen 2. Planificación TFM. Diagrama de Gantt.

1.5 Breve sumario de productos obtenidos

Tras realizar el estudio y el análisis de los productos y servicios, así como regulaciones, normativas, etc. que afectan al almacenamiento de datos y ficheros en soluciones cloud se obtendrán los siguientes productos:

- Buenas prácticas de seguridad en entornos cloud
- Conceptos en los que basar una buena arquitectura en entornos cloud

1.6 Breve descripción de los otros capítulos de la memoria

Este trabajo tendrá cuatro grandes bloques:

- Amazon Web Services: contendrá la información sobre la infraestructura de AWS, productos y servicios que disponibiliza a sus clientes.
- Organismos y regulaciones: Tratará sobre qué deben tener en cuenta las empresas del sector financiero a la hora de procesar y almacenar los ficheros y datos de su negocio.
- Productos de terceros: se revisarán algunas soluciones externas a los proveedores cloud que utilizados en común pueden aportar un extra de seguridad.
- Buenas prácticas de seguridad para el uso de soluciones cloud.

2. Introducción al cloud público

2.1 Uso de la cloud pública

En la RSA Conference de 2020, la empresa Thales, dedicada al desarrollo de electrónica para sistemas de información, expuso una serie de datos [1] que demuestran que cada vez más, las empresas están adoptando soluciones para el despliegue de sus sistemas de información y almacenamiento de datos haciendo uso de los servicios de las cloud públicas. Sin embargo, también se observa que no se están almacenando los datos sensibles de manera correcta.

Algunas de las cifras dadas por Thales son, por ejemplo, que las empresas tienden a adoptar soluciones para su infraestructura de TI basadas en múltiples cloud públicas. El 48% de las organizaciones que hacen uso de la cloud pública, tienen una estrategia multicloud desplegadas en Amazon Web Service (AWS), Microsoft Azure e IBM.

Por otro lado, las empresas usan de media 29 aplicaciones en la nube, en comparación con hace dos años que utilizaban 27. El 10% de las empresas tiene más de 50 aplicaciones en la nube y el negocio promedio de los EE. UU. tiene 41 aplicaciones en cloud.

Como se puede observar, cada vez más empresas están migrando aplicaciones y sus correspondientes datos de los centros de procesamiento de datos (CPD) tradicionales a los CPD de los proveedores cloud.

Ahora bien, en el lado de la seguridad, aún toca ir un paso más allá. Aportando volumetrías respecto a la seguridad de las soluciones adoptadas:

- Sólo el 30% de las empresas tiene un sistema unificado de accesos seguros tanto a sus aplicaciones on-premise como a sus aplicaciones cloud.
- Sólo el 49% de las empresas están cifrando sus datos sensibles en la nube. Por lo tanto, no se están aplicando medidas de seguridad adecuadas para la protección del dato.
- Respecto a las empresas que sí cifran sus datos sensibles, sólo la mitad de las empresas mantienen el control de las claves de sus datos cifrados almacenados en la nube, en torno a un 53% a pesar de que el 78% dice que es importante conservar la propiedad de las claves de cifrado.

Por lo tanto, se puede concluir con que cada vez más empresas están migrando sus aplicaciones, sus CPD, etc. a los proveedores cloud para tratar de ser más competitivos gracias a bondades de estos sistemas. Incluso hay empresas de reciente creación que tienen toda su infraestructura desplegada en el algún proveedor de servicios cloud.

No obstante, también se puede destacar que no se están haciendo de la mejor manera las migraciones a la nube. Sobre todo en cuanto al almacenamiento y gestión del dato sensible.

2.2 Qué proporciona la cloud pública [2]

Como se ha visto en el apartado 2.1, cada vez más organizaciones están migrando o valorando el despliegue de aplicaciones o incluso infraestructura completa en proveedores cloud. Esto es debido a la serie de ventajas que proporcionan. Por ejemplo, por citar y describir algunas de ellas:

- Alta disponibilidad: Hardware y software con la configuración adecuada permiten que un sistema se recupere rápidamente en caso de fallo.

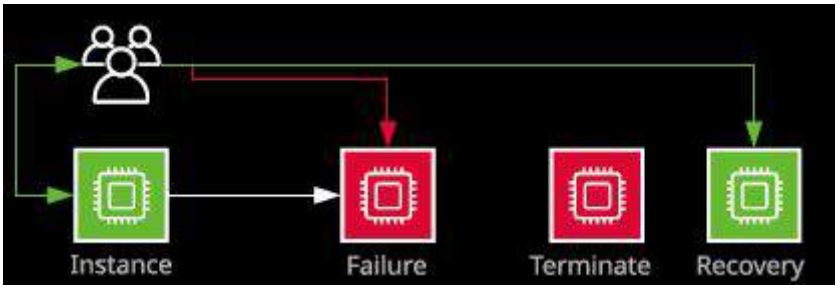

Imagen 3. Concepto alta disponibilidad.

- Tolerancia a fallos: Sistemas diseñados para operar con algún fallo en el mismo sin impacto para el usuario.

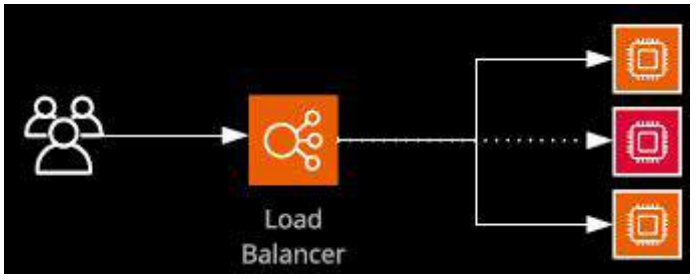

Imagen 4. Concepto tolerancia a fallos con balanceador de carga.

- Escalado vertical: El escalado vertical se logra al agregar recursos adicionales en la forma de CPU o memoria para una máquina existente haciendo que el sistema pueda atender peticiones adicionales. Por lo tanto, el tamaño de la máquina limita la posibilidad de escalado.

- Escalado horizontal: El escalado horizontal se logra agregando máquinas adicionales en un grupo de recursos, cada uno de los cuales proporciona el mismo servicio. La escala horizontal no sufre ninguna de las limitaciones de tamaño de escala vertical y puede escalar a niveles casi infinitos, pero requiere soporte de aplicaciones para escalar de manera efectiva.

- Costes: En las soluciones cloud, en general, se realiza pago por uso. Es decir, por número de peticiones, por número de máquinas levantadas en la infraestructura desplegada, número de discos duros o bases de datos

e información almacenada en estos, etc. Y todo esto a la par que se hace uso del escalado, tanto vertical como horizontal, lo que proporciona una enorme ventaja frente a un CPD tradicional donde se tiene que hacer una inversión previa en máquinas tratando de dimensionar lo mejor posible para asumir picos de carga de la infraestructura, pero sin ser demasiado optimista y que eso sea un problema de recursos ociosos la mayor parte del tiempo.

- Time to market o agilidad en el despliegue: Al no tener que preocuparse por la infraestructura y su configuración de más bajo nivel, las empresas que utilizan este tipo de soluciones cloud “sólo” tienen que realizar las configuraciones que estén bajo su responsabilidad y articular el despliegue de la aplicación para ponerla al servicio de sus clientes.

Ahora bien, la cloud pública no es la solución a todos los problemas y sigue requiriendo de acciones por parte de los administradores de la empresa que contrata los servicios cloud. Un buen ejemplo de esto es el modelo de responsabilidad compartida en función del modelo de uso contratado (los modelos de uso se ven en el apartado 2.3)

A grandes rasgos, los principales proveedores lo tienen documentado de la siguiente manera:

- AWS [4]

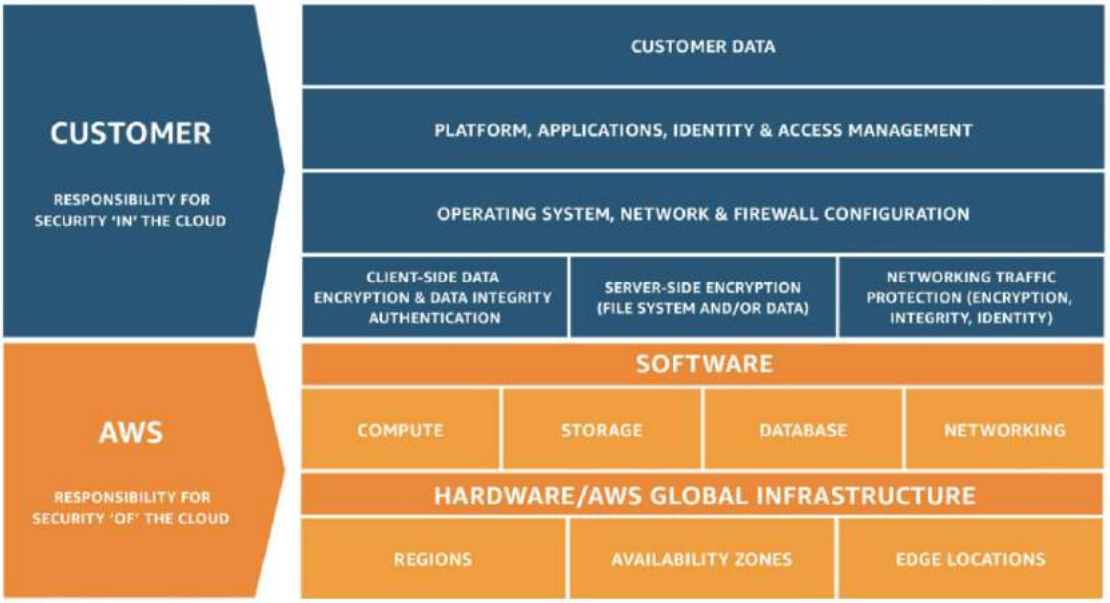

Imagen 5. Modelo de responsabilidad compartida de AWS.

La responsabilidad de AWS en relación con la "seguridad de la nube" es proteger la infraestructura que ejecuta todos los servicios provistos en la nube de AWS. Esta infraestructura está conformada por el hardware, el software, las redes y las instalaciones que ejecutan los servicios de la nube de AWS.

La responsabilidad del cliente en relación con la "seguridad en la nube" estará determinada por los servicios de la nube de AWS que el cliente seleccione.

- Microsoft Azure [5]

Imagen 6. Modelo de responsabilidad compartida de Microsoft Azure.

De la misma manera que sucede con AWS, en función del modelo de uso y servicios contratadas, las responsabilidades de cada una de las partes varía.

2.3 Modelos de uso de cloud pública [6]

Tal y como se ha visto en el apartado 2.2, el modelo de responsabilidad compartida sobre quién debe ocuparse de la seguridad de qué se rige en cierta medida por los modelos de uso de Cloud Pública disponibles. Existen tres modelos de cloud computing:

1. **IaaS** - Infraestructura como servicio, del inglés Infrastructure as a Service: El proveedor proporciona a los clientes acceso de pago por uso al almacenamiento, las redes, los servidores y otros recursos informáticos en el cloud.

2. **PaaS** - Plataforma como servicio, del inglés Platform as a Service: El proveedor de servicios ofrece acceso a un entorno basado en cloud en el cual los usuarios pueden crear y distribuir aplicaciones. El proveedor proporciona la infraestructura subyacente.

3. **SaaS** - Software como servicio, del inglés Software as a Service: El proveedor de servicios proporciona el software y las aplicaciones a través de internet. Los usuarios se suscriben al software y acceden a él a través de la web o las APIs del proveedor.

En la imagen 7, se puede ver qué responsabilidad tiene AWS (en naranja) y qué responsabilidad tiene el cliente (en azul), en función del modelo contratado, de izquierda a derecha, IaaS, PaaS y SaaS, respectivamente.

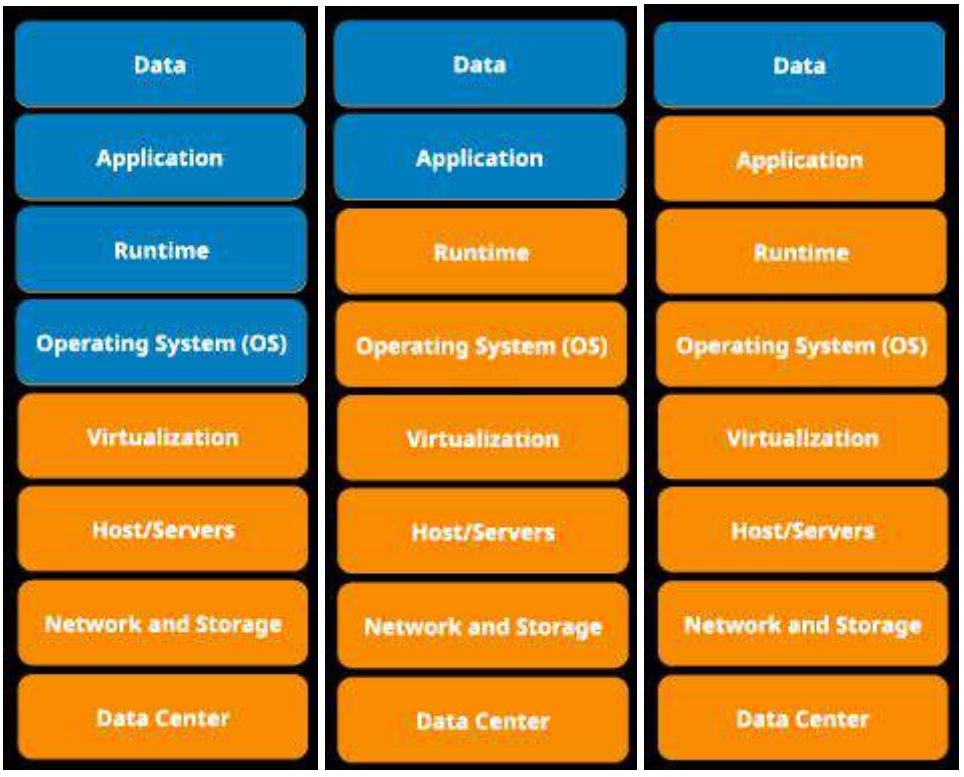

Imagen 7. Responsabilidad compartida de AWS en función del modelo. [2]

Además, existen tres modelos de implementación de informática en la nube:

1. Todo en cloud: Una aplicación basada en la nube se encuentra implementada totalmente en la nube, de modo que todas las partes de la aplicación se ejecutan en esta.

2. Modelo de nube híbrida: Una implementación híbrida es una manera de conectar la infraestructura y las aplicaciones entre los recursos basados en la nube y los recursos existentes situados fuera de la nube como, por ejemplo, un CPD tradicional. El método más común de implementación híbrida consiste en conectar la nube y la infraestructura existente local (CPD) para ampliar e incrementar la infraestructura de la empresa en la nube al mismo tiempo que se conectan estos recursos en la nube con el sistema interno.

3. Implementación de cloud local o privada: La implementación local de recursos mediante herramientas de administración de recursos y virtualización se denomina a veces "nube privada". Este modelo no suene aportar muchas ventajas frente al CPD tradicional.

2.4 Proveedores de servicios de cloud públicos

Existen principalmente seis proveedores a nivel mundial de servicios cloud, estos son: Amazon Web Services (AWS), Microsoft Azure, Google Cloud, Alibaba Cloud, Oracle Cloud e IBM Cloud.

En la siguiente imagen, extraída de un estudio de Gartner sobre el uso de las diferentes cloud públicas (modelo IaaS) se puede observar que AWS es el líder del mercado de proveedores de servicios cloud. Además lo es por noveno año consecutivo.

Imagen 8. Estudio Gartner[1] uso cloud públicas como IaaS.

Por lo tanto, en el siguiente apartado se va a profundizar en algunas de las características más relevantes, así como los servicios más importantes que ofrece AWS.

---

1 https://aws.amazon.com/es/blogs/aws/aws-named-as-a-leader-in-gartners-infrastructure-as-a-service-iaas-magic-quadrant-for-the-9th-consecutiveyear/

This graphic was published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document. The Gartner document is available upon request from AWS. Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

2.5 Introducción a AWS [2] [3]

Como se ha visto en los apartados anteriores, Amazon Web Services (AWS) es la plataforma en la nube más adoptada en el mundo, ofrece más de 175 servicios integrales de centros de datos a nivel global. Ofrece desde tecnologías de infraestructura como cómputo, almacenamiento y bases de datos hasta tecnologías emergentes como aprendizaje automático e inteligencia artificial, lagos de datos y análisis, e internet de las cosas [7].

AWS tiene la infraestructura en la nube más amplia del mundo [8]. Ningún otro proveedor de nube ofrece tantas regiones con múltiples zonas de disponibilidad conectadas por redes de baja latencia, alto rendimiento y altamente redundantes. AWS incluye 69 zonas de disponibilidad en 22 regiones geográficas de todo el mundo. Además, se anunciaron planes para incorporar 16 zonas de disponibilidad y cinco regiones de AWS adicionales en Indonesia, Italia, Japón, Sudáfrica y España.

En las imágenes 9, 10 y 11, se puede ver la infraestructura que tiene AWS desplegada de forma global para proveer sus servicios. Destacar que no todos los servicios están disponibles en todas las regiones de AWS.

Imagen 9. Infraestructura global de AWS.

Imagen 10. Infraestructura global de AWS - Mapa regiones.

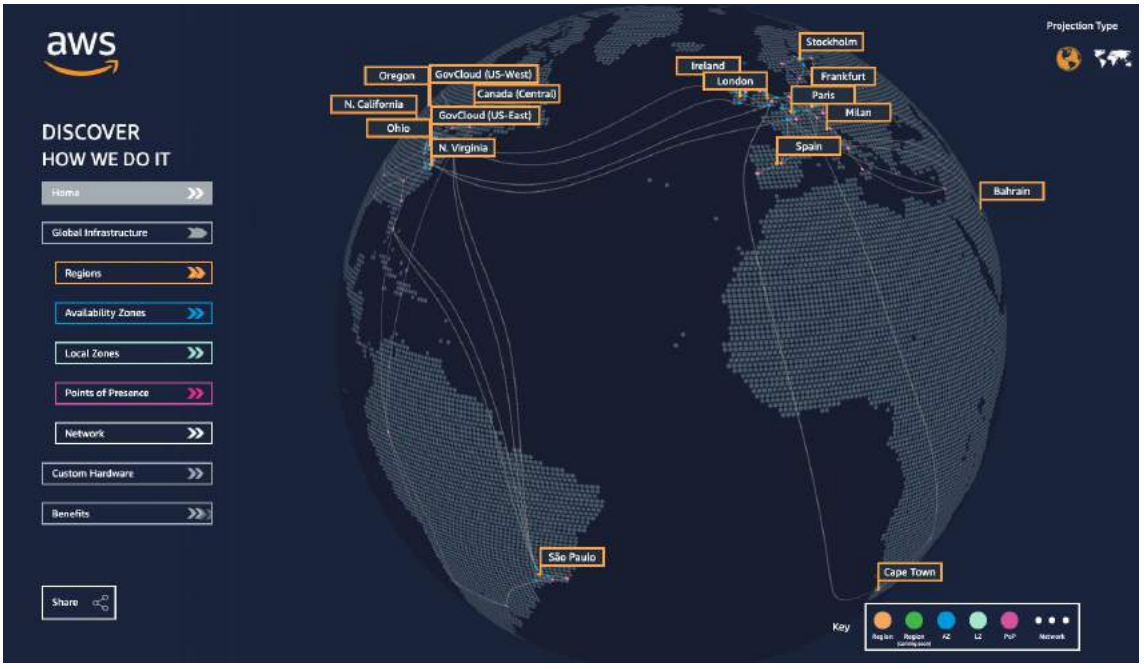

Imagen 11. Infraestructura global de AWS[2].

Por **Region** de AWS se entiende la ubicación física en todo el mundo donde agrupan los centros de datos. Llaman a cada grupo de centros de datos lógicos una zona de disponibilidad (AZ). Cada región de AWS consta de varias AZ aisladas y separadas físicamente dentro de un área geográfica.

Zona de disponibilidad (AZ, del inglés Available Zone): Una zona de disponibilidad (AZ) es uno o más centros de datos con alimentación, redes, conectividad redundantes en una región de AWS y seguridad física independiente.

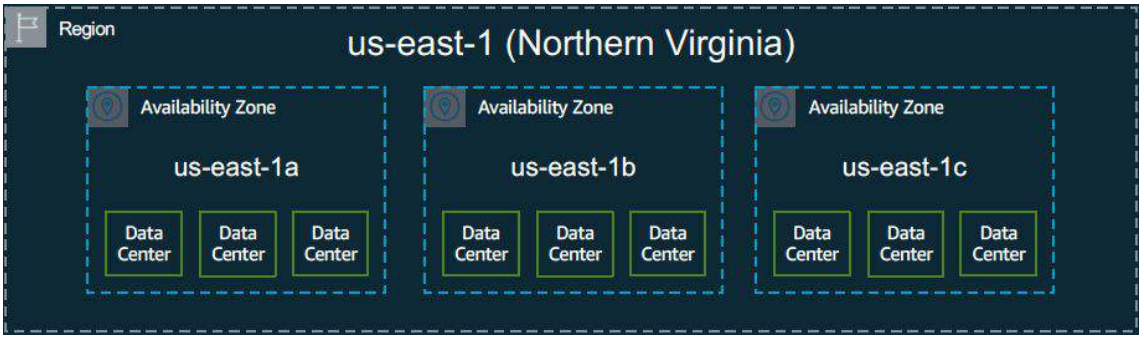

Imagen 12. Region - AZ de AWS.

Las AWS **Local Zones** (zonas locales) son un nuevo tipo de implementación de infraestructura AWS que acercan los servicios de cómputo, almacenamiento, bases de datos y otros servicios seleccionados a donde no existe una región de AWS hoy en día. Las AWS Local Zones (zonas locales) siguen siendo administradas y soportadas por AWS, lo cual ofrece toda la elasticidad, escalabilidad y los beneficios de cualquier otra región.

Tras esta breve introducción a la infraestructura desplegada por AWS a nivel global, se van a introducir algunos de los servicios más representativos que no

[2] https://www.infrastructure.aws/

se van a ver en otros apartados de este trabajo, pero que se consideran relevantes para el despliegue de aplicaciones o infraestructura por parte cualquier empresa que utilice alguno de modelos de implementación de informática en la nube vistos en el apartado 2.3.

- **AWS Organizations**: [9][10] es un servicio de gestión de cuentas que permite consolidar varias cuentas de AWS en una organización para su administración de forma centralizada. AWS Organizations incluye todas las prestaciones de facturación unificada y posibilidades de administración de cuentas para que pueda satisfacer mejor las necesidades presupuestarias, de seguridad y de conformidad de cualquier empresa. Esto permite que una organización pueda disfrutar de descuentos en el precio de los servicios que por cantidad de uso utilizando cuentas de manera independiente no obtendría. Por lo tanto, las características principales son:
    - Administración centralizada de todas las cuentas de AWS.
    - Facturación unificada para todas las cuentas miembro de una empresa.
    - Agrupación jerárquica de todas las cuentas de la empresa para satisfacer las necesidades presupuestarias, de seguridad y de cumplimiento.
    - Control de los servicios y las acciones de la API de AWS a las que puede tener acceso cada cuenta.
    - Integración con otros servicios de AWS.
    - AWS Organizations se ofrece sin cargo adicional. Solo se cobran los recursos de AWS que usen los usuarios y las funciones de las cuentas miembro.

- **Amazon EC2 (Amazon Elastic Compute Cloud)**: [11][12] servicio global básico de AWS, proporciona capacidad de computación escalable en la nube de Amazon Web Services (AWS). Este servicio casi daría para un trabajo de fin de máster completo si se quisiera hacer un estudio de todas las posibilidades de configuración que ofrece AWS para el despliegue de una instancia EC2. Las características principales de EC2 son:
    - Entornos informáticos virtuales, conocidos como instancias.
    - Múltiples tipos de instancias, tanto en fabricante como en finalidad. Varias configuraciones de CPU, memoria, almacenamiento y capacidad de red de las instancias, esto es lo que se conoce como tipos de instancias:
        - Propósito general
        - Optimizadas para computación
        - Optimizadas en cuanto a memoria RAM
        - Optimizadas para uso intensivo de gráficos
        - Optimizadas para el acceso a almacenamiento
    - Múltiples sistemas operativos soportados:
        - Windows
        - Amazon Linux
        - Debian

        - CentOS
        - Red Hat
        - etc.
    - Se pueden utilizar bajo demanda o reservadas.
    - Volúmenes de almacenamiento para datos temporales que se eliminan cuando se detiene o se termina la instancia, conocidos como volúmenes de almacén de instancias.
    - Direcciones IPv4 estáticas para informática en la nube dinámica, conocidas como direcciones IP elásticas.
    - Cuando se crea una instancia EC2, se crea por defecto una Elastic Network Interface (ENI) que es una “tarjeta de red”.
    - Las instancias cuentan con status checks, tanto hardware como a nivel de instancia para tener tener monitorizadas las mismas y saber si todo está correcto a nivel de instancia.
    - Redes virtuales que puede crear que están aisladas lógicamente del resto de la nube de AWS y que, opcionalmente, se pueden conectar a la red del cliente, conocidas como nubes privadas virtuales (VPC). Por lo tanto, las instancias EC2 corren dentro de una VPC.

- **VPC (Virtual Private Cloud - Cloud privada virtual)**: [13] permite aprovisionar una sección de la nube de AWS aislada de forma lógica, en la que se pueden lanzar recursos de AWS en una red virtual definida por el cliente. Características relevantes:
    - Posibilidad de crear en una Amazon VPC infraestructura escalable de AWS y especificar el rango de direcciones IP privadas del cliente.
    - Posibilidad de controlar el acceso de entrada y salida, desde y hacia subredes individuales por medio de listas de control de acceso (ACL).
    - Posibilita el almacenar datos en Amazon S3 y definir permisos de forma que el acceso a los datos sea posible exclusivamente desde el interior de la VPC del cliente.
    - Posibilidad de activar instancias EC2 en la plataforma clásica de EC2 para comunicarse con instancias en una VPC con direcciones IP privadas.

En la imagen 13 se puede ver un ejemplo sencillo en que se ven algunos de los conceptos introducidos en este apartado como, por ejemplo, VPC, Region, AZ, EC2, etc.

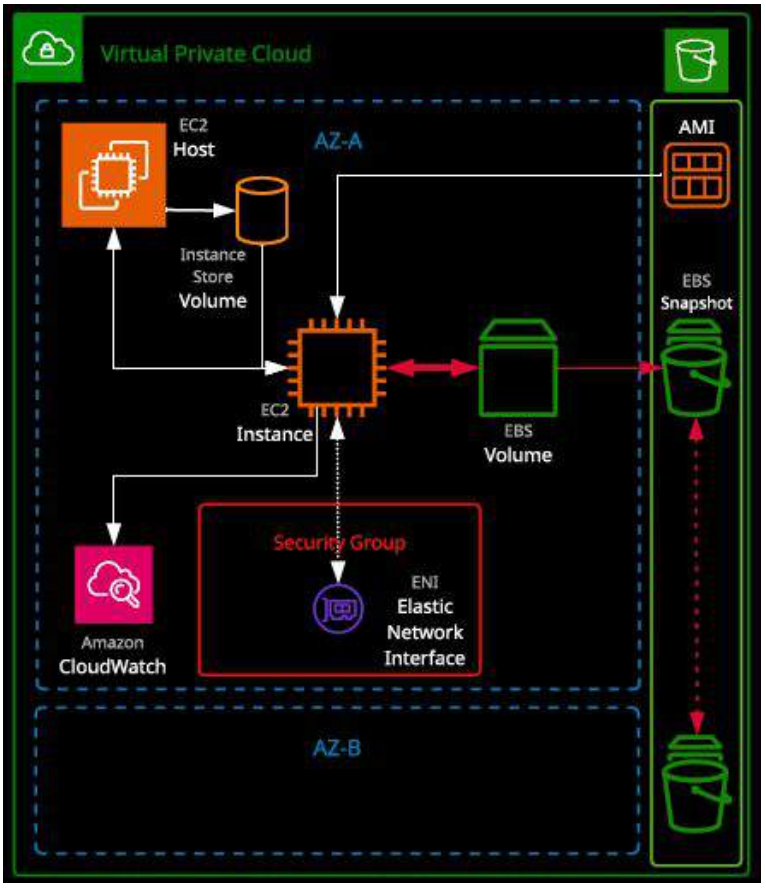

Imagen 13. Infraestructura ejemplo AWS.

Dado que hay cientos de servicios disponibles en AWS, en la imagen 14 se pueden ver las categorías [14] de servicios disponibles para que el lector pueda profundizar en la que más de interese acudiendo a la web oficial de AWS[3] y a la documentación [15] de los servicios correspondientes:

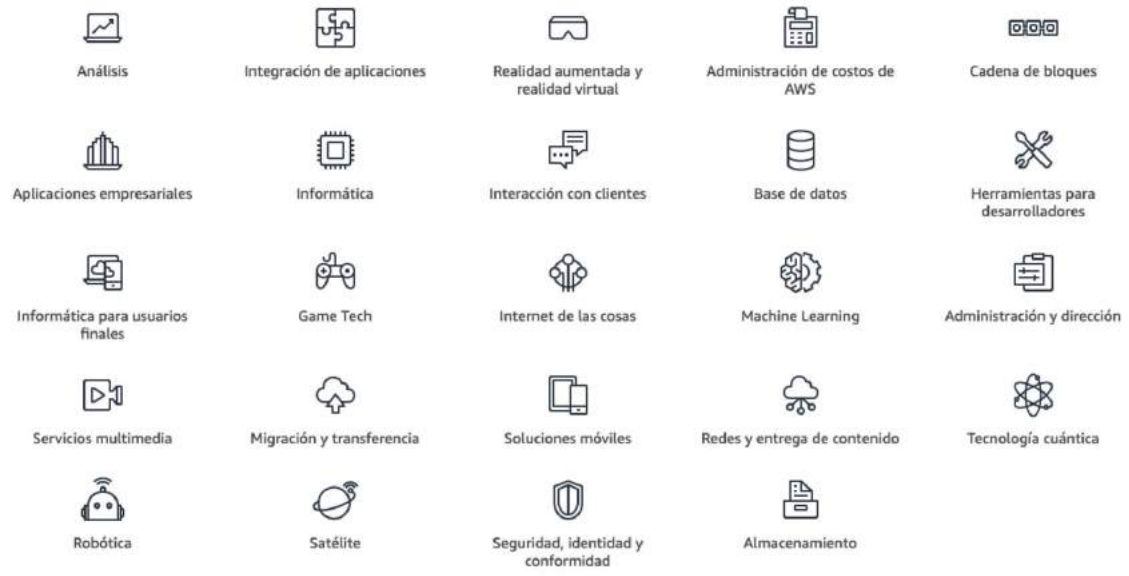

Imagen 14. Categorías de servicios de AWS.

[3] https://aws.amazon.com/es/

AWS pone a disposición de los clientes una tabla para la consulta de qué servicios están desplegados en qué regiones [16].

2.5.1 Servicios de migración y comunicaciones en AWS

En este apartado se pone el foco en algunos de los servicios catalogados en la imagen 14 como migración y transferencia, así como en algún servicio de redes y entrega de contenido, con el objetivo de introducir al lector en las posibilidades que tiene una empresa tradicional para abordar la migración al entorno cloud de AWS. Para ello se enumeran y se definen algunos de los servicios de dichas categorías.

- Migración y transferencia de datos a AWS:
    - **AWS Migration Hub**: Ofrece una interfaz web que permite saber cuáles son los recursos de TI existentes en la organización, además de visualizar y realizar un seguimiento del progreso de migración de las aplicaciones.

      Se integra con servicios de AWS y servicios de terceros como, por ejemplo, WS Server Migration Service, AWS Database Migration Service, CloudEndure Migration, ATADATA ATAmotion y RiverMeadow Server Migration SaaS.

    - **AWS Application Discovery Service**: AWS Application Discovery Service ayuda a los clientes empresariales a planificar proyectos de migración al recopilar información sobre sus centros de datos locales. AWS Application Discovery Service recopila la información de especificaciones de los servidores, los datos de rendimiento y los detalles de los procesos en ejecución y las conexiones de red.

      AWS Application Discovery Service protege los datos recopilados cifrándolos durante el tránsito hacia AWS y en reposo dentro del almacén de datos de Application Discovery Service.

    - **AWS Data Sync**: facilita la migración de los datos entre el almacenamiento local y AWS. El servicio incluye cifrado automático de datos. La imagen 15 muestra el funcionamiento de este servicio de AWS.

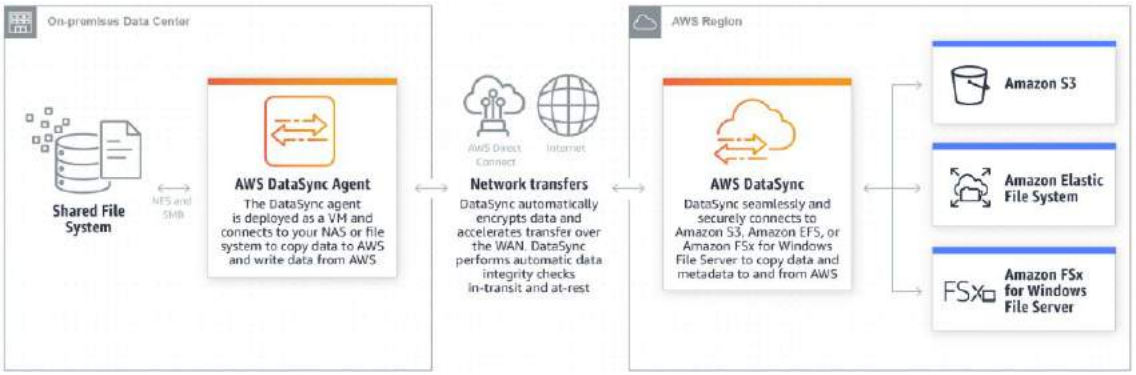

Imagen 15. DataSync.

- **AWS Server Migration Service (SMS)**: servicio sin agente que permite migrar de forma más rápida y sencilla miles de cargas de trabajo locales a AWS. Con AWS SMS, se puede automatizar, programar y monitorizar replicaciones graduales de volúmenes de servidores en directo, lo que facilita la coordinación de migraciones de servidores a gran escala. Permite replicar los volúmenes de servidores en vivo de forma automática en AWS y crea imágenes de máquina de Amazon (AMI) cuando es necesario.

- **AWS Transfer for SFTP**: servicio completamente administrado que permite transferir archivos de manera directa desde y hacia Amazon S3 por medio del protocolo seguro de transferencia de archivos (SFTP), también conocido como “protocolo de transferencia de archivos de shell seguro” (SSH). En la imagen 16 se puede ver el funcionamiento de este servicio.

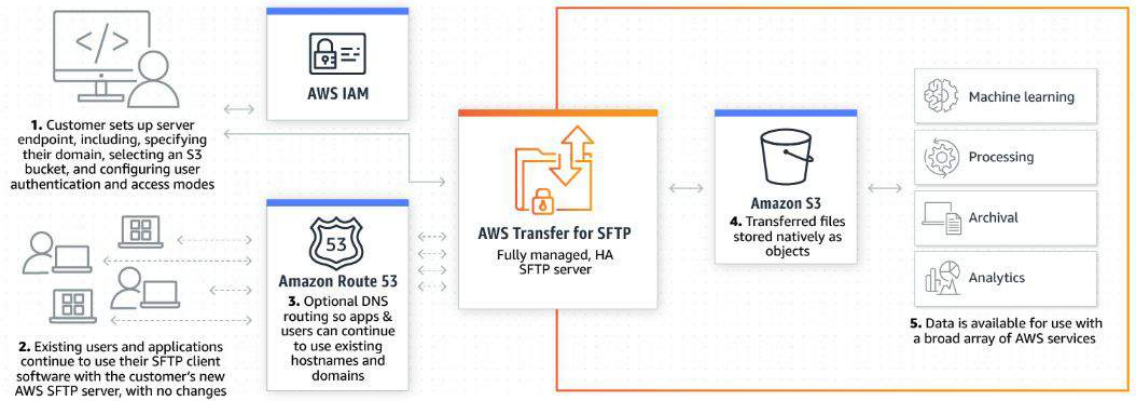

Imagen 16. AWS Transfer for SFTP.

- **Familia de productos Snow***: [17] La familia de servicios Snow* ofrece distintos dispositivos físicos y puntos de capacidad, incluidas algunas capacidades informáticas integradas. Estos

servicios ayudan a transferir físicamente hasta exabytes (EB, equivale a 10^{18} bytes) de datos hacia y desde AWS. La familia de servicios Snow es propiedad de AWS, que también se encarga de su administración. Las empresas deben solicitar un dispositivo a través de la consola de AWS. Se envía a la ubicación del cliente, donde deberá cargarlo con datos y devolverlo a la región de AWS de la que provino. Por lo tanto, no requiere de conexión directa con AWS S3 para subir los datos desde el CPD del cliente.

Todos los dispositivos de la familia Snow están diseñados para ser seguros y resistentes a las manipulaciones, tanto cuando se encuentran en una ubicación como cuando se trasladan a AWS: el hardware y el software cuentan con firma criptográfica y todos los datos se cifran automáticamente con claves de cifrado de 256 bits que son propiedad del cliente, quien también las administra. Los clientes pueden usar AWS Key Management Service (KMS) para generar y administrar las claves. Cuando el trabajo se completa, el contenido de los dispositivos se elimina mediante directrices de borrado del NIST.

Los tres métodos de la familia Snow* que proporciona AWS para mover grandes cantidades de datos sin preocuparse por la velocidad de red, por establecer una VPN, etc. son:

- Snowball: servicio de transferencia de datos a escala de petabytes (PB, equivale a 10^{15} bytes) creado en un dispositivo seguro del tamaño de una maleta que migra datos hacia y desde la nube de AWS de manera rápida y eficiente. Los datos cargados en el dispositivo una vez llegan a AWS se cargan a un bucket de S3 del cliente.

  En la imagen 17 se puede ver la apariencia física del dispositivo proporcionado por AWS para hacer uso de Snowball.

Imagen 17. Snowball.

- Snowball Edge: cuenta con una capacidad levemente mayor a Snowball y una plataforma informática integrada que lo ayuda a realizar tareas de procesamiento simples. Estos dispositivos están pensados para clientes en entornos con conectividad intermitente (como fábricas, industrias y transporte) o en ubicaciones extremadamente remotas (como operaciones militares y marítimas) antes de devolverlos a los centros de datos de AWS.

  Las características principales de Snowball Edge son:
  - Mayor capacidad que Snowball
  - Existen tres versiones:
    - Almacenamiento optimizado: 80 TB, 24 vCPU y 32 GiB RAM
    - Edge Compute optimizado: 100 TB + 7.68 TB NVMe, 52 vCPU y 208 GiB RAM
    - Edge Compute optimizado con GPU
  - Se usa en el mismo tipo de situaciones que Snowballs, pero además cuando se requiere capacidad de cómputo.

  En la imagen 18 se puede ver la apariencia física del dispositivo proporcionado por AWS para hacer uso de Snowball Edge.

Imagen 18. Snowball Edge.

- Snowball Mobile: Transporta hasta 100 PB de datos (equivalente a 1250 dispositivos AWS Snowball) en un contenedor reforzado de 13,71 metros de longitud y es ideal para los cierres de centros de datos y las migraciones de medios digitales con escala de exabytes o varios petabytes.

  Un Snowmobile llega a las instalaciones del cliente y aparece como un almacén de datos conectado a la red

para lograr una transferencia de datos segura y de alta velocidad.

Una vez que los datos se hayan transferido a Snowmobile, se devuelve a la región de AWS en la que los datos deben cargarse a Amazon S3.

Snowmobile es resistente a manipulaciones, resistente al agua y cuenta con control de temperatura. Tiene varios niveles de seguridad física y lógica, que incluyen cifrado, extinción de incendios, personal de seguridad exclusivo, seguimiento por GPS, monitoreo con alarma, vigilancia por vídeo las 24 horas y un vehículo de seguridad escolta durante el traslado.

Obviamente se trata de un servicio que es bajo demanda y sólo está justificado su coste es circustancias especiales.

En la imagen 19 se puede ver la apariencia física del dispositivo proporcionado por AWS para hacer uso de Snowball Mobile.

Imagen 19. Snowball Mobile.

Por último, sobre la familia Snow*, en la imagen 20, se puede ver una comparativa entre AWS Snowball, AWS Snowball Edge y AWS Snowball Mobile.

	AWS Snowball	AWS Snowball Edge	AWS Snowmobile
Caso de uso	Migración de datos	Migración de datos con opciones de preprocesamiento integradas	Migración de datos
Capacidad de almacenamiento	50 TB a 80 TB	100 TB	100 PB
Opciones de informática integradas	N/D	AWS Lambda AMI de Amazon EC2	N/D
Cifrado	Sí, 256 bits	Sí, 256 bits	Sí, 256 bits
Se transfiere a través de NFS	N/D	Sí	Sí
Se transfiere a través de HDFS	Sí	N/D	N/D
Se transfiere a través de la API de S3	Sí	Sí	No
Agrupación	N/D	Sí, hasta 20 nodos	N/D
Montaje en bastidor	Estante	Sí	N/D
Cumple los requisitos de HIPAA	Sí	Sí	No
Plazo normal del trabajo	Días-semanas	Migración de datos: días-semanas Informática local: semanas-meses	Semanas-meses
Duración máxima del trabajo	90 días	Migración de datos: 90 días Informática local: 120 días	120 a 360 días

Imagen 20. Comparativa familia Snow*.

- **AWS Database Migration Service (DMS)**: proporciona ayuda para migrar las bases de datos a AWS de manera rápida y segura. La base de datos de origen permanece totalmente operativa durante la migración, lo que minimiza el tiempo de inactividad de las aplicaciones que dependen de ella.

  AWS Database Migration Service puede migrar datos hacia y desde la mayoría de las bases de datos comerciales de código abierto. Es compatible con Oracle, MSSQL, MySQL, MariaDB, PostgreSQL, MongoDB, Aurora y SAP.

  Admite migraciones homogéneas (motores de las bases de datos de origen y destino son iguales o compatibles), como de Oracle a Oracle, además de migraciones heterogéneas entre diferentes plataformas de base de datos, como de Oracle o Microsoft SQL Server a Amazon Aurora.

  En la imagen 21 se puede ver el funcionamiento para una migración entre bases de datos homogéneas. Dado que la estructura de esquemas, los tipos de datos y el código de base de datos son compatibles entre las bases de datos de origen y destino, este tipo de migración es un proceso de un solo paso.

Imagen 21. Migración BBDD homogéneas con DMS.

En el caso de migraciones heterogéneas (los motores de las bases de datos origen y destino son distintos), se puede usar la herramienta de conversión de esquemas (AWS Schema Conversion Tool - AWS SCT) para transformar entre diferentes motores de bases de datos como parte de una migración. En este caso, la estructura de esquemas, los tipos de datos y el código de base de datos de las bases de datos de origen y de destino pueden ser bastante distintos, y requerir una transformación de códigos y esquemas antes del comienzo de la migración de datos. Esto convierte a las migraciones heterogéneas en un proceso de dos pasos.

Primero se debe utilizar AWS SCT para convertir el código y el esquema de origen de modo que coincidan con los de la base de datos de destino. A continuación, se utiliza AWS Database Migration Service para migrar los datos de la base de datos de origen a la base de datos de destino. AWS Database Migration Service realiza automáticamente todas las conversiones de tipos de datos necesarias durante la migración. En la imagen 22 se puede ver el funcionamiento para una migración entre bases de datos heterogéneas.

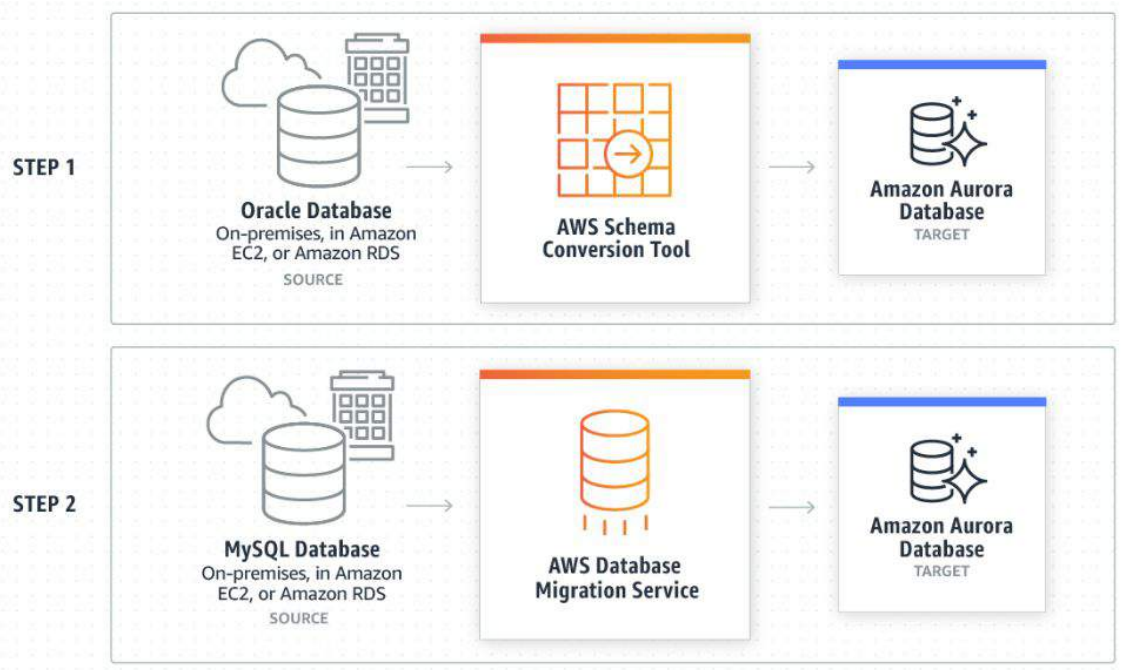

Imagen 22. Migración BBDD heterogéneas con DMS.

También AWS DMS cuenta con la posibilidad de volcar la información de la base de datos origen a dos bases de datos destino exactamente iguales manteniendo, por ejemplo, cada una de las bases de datos destino en regiones diferentes de la infraestructura de AWS con el objetivo de la distribución geográfica de bases de datos, sincronización entre los sistemas de desarrollo y testing, etc.

Otra posibilidad de uso del AWS DMS es consolidación de bases de datos para consolidar varias bases de datos de origen en una sola base de datos de destino.

- **AWS Storage Gateway**: servicio de almacenamiento híbrido que permite migrar datos a AWS, ampliando la capacidad de almacenamiento local mediante AWS. Hay tres tipos principales de Storage Gateway: file gateway, volume gateway, and tape gateway.

  Se trata un servicio de AWS basado en la descarga e instalación de una máquina virtual en el Centro de Procesamiento de Datos (CPD) del cliente que permite la conexión a AWS directa y transparente. Esta conexión puede hacerse a través de internet, a través de Direct Connect (que es una línea dedicada de AWS hasta el CPD del cliente) o a través de la VPC del cliente en AWS.

En la imagen 23 se puede ver una arquitectura típica y sencilla con AWS Storage Gateway como nexo entre CPD *On premises* y AWS.

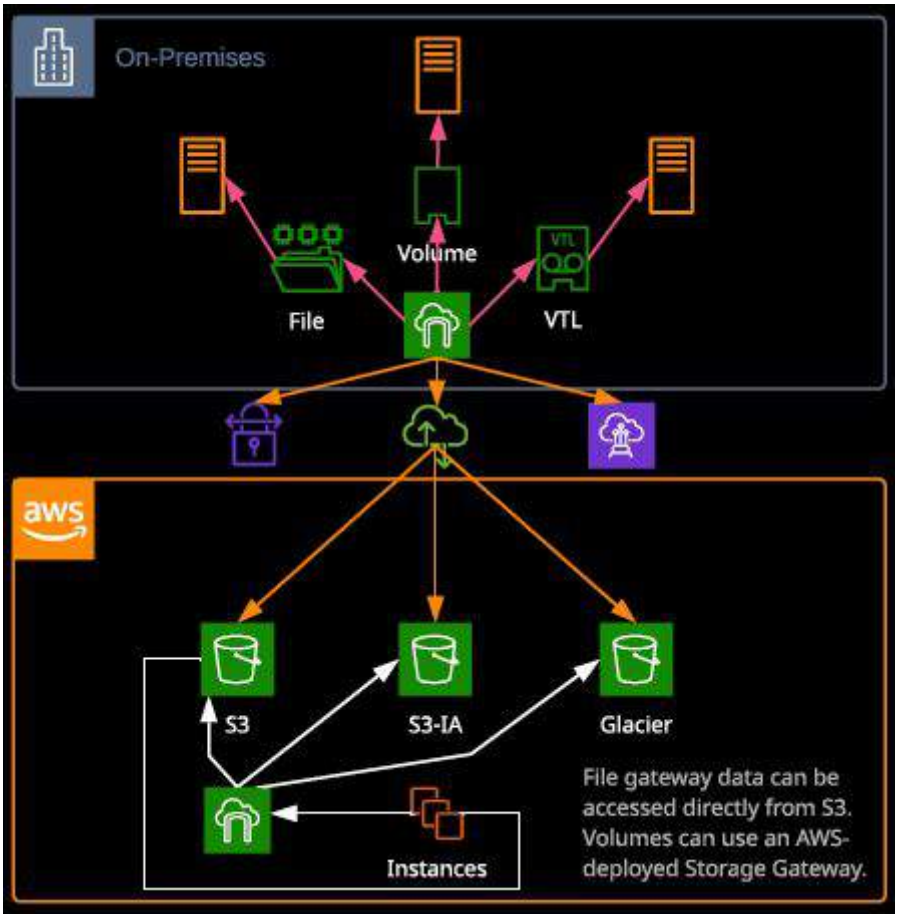

Imagen 23. Storage Gateway.

- Comunicaciones con AWS

A continuación se van a exponer algunos servicios que se han considerado de interés para el alcance de este trabajo. En concreto se van a detallar los servicios de DNS (Route 53 en AWS), AWS PrivateLink, AWS VPN y AWS Direct Connect.

  - **Route 53**: [18] servicio DNS de AWS. Se trata de un servicio global, es decir, no tiene ninguna región asociada. Permite registrar dominios, editar los registros asociados a estos (como los A, los CNAMES, los MX, etc.).

    Los Registros “A” hacen referencia a “Address" y es el parámetro que se devuelve con la IP vinculada al dominio, es decir, la IP del servidor que aloja la web de interés.

    AWS no sólo permite registrar dominio con ellos (pagando el registro del dominio), sino que además también permite gestionar

los name servers (servidores que se encargan de responder a las peticiones de DNS) y los registros DNS en estos. Si se quiere ahorrar los costes de los name servers (En torno a 1$ al mes por dominio), el cliente debe decirle a AWS que será quien aprovisione los name servers en otro sitio.

Existen cinco políticas de enrutamiento:

- Simple Routing Policy: Esta política permite un solo registro “A" con múltiples IP asociadas. Es decir, cuando se pregunte por un dominio DNS, AWS devolverá una IP de todas aquellas IP que el cliente haya registrado para ese dominio. La elección de la IP que se devuelva será completamente aleatoria.
- Weighted Routing Policy: Esta política permite balancear el tanto por ciento que se quiera de las solicitudes a una IP o a otra asignando un peso (weight) a cada IP que se registre como “A".
- Latency Routing Policy: Esta política permite devolver al cliente la IP del servidor que le ofrezca una menor latencia a este.
- Failover Routing Policy: Esta política permite informar de una o varias IP alternativas en caso de que las máquinas/servidores que alojen la web tras el dominio de la organización no estén disponibles por algún motivo. Para hacer uso de esta política, antes se debe crear lo que se denomina health check que no es otra cosa que solicitar a AWS que realice comprobaciones del estado de salud en el que se encuentra el servidor que aloja la web.
- Geolocation Routing Policy: Es prácticamente igual que la política de enrutamiento por latencia, pero en este caso el factor por el cual se determina el enrutamiento (la IP devuelva desde los servidores DNS) es la geolocalización de la petición origen.

- **AWS PrivateLink**: Servicio utilizado para conectar las VPC con servicios en AWS de manera segura y escalable. El tráfico que pasa por AWS PrivateLink no atraviesa Internet, lo que reduce la exposición a vectores de amenazas.

  También se utiliza para evitar que información de identificación personal atraviese Internet para seguir cumpliendo requisitos de conformidad, como los relacionados con la ley HIPAA o normativa PCI. Con AWS PrivateLink se puede compartir información de identificación personal de manera confidencial mediante la

conexión de recursos de AWS con servicios de AWS o VPC de organizaciones externas.

- **AWS VPN (Virtual Private Network)**: [19] AWS VPN se compone de dos servicios: AWS Site-to-Site VPN y AWS Client VPN.

  AWS Site-to-Site VPN permite conectar de forma segura la red local o el sitio de un CPD a Amazon Virtual Private Cloud (Amazon VPC) mientras que AWS Client VPN permite conectar con seguridad usuarios a redes locales o de AWS.

  AWS Site-to-Site VPN: Permite extender de forma segura la red del CPD tradicional con la nube. Utiliza el protocolo de seguridad de Internet (IPSec) para crear túneles de VPN cifrados entre dos ubicaciones. La imagen 24 ilustra el concepto de VPN entre AWS y el CPD tradicional.

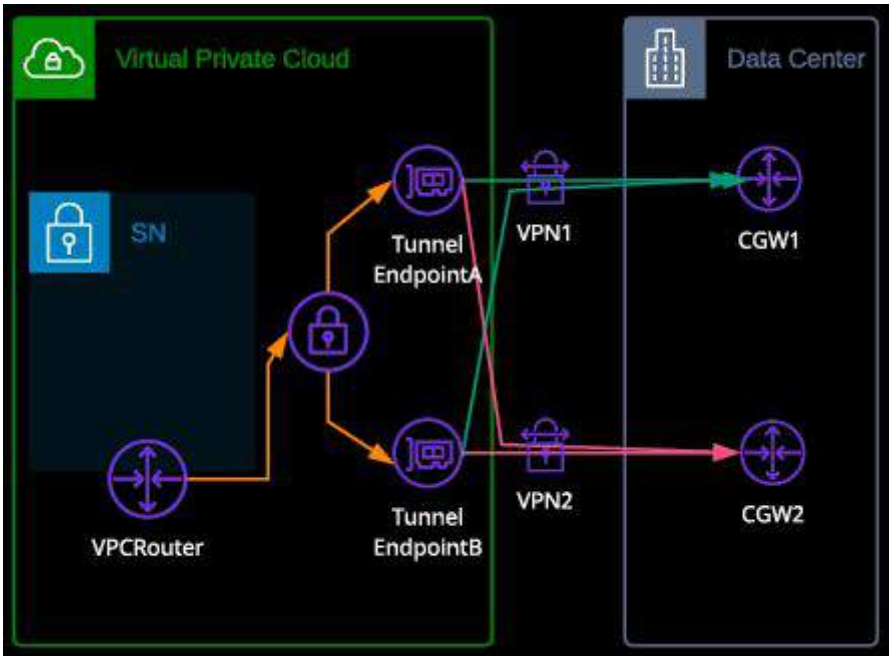

Imagen 24. AWS Site-to-Site VPN.

AWS Client VPN: servicio de VPN totalmente gestionado y elástico que aumenta o disminuye automáticamente el número de conexiones disponibles de Client VPN. No necesita instalar y gestionar un hardware o un software de VPN.

Este tipo de solución basada en VPN proporciona una solución de bajo coste, rápida de desplegar, flexible en cuanto al cambio de ubicación, muy útil para conectividades cortas en el tiempo y para conexiones que requieran cifrado.

Las VPN, como ya se ha descrito en los puntos anteriores, son

muy útiles para realizar comunicaciones entre subredes privadas. Uno de los casos de uso más extendidos son las conexiones entre los data centers on-premise y las VPC de AWS. Cuando una empresa tiene alojados datos en una red y requiere acceso a estos desde otra, las VPN se muestran como una solución barata, rápida, segura y efectiva, aunque siempre se ve superada por otros servicios como AWS Direct Connect.

Sin embargo, el alcance de Direct Connect puede verse limitado por la geografía y su implantación puede prolongarse mucho en el tiempo dadas sus características que se detallan a continuación.

- **Direct Connect**: Se trata de una conexión física directa entre la red del cliente y AWS. Las líneas dedicadas son de 1 Gbps con 1000Base-LX o 10 Gbps con 10GBASE-LR. Por lo tanto, permite establecer una conectividad privada muy rápida entre AWS y el CPD del cliente.

  Frente a la VPN tiene ventajas como, por ejemplo, mayor rendimiento y éste es constante al ser una línea física dedicada punto a punto, baja latencia, para grandes volúmenes de datos es más barato que una VPN.

  La imagen 25 muestra el concepto de Direct Connect entre AWS y el CPD tradicional.

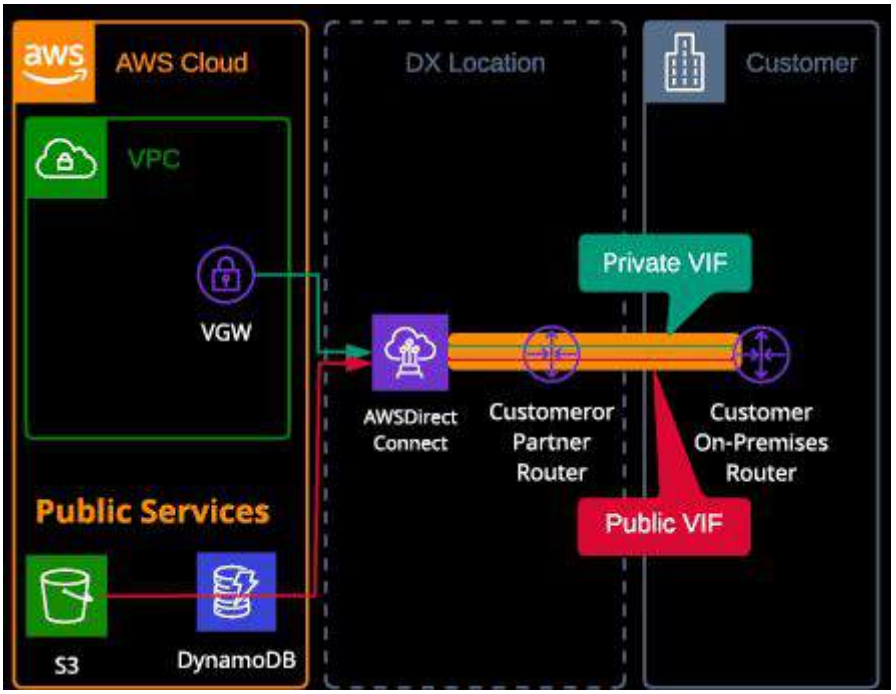

Imagen 25. Direct Connect.

Por último, únicamente se va a introducir en concepto de CASB (Cloud Access and Security Brokers (también conocidos como Cloud Security Gateways)), ya que se revisará algún producto de este tipo en el apartado 4 de este trabajo.

Un CASB sirve para descubrir el uso interno de servicios en la nube utilizando diversos mecanismos tales como monitorización de la red, integrándose con una puerta de enlace de red o herramienta de monitoreo existente. Muchos soportan DLP y otras alertas de seguridad.

2.5.2 Servicios de almacenamiento en AWS

En este apartado se pone el foco en algunos los servicios, siguiendo la clasificación de AWS, catalogados como almacenamiento y bases de datos en la imagen 14 con el objetivo de introducir al lector en las posibilidades que tiene una empresa tradicional para almacenar sus ficheros y datos en el entorno cloud de AWS. Para ello se enumeran y se definen algunos de los servicios de dichas categorías.

2.5.2.1 Almacenamiento en AWS

- **Amazon Simple Storage Service (Amazon S3)**: [20][21] Es un servicio de almacenamiento basado en objetos (ficheros, archivos), es decir, object based storage. Por lo tanto, no es válido para instalar un sistema operativo.

  El tamaño del fichero puede ser desde 0 Bytes hasta 5 TeraBytes. El objeto más grande que se puede cargar en un solo PUT es de 5 gigabytes. El almacenamiento máximo es ilimitado, aunque se paga por gigabyte utilizado.

  Los archivos se almacenan en buckets (cubos) que se comportan como carpetas en la nube. Este bucket debe de tener un nombre único a nivel global, y esto se debe a que cada bucket tendrá una dirección DNS a la cual se pueda acceder (de ahí que no pueda haber 2 buckets con el mismo nombre, independientemente de quién sea el dueño de estos).

  Los objetos que almacenemos en la nube consisten de:

  Key: Nombre del fichero.
  Value: Información que contiene el fichero. Cadena de bits que almacena los datos.
  Version ID: Identificador de la versión del fichero.
  Metadata: Tags, informacion de cuando se subió el fichero, etc.
  Access Control List (ACL): Listas de control de acceso a los ficheros.
  Torrent: Por si se quiere disponibilizar el fichero vía torrent.

S3 está construido para ofrecer un 99,99% de disponibilidad. AWS te garantiza un 99,9% de disponibilidad. AWS también garantiza un 99,999999999 % (son 11 nueves) de durabilidad.

No hay que confundir disponibilidad (poder acceder al recurso) con durabilidad (la información no se elimina por accidente) en S3.

Los objetos subidos a los bucket cuentan con una política de acceso privado por defecto. Es decir, se ha de habilitar el acceso a los recursos (de manera manual) si se quiere acceder a estos desde Internet.

Permite el versionado de los ficheros (una vez activado, sólo se puede deshabilitar pero no quitar permanentemente). En caso de estar habilitado, S3 almacena todas las versiones de los ficheros (lo que aumenta el coste). Se permite la replicación automática de los ficheros en otros buckets. Para ello es necesario tener habilitado el versionado.

Permite el cifrado de los datos. Dado que esta parte se revisará en el apartado 2.5.3 aquí sólo se enuncian las posibilidades:

- Amazon S3 Managed Keys (SSE-S3)
- KMS (Key Management Service SSE-KMS)
- Customer Provided Keys (SSE-C)

También se pueden configurar los buckets para que se generen logs con todos los registros de acceso y que se almacenen en un bucket distinto.

Permite el borrado de los ficheros únicamente a través de validación multifactor de autenticación (MFA).

Amazon S3 ofrece varios tipos de almacenamiento [22] diseñados para distintos casos de uso. Incluyen:

S3 Estándar: almacenamiento de objetos de alta durabilidad, disponibilidad y rendimiento para datos a los que se obtiene acceso con frecuencia.

Amazon S3 Intelligent-Tiering (S3 Intelligent-Tiering): diseñado para optimizar los costes mediante la migración automática de los datos a la capa de acceso más rentable, sin que impacte el rendimiento ni se produzca una sobrecarga operativa.

S3 Estándar - Acceso poco frecuente: se usa con datos a los que se obtiene acceso con menos frecuencia, pero que requieren un acceso rápido cuando es necesario.

S3 Zona única - Acceso poco frecuente: se usa con datos a los que se obtiene acceso con menos frecuencia, pero que requieren un acceso rápido cuando es necesario. A diferencia de las demás clases de almacenamiento de S3, que almacenan datos en un mínimo de tres zonas de disponibilidad (AZ), S3 Única zona – Acceso poco frecuente lo hace en una sola zona y cuesta un 20% menos que S3 Estándar - Acceso poco frecuente.

Amazon S3 Glacier (S3 Glacier): Es el almacenamiento más barato de Amazon y está pensado para almacenar la información a la que no se va a acceder un mucho tiempo. Es una clase de almacenamiento seguro, duradero y de bajo coste para el archivado de datos. S3 Glacier proporciona tres opciones de recuperación, que van desde unos pocos minutos a unas horas.

Amazon S3 Glacier Deep Archive (S3 Glacier Deep Archive): Es la clase de almacenamiento más económica de Amazon S3 y de S3 Glacier, admite la retención a largo plazo y la conservación digital de datos a los que se obtiene acceso una o dos veces al año.

Se diseñó para aquellos clientes que pertenecen a industrias con niveles de regulación muy estrictos, como servicios financieros, sanidad y sectores públicos, que retienen los conjuntos de datos durante un período de 7 a 10 años o más para cumplir los requisitos de cumplimiento normativo.

Para cumplir con las regulaciones, AWS S3 permite bloquear la escritura y el eliminado de los ficheros que se indiquen a través de la opción Object Lock (bloqueo de objeto). Para hacer uso de esta funcionalidad es necesario que el bucket de S3 tenga activado el versionado. En este modo, se determina el intervalo de tiempo por el cual el objeto permanecerá bloqueado, permitiendo únicamente la lectura de este. El intervalo de tiempo puede ser un periodo de retención (retention period) en el que se define el inicio y fin del periodo del bloqueo, o puede ser un bloqueo legal (legal hold) en el que no hay una fecha de expiración del periodo y el fichero permanece bloqueado hasta que se especifique lo contrario.

Se pueden definir dos tipos de bloqueo, *governance* y *compliance*. En *governance* las cuentas que se definan dentro de AWS tendrán permisos para quitar el bloqueo del objeto (y consecuentemente borrarlo después), pero únicamente esas cuentas. Sin embargo, en el modo *compliance*, ninguna cuenta puede retirar el bloqueo sobre el objeto y únicamente podrá ser borrado cuando realmente expire el periodo definido.

Amazon S3 también ofrece capacidades que se pueden configurar para administrar los datos a través de su ciclo de vida. Una vez configurada una política de ciclo de vida de S3, los datos se transferirán automáticamente a una clase de almacenamiento distinta sin generar ningún cambio en la aplicación.

En la imagen 26 se puede ver una comparativa del rendimiento [23] de las distintas clases de almacenamiento S3 ofrecidas por AWS.

	S3 Estándar	S3 Capas inteligentes*	S3 Estándar – Acceso poco frecuente	S3 Única zona – Acceso poco frecuente†	S3 Glacier	S3 Glacier Deep Archive
Diseñado para ofrecer durabilidad	99,999999999% (11 nueves)	99,999999999% (11 nueves)	99,999999999% (11 nueves)	99,999999999% (11 nueves)	99,999999999% (11 nueves)	99,999999999% (11 nueves)
Diseñado para ofrecer disponibilidad	99,99%	99,9%	99,9%	99,5 %	99,99%	99,99%
SLA de disponibilidad	99,9%	99%	99%	99%	99,9%	99,9%
Zonas de disponibilidad	≥3	≥3	≥3	1	≥3	≥3
Cargo mínimo de capacidad por objeto	N/D	N/D	128 KB	128 KB	40 KB	40 KB
Cargo mínimo por duración de almacenamiento	N/D	30 días	30 días	30 días	90 días	180 días
Tarifa de recuperación	N/D	N/D	por GB recuperado	por GB recuperado	por GB recuperado	por GB recuperado
Latencia de primer byte	milisegundos	milisegundos	milisegundos	milisegundos	minutos u horas seleccionados	horas seleccionadas
Tipo de almacenamiento	Objeto	Objeto	Objeto	Objeto	Objeto	Objeto
Transiciones del ciclo de vida	Sí	Sí	Sí	Sí	Sí	Sí

Imagen 26. AWS S3.

- **Amazon Elastic File System (Amazon EFS)**: [24] EFS es una implementación del Sistema de archivos de red (NFSv4) dada como un servicio. Los sistemas de archivos se pueden crear y montar en múltiples instancias de Linux al mismo tiempo.

  Cuenta con dos tipos de almacenamiento: estándar y acceso poco frecuente (EFS IA). Este último es más rentable en el caso de los archivos a los cuales no se necesita acceso diariamente. Además, con habilitar la administración del ciclo de vida de EFS, los archivos de acuerdo con la política de ciclo de vida que se configure se moverán de forma automática y transparente a EFS IA.

  Respecto a los usos para los que se ha diseñado este servicio son, por ejemplo, big data y análisis, flujos de trabajo de procesamiento multimedia, administración de contenido, servidores web y directorios de inicio.

- **Amazon Elastic Block Store (EBS)**: [25][26] Si se piensa en EC2, visto en el apartado 2.5, como un servidor virtual, entonces EBS es su disco duro virtual. Este servicio permite crear volúmenes de almacenamiento y conectarlos a las instancias de EC2. Una vez conectados, se puede crear un sistema de ficheros en ellos y almacenar bases de datos, ficheros, sistemas operativos, etc.

  Todos los tipos de volúmenes de EBS están diseñados para proporcionar una disponibilidad del 99,999 %.

  Los EBS no existen únicamente en un disco duro físico dentro de una única AZ (Availability Zone), sino que se replica automáticamente dentro de la AZ para prevenir la posible pérdida de datos. Sin embargo, no se replican entre distintas AZ.

  Si se busca alta disponibilidad y que el EBS no se vea comprometido, se deben realizar instantáneas (Snapshots) de este y almacenarlos en otras Availability Zones tal y como se observa en la imagen 27.

  Las instantáneas (snapshots) de EBS son una copia de seguridad en un punto en el tiempo concreto de un volumen de EBS almacenada en S3. La instantánea inicial es una copia completa del volumen, mientras que las instantáneas futuras sólo almacenan los datos modificados desde la última instantánea. Las instantáneas se pueden copiar entre regiones, compartir y automatizar utilizando Data Lifecycle Manager (DLM).

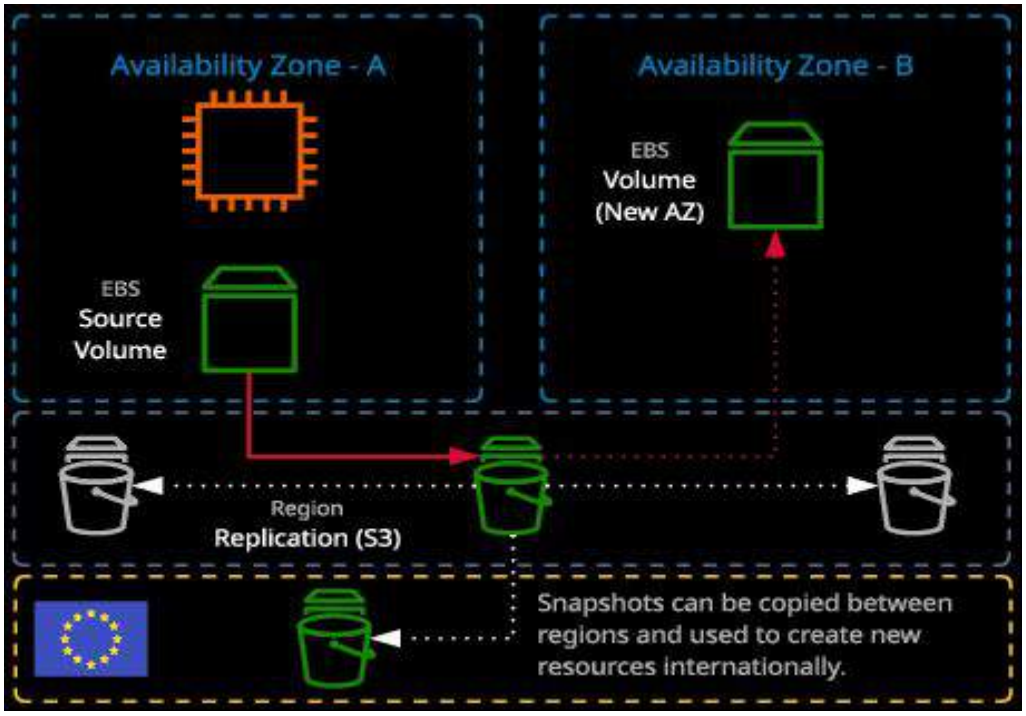

Imagen 27. Snapshots EBS.

Conviene diferenciar entre instantánea (Snapshot) y Amazon Machine Image (AMI). La instantánea es una copia (una foto instantánea) de un volumen EBS mientras que una AMI es una “copia" de una instancia EC2, es decir, una imagen. De hecho, cuando se crea una instancia EC2 con el ayudante de Amazon, cuando se elige el sistema operativo que se quiere instalar en la máquina, lo que se está seleccionando es una de las AMI que tiene Amazon por defecto.

La snapshot como foto instantánea que es, puede realizarse incluso sin que el EBS esté desconectado de la instancia EC2 (aunque es recomendable parar temporalmente las instancias EC2 al realizar las snapshots), permitiendo el normal funcionamiento del EBS tanto de lectura como de escritura mientras se realiza el proceso.

Por último, existen varios tipos de volúmenes de EBS que se muestran en la imagen 28.

	Unidades de estado sólido (SSD)		Discos duros (HDD)	
Tipo de volumen	SSD de IOPS provisionadas de EBS (io1)	SSD de uso general (gp2) de EBS*	HDD optimizados para procesamiento (st1)	HDD fríos (sc1)
Descripción corta	Volumen SSD de mayor rendimiento diseñado para cargas de trabajo transaccionales sensibles a la latencia	Volumen SSD de uso general que equilibra el precio y el rendimiento para una gran variedad de cargas de trabajo transaccionales	Volumen de HDD de bajo costo diseñado para cargas de trabajo de procesamiento intensivo a las que se accede con frecuencia	Volumen de HDD de costo más bajo diseñado para cargas de trabajo a las que se accede con menos frecuencia.
Casos de uso	Bases de datos relacionales y NoSQL con uso intensivo de operaciones de E/S	Volúmenes de arranque, aplicaciones interactivas de baja latencia, desarrollo y pruebas	Big data, almacenes de datos, procesamiento de registros	Datos más fríos que requieren menos escaneos diarios
Nombre de la API	io1	gp2	st1	sc1
Tamaño del volumen	De 4 GB a 16 TB	De 1 GB a 16 TB	De 500 GB a 16 TB	De 500 GB a 16 TB
IOPS máximas**/volumen	64 000	16 000	500	250
Procesamiento máximo***/volumen	1000 MB/s	250 MB/s	500 MB/s	250 MB/s
IOPS máximas/instancia	80 000	80 000	80 000	80 000
Procesamiento máximo/instancia	2375 MB/s	2375 MB/s	2375 MB/s	2375 MB/s
Precio	0,125 USD/GB-mes 0,065 USD/IOPS provisionadas	0,10 USD/GB-mes	0,045 USD/GB-mes	0,025 USD/GB-mes
Atributo de rendimiento dominante	IOPS	IOPS	MB/s	MB/s

Imagen 28. Tipos de volúmenes de EBS.

Una vez conocidos EC2, EBS, EFS y S3:

Amazon EFS es un servicio de almacenamiento de archivos para usar con Amazon EC2. Amazon EFS proporciona una interfaz de sistema de archivos, semántica de acceso a dicho sistema (como una consistencia sólida y bloqueo de archivos) y almacenamiento accesible de forma concurrente para miles de instancias de Amazon EC2.

Amazon EBS es un servicio de almacenamiento por bloques para utilizar con Amazon EC2. Amazon EBS puede ofrecer rendimiento para cargas de trabajo que requieran acceso con la mínima latencia a los datos desde una única instancia EC2.

Amazon S3 es un servicio de almacenamiento de objetos. Amazon S3 pone los datos a disposición de los usuarios a través de una API de Internet a la que se puede obtener acceso desde cualquier parte.

2.5.2.2 Bases de datos en AWS

Antes de comenzar a enumerar cada uno de los servicios de bases de datos que ofrece AWS, es necesario introducir el concepto de base de datos relacional y base de datos no relacional.

Las bases de datos relacionales, también conocidas como secuenciales o SQL (Structured Query Language) almacenan los datos como si fuera una “hoja de excel”.

El fichero Excel es la base de datos, siendo cada hoja una tabla, cada entrada en la tabla una fila y cada campo de la entrada una columna.

La principal característica que tienen las bases de datos secuenciales es que los datos que se introducen en la tabla deben corresponder con los campos (las columnas), es decir, estos no pueden tener más campos que aquellos que estén declarados en la tabla.

Las bases de datos NoSQL (Not Only SQL) no cuentan con tablas, filas y campos, sino que cuentan con colecciones (collections), documentos (documents) y pares de claves valor (Key Value Pairs) respectivamente. Estas bases de datos almacenan la información en formato JSON y la principal diferencia y ventaja con respecto a las bases de datos SQL es que pueden añadir campos (Key Value Pairs) de manera libre sin tener que modificar el resto de la tabla (collection).

AWS ofrece los servicios de bases de datos [27] mostrados en la imagen 29, adaptadas a cada caso de uso que necesite el cliente. En este trabajo se van a introducir las relacionales, clave-valor y en memoria.

Tipo de base de datos	Casos de uso	Servicio de AWS
Relacional	Aplicaciones tradicionales, ERP, CRM y e-commerce	Amazon Aurora, Amazon RDS, Amazon Redshift
Clave-valor	Aplicaciones web de alto tráfico, sistemas de e-comercio, aplicaciones de juegos	Amazon DynamoDB
En memoria	Almacenamiento en caché, gestión de sesiones, marcadores de juegos, aplicaciones geoespaciales	Amazon ElastiCache for Memcached Amazon ElastiCache for Redis
Documento	Gestión de contenidos, catálogos, perfiles de usuario	Amazon DocumentDB
Columna ancha	Aplicaciones industriales de gran escala para mantenimiento del equipo, administración de flotas y optimización de la ruta	Servicio Apache Cassandra administrado por Amazon
Gráficos	Detección de fraudes, redes sociales y motores de recomendaciones	Amazon Neptune
Series temporales	Aplicaciones de IoT, DevOps y telemetría industrial	Amazon Timestream
Contabilidad	Sistemas de registro, cadenas de suministros, registros y transacciones bancarias	Amazon QLDB

Imagen 29. Servicios de bases de datos en AWS.

- **Amazon Relational Database Service (Amazon RDS)**: [28][29] Servicio de bases de datos relacionales de AWS. Se trata de un producto de base de datos como servicio (DBaaS).

  Se puede usar para aprovisionar una base de datos completamente funcional sin la sobrecarga administrativa asociada tradicionalmente con las plataformas de bases de datos. Puede funcionar a escala, hacerse accesible al público y puede configurarse para los escenarios de durabilidad y disponibilidad que se requieran.

  RDS se puede implementar en modo AZ o Multi-AZ único (para resiliencia) y admite los siguientes tipos de instancias:
  - Propósito general
  - Memoria optimizada
  - Burst (ráfaga)

  RDS admite cifrado, pero el cifrado debe configurarse en el momento de creación de la base de datos. El cifrado no se puede eliminar.

  RDS es capaz de realizar diferentes tipos de copias de seguridad. Las copias de seguridad automatizadas a S3 se producen diariamente y se pueden conservar de 0 a 35 días. Las copias manuales se realizan de forma manual y existen hasta que se eliminen.

  Cuenta con varios tipos de instancias de base de datos (optimizadas para memoria, rendimiento u operaciones de E/S) y proporciona seis motores de bases de datos conocidos entre los que elegir, incluidos Amazon Aurora, PostgreSQL, MySQL, MariaDB, Oracle Database y SQL Server.

  Se puede usar AWS Database Migration Service (DMS, visto en el

apartado 2.5.1) para migrar o replicar las bases de datos, existentes en el CPD del cliente, en Amazon RDS con facilidad.

- **Amazon Aurora**: [30] Es un motor de base de datos desarrollado por AWS que es compatible con MySQL, PostgreSQL y herramientas asociadas. Aurora opera con una arquitectura radicalmente diferente en comparación con otros motores de bases de datos relacionales:
  - Aurora utiliza una configuración base de un "clúster"
  - Un clúster contiene una única instancia primaria y cero o más réplicas

  Según AWS, Amazon Aurora, es hasta cinco veces más rápida que las bases de datos de MySQL estándar y tres veces más rápida que las bases de datos de PostgreSQL estándar.

  Amazon Aurora está completamente administrada por Amazon RDS, que automatiza las tareas administrativas como el aprovisionamiento de hardware, la configuración de bases de datos, la aplicación de parches y las copias de seguridad.

- **Amazon Redshift**: [31] Es servicio que ofrece AWS para el Big Data. Está pensado para el almacenamiento gigante de datos (data warehouse) con querys muy complejas. Es escalable a niveles de petabyte, es muy rápida y potente y se basa en transacciones OLAP (On-Line Analytical Processing). Amazon RedShift únicamente opera en una única Availability Zone.

  Existen dos configuraciones posibles en función del tamaño de los datos:

  Single-Node: Un único nodo que permite almacenar hasta 160 GB de almacenamiento.

  Multi-Node: Para Big Data de mayor tamaño.

  Toda la información en tránsito de RedShift está cifrada vía SSL y, en reposo, está cifrada con AES-256.

- **Amazon DynamoDB**: [32][33][34] Es el servicio de AWS de bases de datos NoSQL (Not only SQL). Este servicio está 100% orquestado por AWS, por lo que no hay que preocuparse de las instancias, de los sistemas operativos y demás que haya por debajo del servicio, ya que AWS se ocupa de ello.

  Permite bases de datos basadas tanto en valores clave (key-value, es decir, con primary keys como en las SQL) como sin ellos, es decir, documentos.

  Es un servicio muy escalable. Ya no por la naturaleza de las bases de datos NoSQL, sino porque DynamoDB permite definir la capacidad de

lecturas y escrituras que se espera obtener y modificarla al vuelo, en vez de tener que hacer instantáneas (snapshots) como ocurre con RDS, por un precio más reducido y sin tiempos de indisponibilidad.

DynamoDB se almacena en SSD (solid-state drive) y en tres Availability Zones (AZ) distintas, así que cuenta con redundancia por defecto. El hecho de que la base de datos se separe en tres AZ hace que haya dos opciones para la lectura de esta: Eventual Consistent Reads y Strong Consistent Reads.

Eventual Consistent Reads: La consistencia de la información entre todas Availability Zones en las que esté repartida la base de datos se consigue normalmente en menos de un segundo, por lo que una lectura después de un breve lapso de tiempo de una escritura deberá dar el valor actualizado. Esta latencia se debe al tiempo que tarda en actualizarse la información en todas las Availability Zones.

Strongly Consistent Reads: Devuelve el dato actualizado en el mismo instante que se actualiza en todas las Availability Zones.

Existe un servicio extra dentro de DynamoDB llamado Amazon DynamoDB Accelerator, que reduce el tiempo de respuesta de la base de datos de milisegundos a microsegundos, muy útil cuando se quiere mejorar el rendimiento de una base de datos DynamoDB.

El cifrado de la base de datos también está permitido en este servicio pero, al igual que ocurre con RDS, la base de datos sólo puede ser cifrada en el momento de la creación. Si una base de datos ya existente no está cifrada, esta no podrá cifrarse. De igual manera, si la base de datos está cifrada, no podrá descifrarse. Para el tráfico de entrada y salida a la base de datos, se hace uso de SSL.

- **Amazon ElastiCache**: [35][36][37][38] Es un almacén administrado de datos en memoria que admite los motores Redis o Memcached. ElastiCache se usa comúnmente para dos casos de uso:

  - Descarga de lecturas de bases de datos almacenando en caché las respuestas, mejorando la velocidad de la aplicación y reduciendo los costes.

  - Almacenar el estado de la sesión del usuario, lo que permite instancias de proceso sin estado (utilizado para arquitecturas tolerantes a fallos).

  En función del uso que se le vaya a dar a ElastiCache se recomienda el uso de Redis (Remote Dictionary Server - servidor de diccionarios remoto) o Memcached. En ambos casos, a diferencia de las bases de datos que almacenan datos en el discos HDD o en discos SSD, ambos motores guardan sus datos en la memoria.

Redis está enfocado en la creación de aplicaciones en tiempo real en casos de uso versátiles como juegos, servicio geoespacial, almacenamiento en caché, etc.

Memcached está destinado a la creación de una capa de almacenamiento en caché sencilla y escalable para las aplicaciones con uso intensivo de datos.

2.5.3 Cifrado en cloud públicas

Como se vió en el apartado 2.1, uso de la cloud pública, apoyado sobre los datos proporcionados por Thales [1] en la RSA Conference 2020, cada vez hay más empresas que están migrando su infraestructura y sus datos a soluciones de proveedores cloud. Sin embargo, las políticas de seguridad sobre el cifrado de los datos que se están adoptando por parte de algunas organizaciones deja ver, que dichas organizaciones, tienen oportunidades de mejora sobre cómo almacenan sus datos.

Dado que el modelo de seguridad en la nube es un modelo de responsabilidad compartida, tal y como se refleja en las imágenes 5 y 6, que corresponden a los modelos de responsabilidad compartida de AWS y de Azure, respectivamente, el cliente debe preguntarse, ¿cómo almaceno los datos de mi organización en la nube? ¿Qué tipo de cifrado debo aplicar en función del dato que almaceno? ¿Cómo gestiono las claves de cifrado?

En la matriz de controles cloud (Cloud Controls Matrix - CCM) [39] de la Cloud Security Alliance (CSA) enfocada a la realización de *assessments* de seguridad de proveedores cloud, en las medidas referentes al dominio de Gestión de Claves y Cifrado (Encryption Keys Management - EKM) destacan cuatro controles:

- **EKM-01**: “Todas las decisiones de derechos deberán ser derivadas de las identidades de las entidades involucradas. Estas identidades deberán estar gestionadas por un sistema de gestión de identidades corporativo. Las claves deben tener propietarios identificables (vinculando las claves a las identidades) y deberá haber políticas de gestión de claves.”

- **EKM-02**: “Se establecerán las políticas y los procedimientos y se implementarán las medidas técnicas de apoyo para la gestión de claves criptográficas en los servicios (por ejemplo, la gestión del ciclo de vida desde la generación de la clave hasta la revocación y sustitución, la infraestructura de clave pública, el diseño del protocolo de criptografía y los algoritmos utilizados, el control de acceso en el lugar de generación de claves seguras, el intercambio y almacenamiento con segregación de claves utilizadas para cifrar los datos o sesiones). A petición, los proveedores deberán informar a los clientes de los cambios dentro de los sistemas criptográficos, especialmente si los datos del cliente se

utilizan como parte del servicio, y/o los clientes tienen alguna responsabilidad compartida sobre la implementación del control."

- **EKM-03**: "Se establecerán las políticas y los procedimientos y se implementarán las medidas técnicas de apoyo para el uso de protocolos de cifrado al objeto de proteger datos sensibles ubicados en los sistemas de almacenamiento (ejemplo: servidores de ficheros, bases de datos y estaciones de trabajo) y datos en transmisión (ejemplo: interfaces de sistemas, redes públicas y mensajería electrónica). Todo ello, bajo el marco de la leyes aplicables, las obligaciones legales, reglamentarias y de cumplimiento regulatorio."

- **EKM-04**: "La criptografía fuerte (por ejemplo, AES 256) en formatos abiertos/validados y los estándares de algoritmos deberán ser requeridos. Las claves no deben estar almacenadas en la nube (por ejemplo, en un proveedor de la nube). Las claves deberán ser mantenidas por el consumidor de la nube o el proveedor de gestión. La gestión de claves y el uso de las claves deberán tener funciones segregadas."

Para resolver el requisito EKM-04 existen, al menos, dos métodos de hacerlo:

- Bring Your Own Key (BYOK), es decir, las empresas generan sus propias claves de cifrado, en local, dentro de un HSM y decidiendo lo que pueden o no hacer con esa clave y, posteriormente, podrían exportarla de forma segura a la nube, para que únicamente allí, en dicha nube, se utilice dicha clave.

- Hold Your Own Key (HYOK), es decir, se trabaja con un HSM on premise o de un tercero para mantener la clave de cifrado de manera ajena a donde están alojados los datos cifrados. Se suele trabajar con HSM On premise y las claves de cifrado no salen de ahí.

En general, para que la migración y el almacenamiento de los datos cumpla con los estándares de seguridad de la industria se deben asegurar tanto las transferencias de datos a la nube, como el almacenamiento cifrado de los datos en la nube. [40]

Para realizar la migración de los datos a la nube ya se revisaron algunos servicios ofrecidos por AWS en el apartado 2.5.1, pero en general, para cualquier proveedor cloud se deberían tener en cuenta las siguientes directrices, siendo la primera básica y obligatoria, para realizar la migración de los datos:

1. Cifrado del canal haciendo uso de protocolos como TLS, SFTP, etc. La mayoría de las APIs de los proveedores de servicios en la nube utilizan Seguridad de Capa de Transporte (TLS). Cifrado en tránsito (cipher in transit).
2. Cifrar los datos antes de enviar a la nube (cifrado en el lado del cliente).

3. Cifrado basado en proxy, es decir, se instala un proxy de cifrado en un área de confianza entre el usuario de la nube y el proveedor de servicios cloud y el proxy gestiona el cifrado antes de transferir los datos hacia el proveedor.

Para el cifrado en reposo (at rest) en el proveedor de servicios cloud, las recomendaciones varían dependiendo del modelo de servicio (IaaS, PaaS y SaaS, vistos en el apartado 2.3) y del proveedor del servicio.

Respecto a la gestión de las claves de cifrado de los datos almacenados en el proveedor de servicios cloud existen varias opciones; El decantarse por unas u otras dependerá del usuario y lo que espere en cuanto al rendimiento, a la accesibilidad, a la latencia y a la seguridad.

Las opciones que existen para la gestión de claves son:

- HSM on premise: Utilizar un módulo de seguridad de hardware (HSM) tradicional, el cual típicamente requiere estar en instalaciones del cliente, y entregar las claves a la nube sobre una conexión dedicada. Solución BYOK vista en este mismo apartado.
- Appliance virtual/software: Instalar un gestor de claves basado en appliance virtual o en software, en la nube. Solución HYOK vista en este mismo apartado.
- Servicio de proveedor de servicios en la nube: Este es un servicio de gestión de claves ofrecido por el proveedor de servicios cloud. Por ejemplo, Key Management Service (KMS) de AWS que se expondrá a continuación.
- Híbrido: Utilizar una combinación de opciones, es decir, utilizar un HSM como la raíz de confianza para las claves, pero luego entregar claves específicas para cada aplicación a un appliance virtual que está ubicado en la nube y solo gestiona claves para un contexto particular.

2.5.3.1 Servicios de cifrado en AWS

En este apartado se pone el foco en algunos los servicios catalogados como seguridad, identidad y conformidad en la imagen 14 con el objetivo de introducir al lector en las posibilidades que tiene una empresa tradicional para el cifrado de sus ficheros y datos en el entorno cloud de AWS. Para ello, se enumeran y se definen algunos de los servicios de dichas categorías.

- **Cloud HSM (Cloud Hardware Security Module)**: [41][42] Un módulo de seguridad de hardware (HSM) proporciona seguridad para el almacenamiento de claves y las operaciones criptográficas en una unidad de hardware resistente a manipulaciones.

  Los dispositivos HSM están diseñados para almacenar de forma segura el material relacionado con las claves criptográficas y para utilizar dicho material sin exponerlo fuera de los límites criptográficos del hardware.

Estos dispositivos implementan medidas como el borrado automático de su contenido en caso de introducir mal la clave de descifrado un número determinado de veces, o ante la detección de un acceso no autorizado, o incluso la manipulación del hardware.

Para que las empresas puedan migrar completamente sus servicios a la nube y no haya que establecer conexiones con los HSM on-premise desde la nube (introduciendo latencias enormes), AWS ha puesto a disposición de los usuarios el servicio AWS Cloud HSM. De esta manera, los usuarios pueden almacenar sus claves asegurándose de que ellos sean los únicos que tengan acceso a este contenido y pudiendo cumplir las normativas vigentes para cada caso de uso.

Es más, haciendo uso de AWS Cloud HSM es la única manera en la que AWS no es capaz de manejar las claves. Con el resto de servicios de KMS, AWS las maneja de una manera u otra pero con AWS Cloud HSM no. Permite generar, almacenar, administrar y proteger las claves de cifrado de manera que estas claves sólo sean accesibles por el cliente o los usuarios autorizados, nadie más.

El servicio AWS Cloud HSM ha de usarse en una VPC, en una subnet (particularmente, en una Availability Zone), por lo que se recomienda encarecidamente que, con el fin de obtener alta disponibilidad, se haga uso de al menos dos AWS Cloud HSM ubicándose en distintas Availability Zones. En caso de contratar 2 o más AWS Cloud HSM, AWS lo muestra como uno único encargándose AWS de gestionar las copias de estas réplicas de AWS Cloud HSM.

Esta gestión puede hacerse gracias a que AWS organiza los Cloud HSM contratados en clusters, pudiendo tener un clúster de hasta 28 Cloud HSM repartidos en distintas Availability Zones, y balanceando el tráfico entre estos Cloud HSM.

AWS Cloud HSM permite administrar la infraestructura y replicación de los Cloud HSM mediante clusters de Cloud HSM, pero la gestión de las claves (que es lo importante) corre a cuenta del cliente. Si pierde las claves, el cliente habrá perdido todo lo que esté cifrado con dichas claves.

En resumen, las claves de cifrado se pueden transferir entre Cloud HSM y con otras soluciones de hardware on premise. No hay alta disponibilidad (HA) a menos que se desplieguen múltiples Cloud HSM. Si es así, las claves se comparten entre los Cloud HSM del clúster. Sin embargo, si se requiere tener control sobre el hardware físico sólo queda HSM on premise.

En la imagen 30 se puede ver una arquitectura sencilla con dos Cloud HSM en un clúster en distintas zonas de disponibilidad.

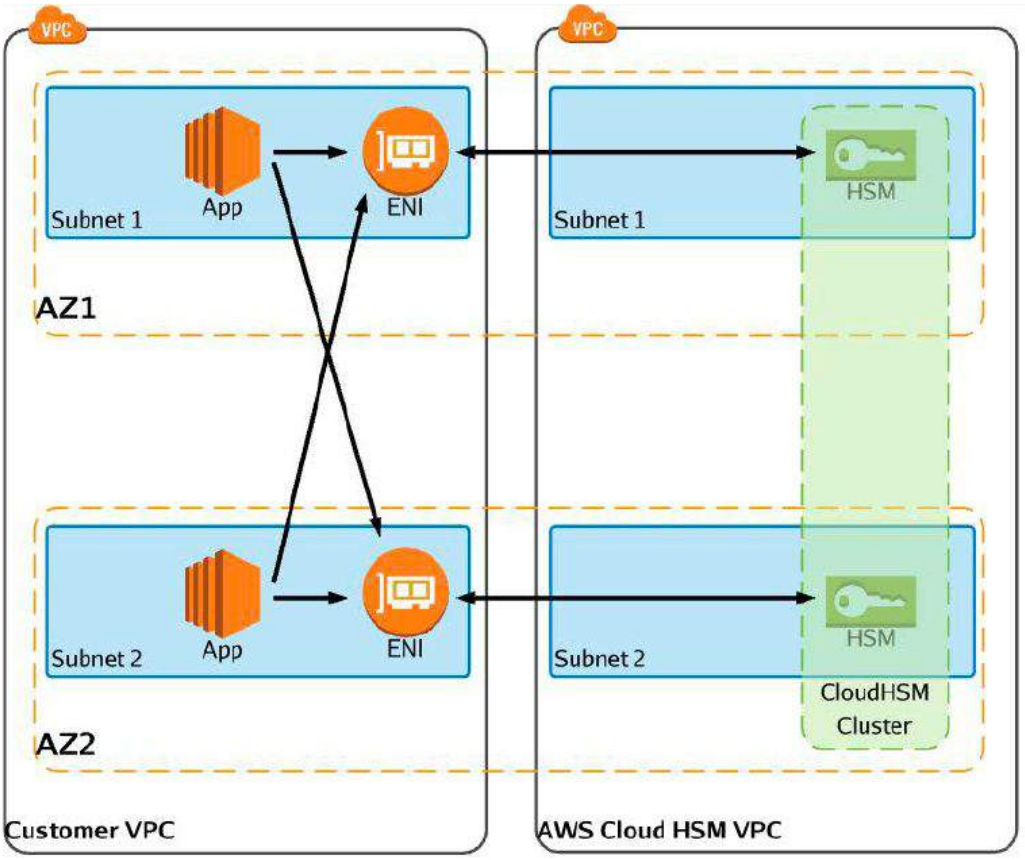

Imagen 30. Cloud HSM.

- **AWS Key Management Service (KMS - Servicio de gestión de claves)**: [43][44] Es un servicio de gestión de claves que utiliza módulos de hardware (HSM) que cumplen con FIPS 140-2 [45] para gestionar el acceso al material de cifrado. Se integra completamente con IAM y CloudTrail, servicios explicados en el apartado 2.5.4, para la gestión de permisos y funciones de auditoría. AWS KMS se puede utilizar opcionalmente con la mayoría de los servicios de AWS que admiten cifrado.

  En la imagen 31 se pueden ver los servicios de AWS que admiten cifrado.

Alexa for Business*	Amazon EMR	Amazon Relational Database Service (RDS)	AWS CodeCommit*
Amazon Athena	Amazon Forecast	Amazon S3	AWS CodeDeploy
Amazon Aurora	Amazon FSx for Windows File Server	Amazon SageMaker	AWS CodePipeline
Amazon CloudWatch Logs	Amazon Glacier	Amazon Simple Email Service (SES)	AWS Database Migration Service
Amazon Comprehend	Amazon Kendra	Amazon Simple Notification Service (SNS)	AWS Glue
Amazon Connect	Amazon Kinesis Data Streams	Amazon Simple Queue Service (Amazon SQS)	AWS Lambda
Amazon DocumentDB	Amazon Kinesis Firehose	Amazon Transcribe	AWS Secrets Manager
Amazon DynamoDB Accelerator (DAX)*	Amazon Kinesis Video Streams	Amazon Translate	AWS Snowball
Amazon DynamoDB	Amazon Lex	Amazon WorkMail	AWS Snowball Edge
Amazon EBS	Amazon Lightsail*	Amazon WorkSpaces	AWS Snowmobile
Amazon EC2 Image Builder	Amazon Managed Streaming for Kafka (MSK)	AWS Backup	AWS Storage Gateway
Amazon EFS	Amazon MQ	AWS Certificate Manager*	AWS Systems Manager
Amazon Elastic Transcoder	Amazon Neptune	AWS Cloud9*	AWS X-Ray
Amazon ElastiCache	Amazon Personalize	AWS CloudTrail	
Amazon Elasticsearch Service	Amazon Redshift	AWS CodeBuild	

** Admite únicamente claves de KMS administradas por AWS KMS.*

Imagen 31. Servicios de AWS que admiten integración con KMS.

AWS KMS es un servicio global, pero las claves son regionales. Es decir, no se pueden exportar las claves fuera de la región en la que se crearon, como son el caso de las CMK (que se verán qué son a continuación). Esto implica que, aunque se pueda llamar al servicio AWS KMS para cifrar o descifrar, no se podrá hacer uso directamente de las claves de una región distinta a la que se encuentre. En consecuencia, los servicios de AWS que directamente usen CMK, sólo podrán hacer uso de las claves ubicadas en su región y no en otra distinta.

Por ejemplo, si se tiene un EBS (recordad, “disco duro virtual” de un instancia EC2, visto en el apartado 2.5.2) cifrado en una región, pero se quiere llevar a otra región, puesto que el EBS estará cifrado por medio de una CMK regional, este no podrá funcionar directamente en la segunda región. Lo que se puede hacer es descifrar el EBS con la CMK regional (origen) y cifrarlo con una nueva CMK perteneciente a la segunda región (destino).

Se van a definir, aunque ya se habían mencionado, dos conceptos

importantes para el funcionamiento de AWS KMS, Customer Master Keys (CMK) y Data Keys (DEK, Claves de cifrado de datos).

- Customer Master Keys (CMK, Claves maestras del cliente): Son claves que se emplean para cifrar las Data Keys dentro del servicio KMS. Pueden cifrar hasta un tamaño máximo de 4 KB, pero únicamente se utilizan para cifrar, descifrar o generar claves (data keys). Existen varios tipos de CMK:

AWS Managed Keys: AWS se encarga de crear tanto las claves de cifrado (Data Keys) como la clave maestra (CMK) que las cifre, haciendo su uso transparente a los clientes. El cliente no podrá administrar las CMK. Es decir, AWS se encarga automáticamente de establecer fechas de caducidad a las CMK, de renovarlas (cada 3 años), de las políticas asociadas, etc.

Customer Managed Keys: El usuario es el encargado de crear, así como de asignar permisos de administración y/o uso a los distintos usuarios de la cuenta de AWS sobre las CMK. La renovación de las claves puede ser manual (si el cliente aporta el material criptográfico) o automática (si AWS se encarga de generar la nueva CMK, realizándose anualmente).

AWS owned CMK: En este caso las CMK no están en la cuenta del usuario porque pertenecen a otra cuenta. Este caso es muy típico cuando se hace uso de AWS Organizations. La cuenta padre es la que gestiona las claves maestras y las cuentas que dependen de ella no tienen acceso a las CMK para administrarlas.

- Data Keys (Claves de datos): Son las claves que se utilizan para cifrar los datos, incluidos ficheros de gran tamaño.

Es importante destacar que AWS nunca facilitará al usuario la clave maestra (CMK) de cifrado que se ha utilizado para cifrar las claves (data keys). Si se quiere usar una data key, bastará con referenciarla haciendo uso del alias que se le haya asignado en el momento de su creación y AWS se encargará de descifrarla y de usarla.

Por lo tanto, AWS KMS asume la responsabilidad de su durabilidad. AWS KMS almacena varias copias de las versiones cifradas de las claves en sistemas diseñados para ofrecer una durabilidad del 99,999999999 %, a fin de garantizar que la disponibilidad de las claves y de los datos sea muy alta.

Las CMK, por utilizar cifrados simétricos (las claves sirven para tanto para cifrar como para descifrar), si se borra la clave maestra, se pierde automáticamente todo lo cifrado con esa clave.

Debido a esto, AWS obligatoriamente establece un periodo mínimo de espera de 7 días, hasta 30 si así se solicita, desde que se pide borrar la

Customer Master Key (CMK) hasta que realmente se borra. Durante ese periodo de espera, no se puede utilizar la clave maestra para cifrar y tampoco para descifrar.

No obstante, AWS KMS ofrece la posibilidad de crear y utilizar CMK asimétricas y pares de claves de datos. Se puede indicar una CMK para utilizar como par de claves de firma o par de claves de cifrado. Las operaciones criptográficas asimétricas y la generación de pares de claves mediante el uso de estas CMK se realizan dentro de los HSM. Se puede solicitar la sección pública de la CMK asimétrica para utilizarla en las aplicaciones locales del cliente, pero la parte privada jamás abandonará el servicio.

También se pueden llevar claves propias a AWS KMS. Para importar una copia de la clave durante el proceso de importación, la clave estará envuelta en una clave pública proporcionada por AWS KMS para protegerla en el tránsito mediante el uso de uno de los dos esquemas RSA PKCS#1[4]. Eso garantiza que la clave cifrada sólo pueda ser descifrada por AWS KMS.

Por último, se van a exponer algunos ejemplos sobre cómo se utiliza AWS para la integración con otros servicios.

Para un volumen EBS, el cifrado se realiza utilizando la clave de datos generada a partir de una CMK. La clave de datos de cifrado se almacena con el volumen.

Para una una base de datos DynamoDB, para cualquier tabla cifrada creada en una región, DynamoDB utiliza KMS para crear un CMK predeterminado del servicio AWS/DynamoDB (en cada región). Cuando se crea una tabla y se indica que se cifre, esta CMK se usa para crear una clave de datos única para esa tabla, llamada clave de tabla (table key). DynamoDB administra esta clave y se almacena junto con la tabla de manera cifrada.

Cada ítem que DynamoDB cifra, se realiza con una clave de datos cifrada. Esa clave se cifra con esta clave de tabla y se almacena con los datos.

DynamoDB almacena en caché las claves de tabla (table key) hasta 12 horas en texto plano, pero se envía una solicitud a KMS después de 5 minutos de inactividad de la clave de tabla (table key) para verificar los cambios de permisos.

Para ilustrar el proceso se puede ver la imagen 32.

[4] https://tools.ietf.org/html/rfc8017

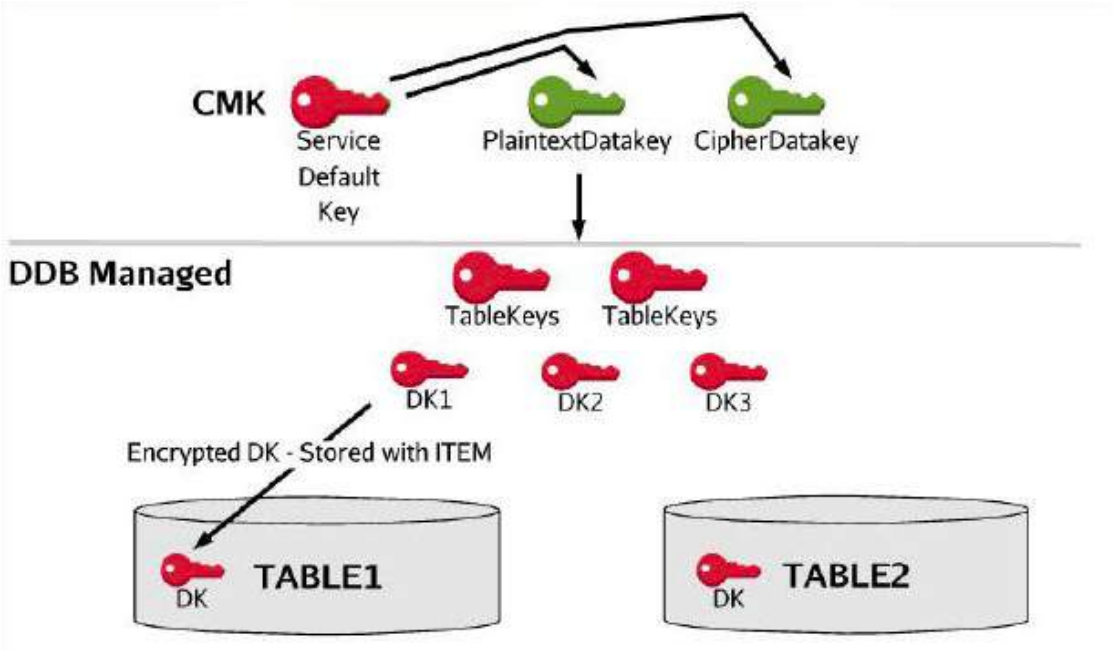

Imagen 32. KMS - DynamoDB.

Respecto a AWS S3, cada objeto en el bucket es cifrado por S3 utilizando la clave de datos (data key) provista por KMS. La clave de datos es generada desde un CMK. La clave de cifrado se almacena con el objeto como metadato. Cuando se requiere descifrar un objeto, la clave de cifrado se pasa a AWS KMS, éste descifra la clave de datos y es usada por AWS S3 para descifrar el objeto.

Las opciones para la generación de las claves de datos desde un CMK son las vistas anteriormente en este apartado. Por lo tanto, los objetos se cifran utilizando el cifrado del lado del servidor con las claves administradas de Amazon S3 (SSE-S3), o con las claves maestras del cliente (CMK) almacenadas en AWS KMS que se denomina S3 Customer Provided Encryption Keys (SSE-C).

Otra característica adicional es el forzar el cifrado de AWS S3. Por defecto, AWS S3 no cifra el bucket, los objetos se cifran y, como se ha visto, la configuración se define a nivel de objeto. Históricamente, no era posible definir el cifrado a un nivel de bucket, pero ahora sí se puede establecer el cifrado predeterminado en S3 a nivel de bucket.

Si se establece, cualquier objeto colocado en un bucket sin cabeceras de cifrado se cifra utilizando la configuración predeterminada a nivel de bucket.

Además, las políticas del bucket se pueden usar para denegar los intentos de añadir objetos al bucket con métodos de cifrado individuales.

- **AWS Certificate Manager**: [46][47] servicio que permite aprovisionar, administrar e implementar con facilidad certificados de seguridad de la capa de transporte (SSL/TLS) públicos y privados para su uso con servicios de AWS y recursos internos conectados.

  Los certificados públicos identifican recursos en el Internet público, mientras que los certificados privados hacen lo mismo en las redes privadas.

  Los certificados de SSL/TLS permiten a los navegadores web identificar y establecer conexiones de red cifradas con sitios web mediante la seguridad de la capa de transporte (SSL/TLS). Por lo tanto, se utilizan para el cifrado de los datos en tránsito (in transit) en comparación con los últimos apartados vistos que se ha hablado sobre cifrado en reposo (at rest).

  Los certificados se emiten con un sistema criptográfico conocido como infraestructura de claves públicas (PKI). PKI permite que una parte establezca la identidad de otra parte mediante el uso de certificados si ambos confían en un tercero, conocido como autoridad de certificación (CA).

  Las CA públicas, son las entidades que emiten los certificados públicos, y deben respetar normas estrictas, proporcionar visibilidad operativa y cumplir estándares de seguridad impuestos por los proveedores de sistemas operativos y navegadores, quienes deciden en qué CA confiarán automáticamente sus navegadores y sistemas operativos.

  La administración de las CA privadas [48] está a cargo de organizaciones privadas y los administradores de CA privadas pueden crear sus propias normas para la emisión de certificados privados. Para ello, AWS cuenta con AWS Certificate Manager (ACM) Private Certificate Authority, servicio de CA privadas que extiende las capacidades de administración de certificados de ACM a certificados públicos y privados.

2.5.4 Servicios de seguridad de AWS

Por último, esta sección únicamente pretende ser una introducción a algunos de los servicios de AWS más representativos que no se han tratado en apartados anteriores. No obstante, en la imagen 33 se pueden ver todos los servicios que AWS proporciona en cuanto a seguridad, identidad y conformidad/cumplimiento (compliance) con el caso de uso para el que fueron diseñados:

Categoría	Casos de uso	Servicio de AWS
Identity & Access Management	Administración de identidades para las aplicaciones	Amazon Cognito
	Microsoft Active Directory administrado	AWS Directory Service
	Administre el acceso de usuarios y las claves de cifrado	AWS Identity & Access Management (IAM)
	Servicio simple y seguro para compartir recursos de AWS	AWS Resource Access Manager
	Alterne, administre y recupere datos confidenciales	AWS Secrets Manager
	Servicio de inicio de sesión único (SSO) en la nube	AWS Single Sign-On
Controles de detección	Centro unificado de seguridad y conformidad	AWS Security Hub
	Servicio administrado de detección de amenazas	Amazon GuardDuty
	Analice la seguridad de las aplicaciones	Amazon Inspector
	Descubra, clasifique y proteja sus datos	Amazon Macie
	Investigue los posibles problemas de seguridad	Amazon Detective
Protección de infraestructuras	Protección frente a ataques DDoS	AWS Shield
	Filtre el tráfico web malintencionado	AWS Web Application Firewall (WAF)
	Administración central de reglas de Firewall	AWS Firewall Manager
Protección de datos	Administración y almacenamiento clave	AWS Key Management Service (KMS)
	Almacenamiento de claves en hardware a efectos de conformidad normativa	AWS CloudHSM
	Aprovisionamiento, administración e implementación de certificados públicos y privados SSL/TLS	AWS Certificate Manager
Conformidad	Portal gratuito autoservicio para el acceso bajo demanda a los informes de conformidad de AWS	AWS Artifact

Imagen 33. Servicios de seguridad, identidad y conformidad de AWS.

2.5.4.1 Identity & Access Management - Gestión de acceso e identidad

- **Amazon Cognito**: [49] Servicio que facilita la autenticación de los usuarios en un aplicativo. Este servicio facilita la implementación de protocolos de autenticación delegada como SAML 2.0[5] o mediante OAuth 2.0[6] para delegar la autorización en terceros como Facebook o

[5] http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.html
[6] https://tools.ietf.org/html/rfc6749 y https://tools.ietf.org/html/rfc6750

Google.

AWS Cognito ofrece 2 características principales a configurar: los User pools y los Identity Pools:

- User pool: Define los tipos de usuarios que habrán en el sistema y permite definir las normas o políticas que estos han de seguir como, por ejemplo, método de login en función del tipo de usuario, política de contraseñas, si es requisito tener validado el email o el teléfono móvil, posibilidad de permitir que el usuario sea recordado en el dispositivo que esté empleando para conectarse al aplicativo, etc.

- Identity pool: gestiona la delegación de la identificación/autenticación. Es decir, definir que los usuarios puedan hacer uso de su cuenta ya existente, por ejemplo, en Facebook o Twitter.

- **AWS Identity & Access Management (IAM - Gestión de acceso e identidad)**: [50][51][52] Se trata un servicio global, es decir, que no está asociado a ninguna región de AWS en particular y todos los cambios se aplican en todas las regiones.

  IAM se resume en la gestión de usuarios, grupos, roles y políticas de toda la cuenta/s de AWS.

  Usuario (user): Un usuario en IAM es una entidad única reconocida por los servicios y aplicaciones de AWS. Un usuario puede ser una persona, una máquina (como una instancia EC2) o una aplicación que solicite acceso a los servicios de AWS.

  El uso principal de los usuarios es dar a personas la posibilidad de autenticarse en la AWS Management Console o realizar llamadas a servicios AWS haciendo uso de las API o de la AWS CLI (AWS Command Line Interface).

  Un usuario consiste en un nombre, una contraseña para acceder a la consola, un Access ID y un Secret Access ID que serán las credenciales para acceder a AWS vía API o CLI.

  Cuando se crea un usuario, se le otorgan los permisos pertinentes haciéndole parte de un grupo (group).

  Grupo: Un grupo es un conjunto de usuarios de IAM. Pueden especificarse permisos a los grupos de tal manera que, cuando un nuevo usuario sea asignado a un grupo, automáticamente se le asignen los permisos correspondientes que pueda necesitar. De igual manera, si dicho usuario cambia de grupo, los permisos que tendrá este usuario también cambiarán de manera automática.

  Los grupos pueden contener muchos usuarios de IAM, y los usuarios

pueden estar en muchos grupos. Destacar que los grupos no tienen credenciales.

Rol (role): similar a un usuario, pero con la diferencia de que un rol no tiene ningún tipo de credenciales asociadas. Los roles no se pueden asignar a un usuario propio de la cuenta.

Los roles están pensados para ser asumidos bien por usuarios de otras cuentas ajenas a la del usuario, bien por un servicio que necesite permisos para realizar una tarea.

Un mismo rol puede ser asumido por más de un recurso a la vez, por lo que no hay que verlos como si fueran grupos de un único recurso/usuario de otra cuenta, sino más bien como un papel que puede ser asumido para realizar una acción específica.

Cuando se asume un rol, el service de token de seguridad (Security Token Service - STS) genera un conjunto de claves de acceso temporales. Estas claves de acceso temporal tienen los permisos definidos en la política de permisos. Por lo tanto, los roles de IAM no tienen credenciales a largo plazo (acceso basado en claves o nombre de usuario y contraseña).

Política (policy): Una política de IAM es un documento JSON que describe los permisos y derechos que se le asignan a un usuario, grupo o rol. Una política no tiene ningún tipo de efecto hasta que se asigna a un usuario, a un grupo o a un rol.

Existen tres clases de políticas:

- AWS-Managed Policies: políticas gestionadas por AWS. Estas políticas predeterminadas se pueden asignar y utilizar directamente.

- Customer-Managed Policies: políticas creadas y gestionadas por los usuarios.

- Inline Policies: En caso de que se quiera asignar un permiso de manera exclusiva a un usuario o a un recurso, y no se quiera que por error dicho permiso sea asignado a otro usuario o recurso, se usan las Inline Policies. Estas políticas se asocian directamente uno a uno a un recurso o a un usuario. Si el recurso o usuario son eliminados, las políticas asociadas también se eliminan.

  Estas políticas no pueden ser compartidas. AWS recomienda el uso de las Customer-Managed Policies antes que las Inline Policies.

Un ejemplo sencillo de política de AWS es el siguiente:

```
{
      "Version": "yyyy-mm-dd",
      "Statement": {
      "Effect": "Allow",
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::example_bucket"
      }
}
```

Se compone de los campos Statement, Effect, Action y Resource. Todos ellos obligatorios.

Statement: Es el elemento principal para definir una política.
Effect: Únicamente puede tener 2 valores: Allow (Permitir) o Deny (Denegar).
Action: Se define la acción que se está permitiendo o denegando.
Resource: Define sobre qué recurso/s aplica la política.

La versión simplemente hace referencia a la propia versión de la política. Si este campo existe, es porque se pueden tener dos tipos de versiones distintas para definir una política en IAM. AWS recomienda que se haga uso únicamente de la versión más reciente.

Existe un campo adicional y opcional, llamado Principal, que define quién tiene permiso para realizar la acción (action) sobre el recurso (resource). Normalmente se utiliza para usuario ajenos a la cuenta de AWS, pero puede utilizarse a la hora de definir una política para acotar más el alcance de los permisos asociados.

ARN, son las siglas de Amazon Resource Name, y se utilizan como identificador único de un recurso de Amazon. Es decir, cada instancia EC2, cada bucket, cada base de datos, etc., tendrá un identificador único ARN.

ARN siempre comienza con:

```
arn:partition:service:region:account-id:
```

Y, dependiendo del servicio, finaliza con:

```
resource
resourcetype/resource
resourcetype/resource/qualifier
resourcetype/resource:qualifier
resourcetype:resource
resourcetype:resource:qualifier
```

Los campos con `::` omiten el valor, y `*` es un comodín. Por ejemplo:

```
arn:aws:s3:::documentosUOC/*
```

De manera resumida, AWS evalúa [53] las distintas políticas que pueda haber sobre un mismo recurso tal y como se muestra en la imagen 34:

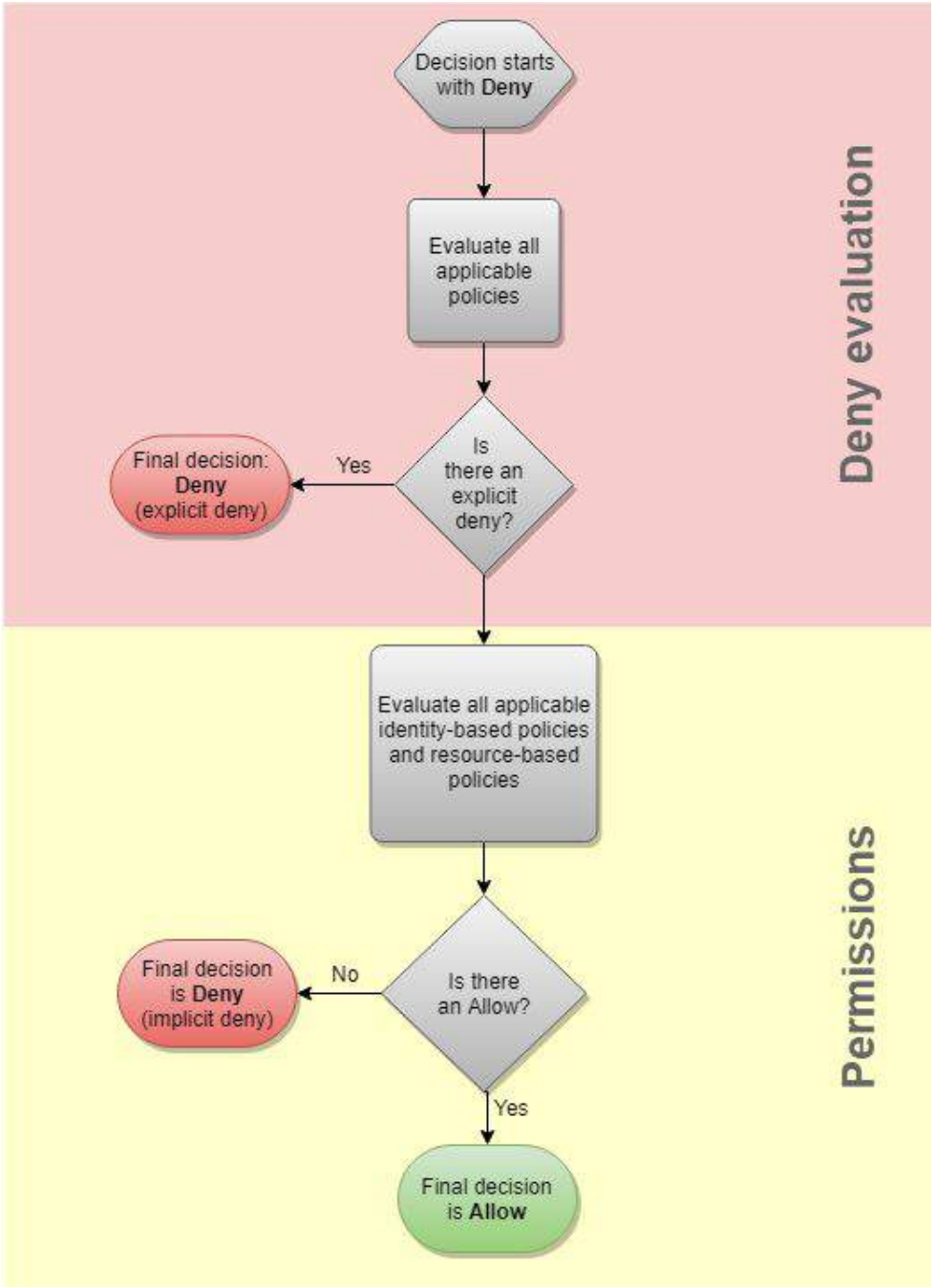

Imagen 34. Decisión aplicación políticas AWS.

Por lo tanto, la política por defecto de AWS es denegar el permiso. En el siguiente paso, AWS comprueba si existe alguna política de denegación de permiso explícita. En ese caso, deniega el acceso y finaliza la

evaluación. En caso de que no exista la política expresa de denegación, comprueba si existe alguna política que autorice expresamente el acceso al recurso. En caso de que no exista, de la misma manera, se deniega el acceso y se finaliza la evaluación. En caso de que sí haya encontrado una sentencia que permita el acceso al recurso, se permite.

En resumen, en caso de tener sentencias contradictorias en las políticas se deniega. Y en caso de que no haya ninguna sentencia que permita expresamente el acceso al recurso también se deniega.

- **AWS Secrets Manager**: [54][55] Servicio que permite administrar, recuperar y rotar credenciales de bases de datos, claves de API, tokens de OAuth y otros datos confidenciales durante su ciclo de vida. Los datos confidenciales se recuperan con una llamada a las API de Secrets Manager, lo que elimina la necesidad de codificar la información en texto plano.

  AWS Secrets Manager cifra en reposo (at rest) utilizando claves de cifrado que posee y almacena en AWS Key Management Service (KMS). De forma predeterminada, Secrets Manager no escribe ni almacena en caché ningún dato confidencial para almacenamiento persistente.

  AWS Secrets Manager utiliza AES-256 para cifrar sus datos confidenciales en AWS KMS. Cuando se utiliza Secrets Manager por primera vez, se puede especificar las claves maestras del cliente (CMK) para cifrar datos confidenciales. Si no se proporciona una CMK, Secrets Manager crea automáticamente las claves predeterminadas de AWS KMS.

  AWS Secrets Manager permite controlar el acceso a los datos confidenciales a través de las políticas de AWS IAM. Cuando recupera un dato confidencial, Secrets Manager lo descifra y lo transmite de forma segura a través de TLS.

  Este servicio se cobra por la cantidad de datos confidenciales que almacena y por las solicitudes al API del servicio.

- **AWS Single Sign-On (SSO)**: [56][57] Este servicio permite administrar de forma centralizada el acceso a múltiples cuentas de AWS y a aplicaciones propias de la organización, además de proporcionar a los usuarios un acceso de inicio de sesión único (SSO) a todas las aplicaciones y las cuentas asignadas.

  Posibilita la administración del acceso SSO y los permisos de usuario a todas sus cuentas de AWS Organizations de forma centralizada. Permite asignar permisos de usuario basados en funciones de trabajo comunes y personalizarlos para que se cumplan los requisitos de seguridad. AWS

SSO también incluye integraciones nativas para muchas aplicaciones empresariales, como Salesforce, Office 365, etc.

Con AWS SSO, se pueden crear y administrar identidades de usuario en el almacén de identidades de AWS SSO, o conectarse a un directorio activo donde estén los empleados de la organización, como Microsoft Active Directory y Azure Active Directory (Azure AD).

Si se pretende establecer SSO entre una empresa y AWS para que los empleados puedan acceder a la consola de AWS sin tener que volver a introducir sus credenciales corporativas, son necesarias dos cosas:

1. Crear una conexión Direct Connect con Amazon. Es decir, tener un cable de fibra dedicado desde el data center del cliente hasta AWS.
2. Crear en IAM un rol (role) que establezca la relación de confianza entre IAM y el directorio activo de la empresa que hace de IdP (Identity Provider).

2.5.4.2 Controles de detección

- **Amazon GuardDuty**: [58] Servicio que monitoriza de forma continua la seguridad de la VPC del cliente a partir de logs. Estos logs son los logs de flujo de la VPC (Flow Logs), logs de eventos de AWS CloudTrail y logs de DNS.

  Haciendo uso de un aprendizaje automático, ayuda a detectar actividad inesperada a partir fuentes de información de amenazas (como listas de direcciones IP y dominios maliciosos).

  GuardDuty facilita la detección de escalado de privilegios, uso de credenciales expuestas, malware o incluso minado de bitcoins.

  Permite configurar listas blancas de IP para no alertar de falsos positivos.

  GuardDuty es capaz de detectar un ataque de fuerza bruta y actuar en consecuencia, pero no es capaz de afrontar un ataque de DDoS.

  No tiene coste inicial y sólo se paga por los eventos analizados, no es necesario software adicional para implementar este servicio ni suscripción a fuentes de amenazas.

- **Amazon Inspector**: [59][60] Es el analizador de vulnerabilidades de AWS para su nube. Este servicio que AWS ofrece puede analizar la plataforma del cliente basándose en los Assessment Rules (o reglas de evaluación) que se le indique. Para poder realizar estos escaneos o análisis, AWS Inspector se ayuda de un agente que se ha de instalar en

aquellos servidores que se quieran analizar.

Destacar que, AWS Inspector no parchea las vulnerabilidades que detecte, únicamente informa de ellas. No se pueden crear análisis personalizados con AWS Inspector, únicamente se pueden solicitar los análisis que la propia herramienta ofrece.

AWS Inspector se basa en 4 puntos a la hora de realizar sus análisis:

- Buenas prácticas en seguridad: Se comprueban si las buenas prácticas de seguridad han sido implementadas correctamente. Estas son:
  - Deshabilitar el acceso a la cuenta root por SSH.
  - Tener habilitado únicamente la conexión por SSH con la version v2.
  - Deshabilitar la autenticación por contraseña a través de SSH.
  - Configurar políticas de contraseñas que tengan en cuenta el tiempo de vida, la longitud y la complejidad de las mismas.
  - Habilitar Address Space Layout Randomisation (ASLR) y Data Execution Prevention (DEP).

    Address Space Layout Randomisation (ASLR) y Data Execution Prevention (DEP) son dos medidas de seguridad que evitan la ejecución de exploits en las máquinas.
  - Configurar correctamente los permisos en los directorios.

- Análisis de comportamiento: Comprueba que el comportamiento de la instancia y alerta en caso de que detecten protocolos de comunicación inseguros contra clientes u otros servidores, puertos TCP abiertos y software sin ASLR o sin DEP.

- CVE: El agente de Inspector, una vez instalado en el servidor, se encarga de hacer un listado de todas las versiones de todos los paquetes o programas instalados en el sistema. Una vez hecho el listado, AWS Inspector consulta a la web de CVE[7] para verificar si las versiones instaladas cuentan con vulnerabilidades detectadas. Similar al programa “Nessus”, pero en vez de pagar una licencia se paga por análisis realizado.

- CIS Benchmark de Sistemas Operativos: AWS Inspector comprueba que el servidor cumple los requisitos necesarios de “hardening" determinados en el CIS para sistemas operativos. Únicamente se limita a comprobar los requisitos de las máquinas Linux de sus AMI (Amazon Machine Image).

[7] https://cve.mitre.org/

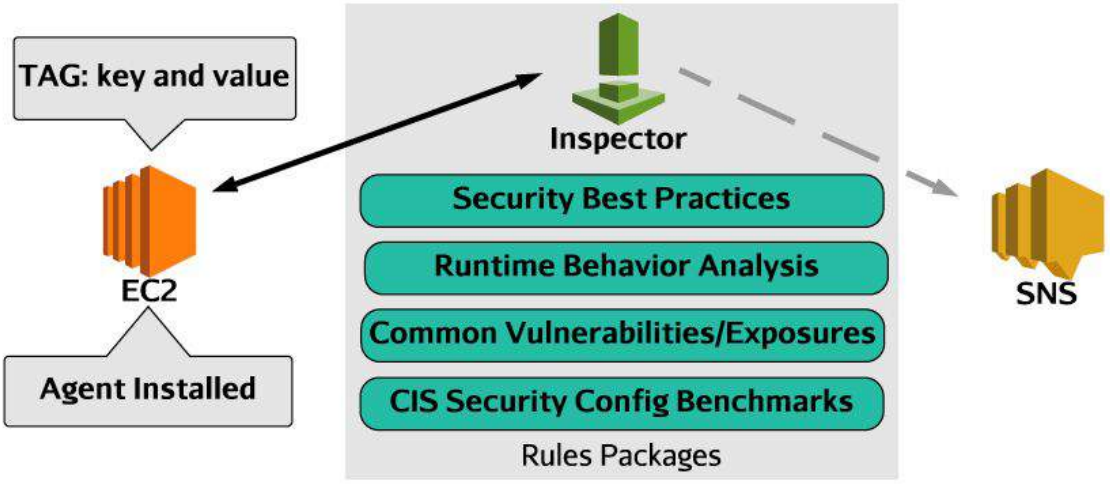

Imagen 35. AWS Inspector.

- **Amazon Macie**: [61][62] Servicio de seguridad que utiliza el aprendizaje automático para detectar, clasificar y proteger información confidencial automáticamente en AWS.

  Macie es compatible con Amazon S3 y la API de administración de AWS CloudTrail y eventos a nivel de objeto S3 para los buckets y prefijos inscritos en Amazon Macie. Únicamente buscará información no cifrada en los buckets de S3, ya que en caso de estar cifrada, obviamente, AWS Macie no podrá detectarla.

  Macie es capaz de detectar información como números de tarjetas de crédito, números de cuentas bancarias, credenciales de Amazon, números de teléfono, números de identificación personales, número de la seguridad social, etc. La clasificación de objetos por información personal identificable (PII) se basa en el reconocimiento de cualquier dato personal identificable según los estándares del sector, tales como NIST-80-122 o FIPS 199. [63]

  Para ello, Macie hace uso de expresiones regulares a las que les asigna un nivel de riesgo. Cuando se lanza el servicio y encuentra un patrón que se asemeje a una expresión regular, éste lo dejara indicado en el dashboard, e incluso podrá enviar una alerta, con su nivel de criticidad asociado. [64]

  El problema es que actualmente, marzo de 2020, este servicio de AWS sólo está disponible en dos regiones de Estados Unidos: US East (N. Virginia) (us-east-1) y US West (Oregon) (us-west-2).

- **Amazon Detective**: [65] Este servicio facilita el análisis, la investigación y la identificación de la causa raíz de posibles problemas de seguridad o actividades sospechosas. Para ello, recopila datos de logs de manera

automática a partir de los recursos del cliente en AWS y utiliza el aprendizaje automático, el análisis estadístico y la teoría de gráficos para crear un conjunto de datos vinculados que le permite llevar a cabo fácilmente investigaciones sobre la seguridad.

Amazon Detective recopila y analiza eventos de orígenes de datos, como AWS CloudTrail, logs de flujos de VPC y hallazgos de Amazon GuardDuty, esto último si se tiene habilitado en la cuenta de AWS.

Amazon Detective está disponible, a marzo de 2020, en versión preliminar en las siguientes regiones: EE. UU. Este (Norte de Virginia), EE. UU. Este (Ohio), EE. UU. Oeste (Oregón), UE (Irlanda) y Asia Pacífico (Tokio).

2.5.4.3 Protección de infraestructuras

- **AWS Shield**: [66] Servicio de protección contra DDoS (Distributed Denial of Service - ataque distribuido de denegación de servicio). Siempre está activo, se encarga de detectar y minimizar los ataques, de tal forma que las latencias y tiempos de caída queden reducidos lo máximo posible.

  Existen 2 modalidades: Standard y Advanced. Todo el mundo cuenta con la protección standard sin coste adicional mientras que la versión advanced sí que supone un coste adicional.

  AWS Shield Standard proporciona protección para todos los clientes de AWS ante ataques comunes que normalmente ocurren en la infraestructura (capas 3 y 4) como ataques flood SYN/UDP, ataques de reflexión, etc. para respaldar la alta disponibilidad de las aplicaciones en AWS. Además incluye WAF sin coste adicional.

  AWS Shield Advanced ofrece una protección optimizada para las aplicaciones que se ejecutan en recursos protegidos de Amazon EC2, Elastic Load Balancing (ELB), Amazon CloudFront, AWS Global Accelerator y Route 53 contra ataques mayores y más sofisticados. La protección de AWS Shield Advanced ofrece monitorización siempre activa del tráfico de red y monitorización de aplicaciones activas para proporcionar notificaciones casi en tiempo real de supuestos incidentes de DDoS.

  También el servicio avanzado cuenta con soporte 24x7 del equipo de respuesta a DDoS (DRT - DDoS Response Team) para tener asistencia durante un ataque.

  Por lo tanto, AWS Shield se encarga de proteger los principales puntos más vulnerables a los ataques DDoS como lo son las instancias EC2,

ELB, CloudFront y Route53.

- **AWS Web Application Firewall (AWS WAF)**: [67] AWS WAF es un firewall para aplicaciones web que ayuda a proteger a las aplicaciones web contra ataques al permitir configurar reglas que habilitan, bloquean o monitorizan (cuentan) las solicitudes web a partir de las condiciones que el cliente defina. Las condiciones incluyen direcciones IP, encabezados HTTP, cadenas URI, inyección de código SQL y scripting entre sitios.

  El servicio AWS WAF se cobra en función del número de listas de control de acceso web (ACL web) que se creen, del número de reglas que se añadan por ACL web y del número de solicitudes web que se reciban.

  AWS WAF sólo puede asociarse a una distribución de AWS CloudFront (para nivel global), o bien a API Gateway, o ALB (Application Load Balancers, para nivel regional).

  Tras determinar el ámbito de aplicación, se deben determinar las condiciones como, por ejemplo, que el tráfico sea desde una IP específica, que un cabecera (header) en una petición HTTP contenga un valor determinado o que los valores introducidos en un formulario y enviados en un POST se asemejen a una SQL Injection. Con estas condiciones ya se pueden definir reglas simples (1 regla - 1 condición) o complejas (1 regla - varias condiciones) y se compararán con el tráfico recibido.

  Si existen múltiples condiciones en un regla, el resultado del análisis debe incluir todas las condiciones.

  Por ejemplo, una regla que indique bloquear el tráfico desde la red 2.2.0.0/16 que tenga apariencia de tener un código SQL, sólo bloqueará las peticiones que cumplan con ambas condiciones como puede observarse en la imagen 36.

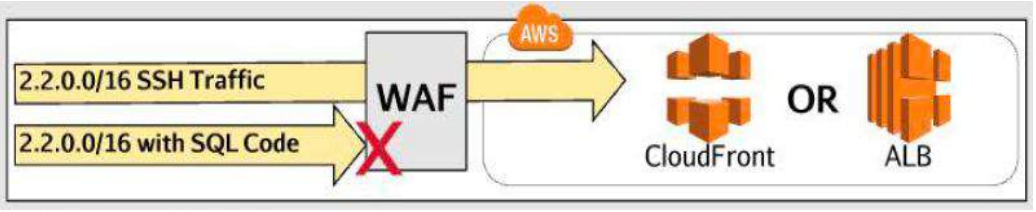

Imagen 36. AWS WAF - Regla con varias condiciones.

- **AWS Firewall Manager**: [68] Este servicio permite centralizar la gestión de todas las reglas de *firewall* que aplican en una organización.

  Es decir, permite aplicar políticas automáticamente en los recursos de

AWS que existen actualmente o que se creen en el futuro para así garantizar el cumplimiento de las reglas de *firewall* en toda la organización.

Por lo tanto, de manera centralizada se puede responder rápidamente a los incidentes de seguridad, por ejemplo, bloqueando una dirección IP o aplicando una actualización de parche CVE para toda la organización y todas las cuentas asociadas (AWS Organizations, visto en la sección 2.5).

Cada política de Firewall Manager puede configurar reglas de WAF para un máximo de 2500 cuentas, que es el límite predeterminado para la cantidad de cuentas en AWS Organizations.

En AWS Firewall Manager se puede configurar una política en dos modos:

- Solución automática: permite monitorizar automáticamente los cambios en las políticas y aplicar reglas sobre los recursos que no cumplan con los requisitos.
- Solución manual: crea una nueva política y los grupos de reglas WAF asociados en cada cuenta, pero no aplica las reglas sobre los recursos de la cuenta.

AWS Firewall Manager permite al administrador de las reglas de *firewall* de una empresa visualizar en un panel de cumplimiento de este servicio para cada política qué cuentas están cumpliendo o que cuentas no lo están haciendo. Además, en el caso de no cumplir con los requisitos se pueden crear notificaciones en tiempo real que alerten de esta situación.

2.5.4.4 Protección de datos

Los servicios de AWS de esta sección ya se han introducido en este trabajo, en concreto, en el apartado 2.5.3.1 Cifrado en AWS.

2.5.4.5 Conformidad

- **AWS Artifact**: [69] Más que un servicio, es un portal de alcance global, ya que se encuentra en todas las regiones dentro de la consola de AWS, donde AWS almacena todos los certificados de cumplimiento de normativas de todos sus servicios. Es decir, si a petición de un auditor, interno o externo, se necesitan obtener los certificados de cumplimiento, por ejemplo, de PCI[8] de los servicios de AWS que se están utilizando, bastará con acudir a este portal, descargar las certificaciones y entregárselas al auditor.

  Entre las distintas normativas, se pueden encontrar informes de Certificaciones ISO, de la Industria de tarjetas de pago (PCI) y Control

[8] https://www.pcisecuritystandards.org/

de Organizaciones de Servicios (SOC), Reglamento General de Protección de datos (RGPD o en inglés, GDPR), NIST, etc.

Para la protección de los documentos, AWS se apoya en el modelo de responsabilidad de conformidad compartida para los documentos del cliente. Es decir, AWS es responsable de mantener los documentos protegidos mientras se encuentran en la nube de AWS, pero la responsabilidad recae en el cliente cuando este los descarga.

Además, AWS pone restricciones a compartir documentos marcados como confidenciales. En este sentido indica que, sólo se podrá compartir documentos marcados como confidenciales dentro de la empresa del cliente, con las autoridades reguladoras y con los auditores. El resto no está permitido.

2.5.4.6 Monitorización y trazabilidad

Aunque para AWS son servicios de administración y dirección según la clasificación de la imagen 14, los servicios de Amazon CloudWatch y AWS CloudTrail, son servicios que pueden ser muy relevantes en el ámbito de la seguridad de cualquier organización. De hecho, actualmente (marzo 2020), AWS le da un 20% de valor a las preguntas sobre *Logging and Monitoring* en la certificación AWS Certified Security Specialty[9]. Por lo tanto, a continuación, se introducen estos servicios como servicios de seguridad de AWS.

- **AWS CloudWatch**: [70][71][72] CloudWatch es el servicio de AWS que permite gestionar y monitorizar de manera personalizada multitud de datos de la nube, desde el nivel de usabilidad de las máquinas hasta el gasto repercutido por estas. Permite la creación de alertas cuando un valor supere, o no, cierto umbral.

  Permite la creación de un panel de monitorización personalizado en función de las necesidades del cliente, así como un lugar centralizado de almacenamiento de logs en el que el cliente puede recopilar los logs de las distintas instancias y observarlos en un único lugar.

  Esto resulta extremadamente útil no sólo por la facilidad de tener toda la información del estado de las instancias y aplicaciones centralizado en un único punto, sino porque evita el tener que dar acceso al personal de la organización a los distintos servidores, proporcionando así únicamente acceso a los distintos paneles de control definidos.

  Una métrica de CloudWatch es un conjunto datos recogidos a lo largo del tiempo. Un ejemplo es la utilización de la CPU de una instancia EC2.

  Las alarmas se pueden crear en base a las métricas, lanzando una acción si se supera el umbral determinado. Las alarmas tienen tres

[9] https://d1.awsstatic.com/training-and-certification/docs-security-spec/AWS-Certified-Security-Specialty_Exam-Guide_v1.6_FINAL.pdf

estados:

- Insuficiente: No hay suficientes datos para evaluar el estado.
- Alarma: Se ha superado el umbral de alarma definido. Por ejemplo, uso de CPU de más del 90% durante un periodo determinado.
- Ok: el umbral no se ha superado.

Las alarmas tienen varios componentes clave:

- Métrica: Las medidas de datos que se hacen a lo largo del tiempo.
- Umbral: Punto que dispara la alarma en función del periodo definido.
- Período: Durante cuánto tiempo el umbral debe ser superior/inferior antes de lanzar una alarma.
- Acción: qué hacer cuando se dispara una alarma. Por ejemplo, lanzar una notificación, autoescalar, etc.

CloudWatch Logs [73]

CloudWatch Logs proporciona la funcionalidad para almacenar, monitorizar y acceder a logs de EC2, servidores locales, Lambda, CloudTrail, Route 53, VPC Flow Logs, aplicaciones personalizadas, etc.

Para poder recopilar los logs de las instancias, se debe crear un rol (Role) al que se asociarán unas políticas (policies) con unos permisos asociados que autoricen la creación de grupos de logs (Log Groups), crear streams de logs, etc. Posteriormente, se debe asignar este rol a las instancias.

CloudWatch cataloga estos logs como Log Stream (flujo de logs). Los flujos de logs (Logs streams) son una secuencia de logs con la misma fuente origen.

Un grupo de logs (Log Group) es un contenedor para flujos de logs. Controlan la retención, la monitorización y el control de acceso. También se define como un conjunto de Log Streams. No existe un límite de Log Streams que componen un Log Group.

CloudWatch Logs permite la configuración del periodo de retención de los logs. Este periodo se asigna a los grupos de logs, pero se aplica a todos los streams (flujos) en un grupo (group). Este periodo varía desde un día hasta que nunca caduque.

Destacar que los logs pueden exportarse a AWS S3 para su explotación como lago de logs.

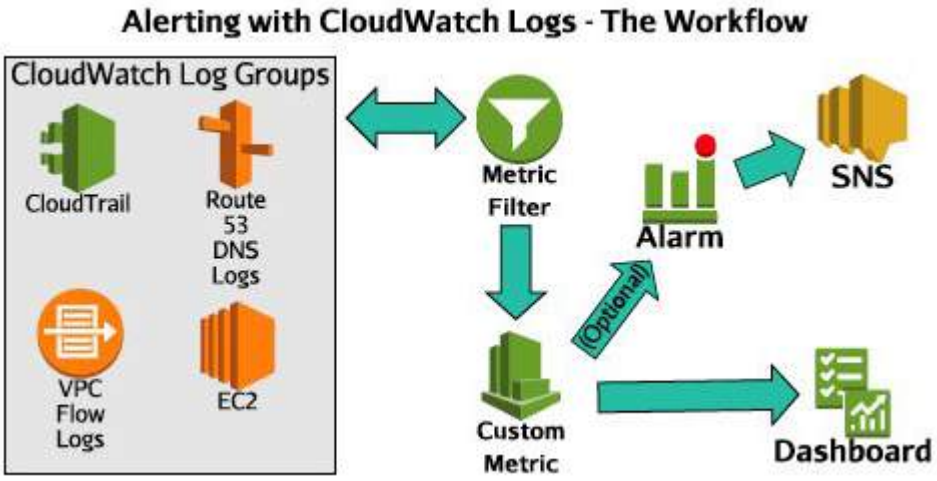

Imagen 37. Flujo CloudWatch Logs.

CloudWatch Events [74]

Los eventos de CloudWatch son similares a las alarmas. En lugar de configurar umbrales y alarmas en función de las métricas, los eventos de CloudWatch coinciden con los posibles eventos de los servicios. De igual manera, CloudWatch Events permite también la programación de eventos como, por ejemplo, el apagado de una instancia EC2 en una franja horaria definida.

Constan de tres partes:

- Fuente del evento (Event source): Un cambio en un servicio o un evento planificado.
- Reglas (Rules): Enrutado de los eventos en base a los objetivos.
- Objetivos: Los servicios que se verán impactados por el evento. Pueden ser más de uno. Por ejemplo, EC2, una función Lambda, SNS, etc.

CloudWatch Buses

Se trata de una funcionalidad que fue lanzada por AWS hace pocos años, en torno a 2017, y permite que diferentes cuentas de AWS de una organización (AWS Organizations) compartan eventos de CloudWatch.

Permite recopilar eventos de todas las cuentas de la organización en una sola cuenta. En la imagen 38 se puede observar el funcionamiento.

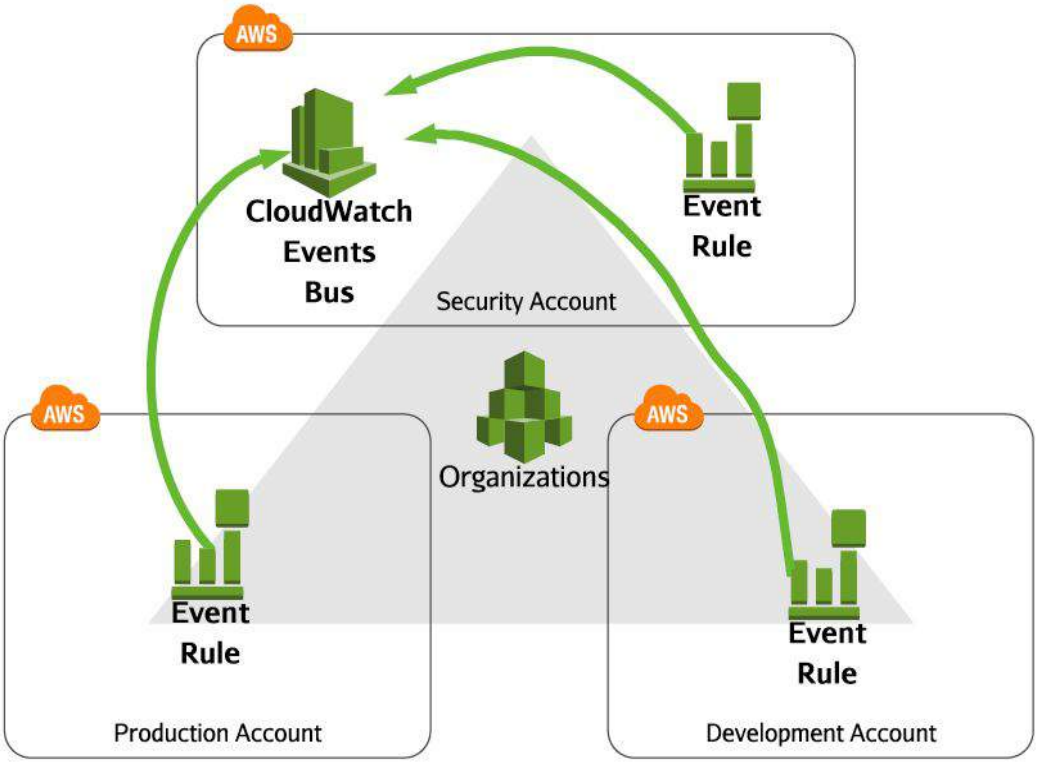

Imagen 38. Cloudwatch Bus.

- **AWS CloudTrail**: [75][76][77] CloudTrail es la herramienta por excelencia que AWS proporciona para la realización de auditorías. AWS CloudTrail monitoriza todas las llamadas a las API que se realicen en la cuenta AWS del usuario. Esto incluye las llamadas a S3, Lambda, API Gateway, etc. además de todos los cambios que se realicen como inicio o apagado de instancias, cambios en la VPC, etc.

  En resumen, se encarga de trazar todos los cambios que tengan lugar en la cuenta de AWS. Eso sí, no hay que confundir con aquello que ocurra dentro de instancias EC2. Para ello se cuenta con AWS CloudWatch. AWS CloudTrail es para todo lo que sucede sobre la propia cuenta de AWS.

  AWS CloudTrail almacena las trazas de login así como las llamadas a cualquier servicio de AWS que se intente consumir por cualquier usuario (o desde un servicio en nombre de un usuario) dentro de AWS. Pero CloudTrail no solo almacena las trazas/eventos de cuando un usuario se autentica correctamente, sino que también registra todos los intentos fallidos de autenticación.

  Todas estas trazas se almacenan cifradas de manera automática por un periodo de hasta 90 días. Si se quieren almacenar los logs durante más tiempo, se puede crear un *Trail* que se encarga de almacenar los logs en el bucket de S3 que se le indique.

Un ejemplo del funcionamiento de AWS CloudTrail se puede ver en la imagen 39.

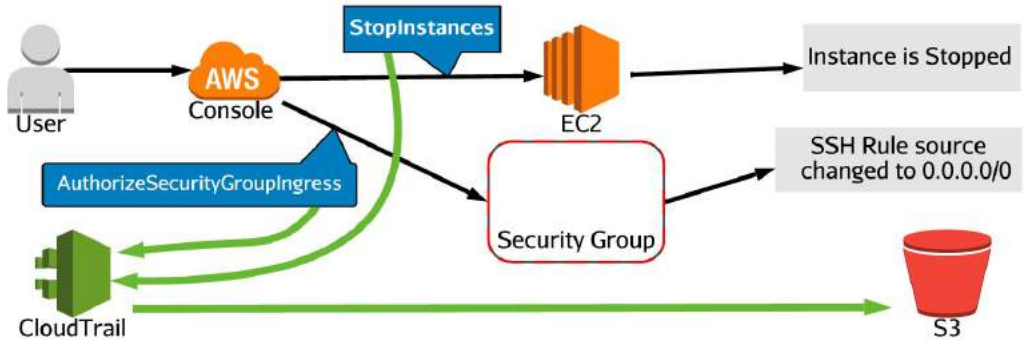

Imagen 39. AWS CloudTrail.

AWS hace algunas recomendaciones si se realiza el volcado de los logs en un bucket de S3 como, por ejemplo, configurar el ciclo de vida del bucket que almacene los logs, aplicar políticas de mínimo privilegio sobre los logs, obligar al uso de un segundo factor de autenticación (2FA) para el borrado de los logs y habilitar el versionado del bucket.

2.6 Relación de servicios de proveedores Cloud

En los apartados anteriores se ha presentado una introducción a los servicios de AWS que se han considerado más importantes en el ámbito de este trabajo, pero hay que destacar que los conceptos en los que se basa el servicio y su propio funcionamiento son extrapolables a cualquiera de los servicios equivalentes de otros proveedores cloud.

En este apartado, se va a identificar la relación entre algunos de los servicios más relevantes de AWS, Azure y Google Cloud por ser los tres principales proveedores de servicios cloud tal y como se mostró en la imagen 8, que hace referencia al estudio de Gartner respecto al uso de las cloud públicas durante el 2019.

Los conceptos son extrapolables porque aunque por debajo utilicen una tecnología u otra, la facturación sea en base a segundos, minutos o como considere cada proveedor, etcétera, la esencia de los servicios es equivalente en lo ofrecido al cliente.

A continuación, en la tabla 1, se muestra una comparativa basada en la realizada por CCSI [117] donde se puede ver la relación entre algunos servicios de Azure, AWS y Google:

Relación de servicios Azure, AWS y Google Cloud			
Servicio \ Proveedor	**Azure**	**AWS**	**Google Cloud**
Regiones disponibles	Azure Region	AWS Region and Zones	Regions & Zones
Computación	Virtual Machines	EC2	Compute Engine
Hosting aplicaciones	Azure Cloud Services	Amazon Elastic Beanstalk	Google App Engine
Computación sin servidor	Azure Functions	AWS Lambda	Google Cloud Functions
Contenedores	Azure Container Service	EC2 Container Service	Container Engine
Opciones escalado	Azure Autoscale	Auto Scaling	Autoscaler
Almacenamiento de objetos	Azure Blob Storage	Amazon S3	Cloud Storage
Almacenamiento de bloques	Azure Managed Storaged	Amazon EBS	Persistent Disk
Content Delivery Network	Azure CDN	Amazon CloudFront	Cloud CDN
Bases de datos SQL	Azure SQL Database	Amazon RDS	Cloud SQL
Bases de datos NoSQL	Azure DocumentDB	AWS DynamoDB	Cloud Datastore

Redes virtuales	Azure Virtual Network	Amazon VPC	Cloud Virtual Network
Conectividad privada	Azure Express Route	AWS Direct Connect	Cloud Interconnect
Servicios DNS	Azure Traffic Manager	Amazon Route 53	Cloud DNS
Monitorización Auditoría	Azure Operational Insights	Amazon CloudTrail	Cloud Logging
Monitorización rendimiento	Azure Application Insights	Amazon CloudWatch	Stackdriver Monitoring
Analítica	Azure Stream Analytics	Amazon Kinesis	Cloud Dataflow
Automatización	Azure Automation	AWS Opsworks	Compute Engine Management
Servicio de gestión	Azure Resource Manager	Amazon CloudFormation	Cloud Deployment Manager
Notificaciones	Azure Notification Hub	Amazon SNS	-
Balanceo de carga	Load Balancing for Azure	ELB	Cloud Load Balancing

Tabla 1. Relación servicios AWS - Azure - Google.

Respecto a algunos de los servicios de seguridad vistos en este trabajo, se presenta la tabla 2 [118][119]:

Relación de servicios Azure, AWS y Google Cloud			
Servicio \ Proveedor	**Azure**	**AWS**	**Google Cloud**
Autenticación y autorización	Active Directory	IAM	Cloud IAM
Cifrado	Key Vault	AWS KMS Cloud HSM	Cloud KMS
Firewall	Application Gateway	AWS WAF	-
Evaluación de riesgos	Security Center	AWS Inspector	-
Gestión de certificados	App Services Directory	Certificate Manger	-
Servicios de directorio	Active Directory Domain Services	AWS Directory Service	-
Administración de	Azure Active	AWS Cognito	Identity

identidades	Directory B2C		Platform
Autenticación multifactor	MFA	MFA	MFA
Detección de amenazas y actividades anómalas	Azure Advanced Threat Protection	GuardDuty AWS Macie	Cloud Security Command Center
Cumplimiento	Service Portal Trust	AWS Artifact	-
API	Azure API Apps	AWS API Gateway	Apigee
Protección DDoS	DDoS Protection Service	AWS Shield	Cloud Armor
VPN	VPN Gateway	AWS Manager VPN	Cloud VPN
Asesoramiento - optimización	Azure Advisor	AWS Trusted Advisor	Cloud Platform Security

Tabla 2. Relación servicios ámbito seguridad en AWS - Azure - Google.

En general, AWS y Microsoft Azure, actualmente están un escalón por encima de Google Cloud tal como se muestra en la imagen 8 y se refuerza con la disponibilidad de los diferentes servicios mostrados en las tablas 1 y 2. No obstante, los servicios *core* como son los de computación, almacenamiento, comunicaciones, redes, cifrado, etc. los ofrecen cualquiera de los tres proveedores con absolutas garantías de rendimiento y calidad.

3. Reguladores, normativas, directivas y otros estándares que afectan a la industria financiera tradicional en entornos cloud

3.1 Banco de España (BdE) / Autoridad Bancaria Europea (ABE)

El Banco de España (BdE) es el banco central nacional y, en el marco del Mecanismo Único de Supervisión (MUS), el supervisor del sistema bancario español junto al Banco Central Europeo. Su actividad está regulada por la Ley de Autonomía del Banco de España. [78]

La Autoridad Bancaria Europea (ABE; EBA, por sus siglas en inglés, European Banking Authority) es una autoridad europea independiente fundada el 1 de enero de 2011, como parte del Sistema Europeo de Supervisión Financiera. [79]

El objetivo principal del sistema es asegurar que las reglas de aplicación al sector financiero se implementan adecuadamente, con el fin de preservar la estabilidad financiera. El sistema tiene como meta fomentar la confianza en el sistema financiero, y garantizar una protección adecuada a los consumidores de servicios financieros.

Cuando procede, se llevan a cabo consultas públicas abiertas en relación con los productos normativos (normas técnicas, directrices, etc.) a fin de asegurar que todas las partes interesadas puedan contribuir a las futuras normas y directrices sobre el sector bancario.

El Banco de España es el representante español en la Autoridad Bancaria Europea.

El Banco de España, de acuerdo con lo previsto en el artículo 54 de la Ley 10/2014 [80], de 26 de junio, de ordenación, supervisión y solvencia de las entidades de crédito, podrá elaborar y publicar guías técnicas, dirigidas a las entidades y grupos supervisados, indicando los criterios, prácticas, metodologías o procedimientos, que considera adecuados para el cumplimiento de la normativa de supervisión. Dichas guías podrán incluir los criterios que el propio Banco de España seguirá en el ejercicio de sus actividades de supervisión. Adicionalmente, el Banco de España podrá hacer suyas, y transmitir como tales a las entidades y grupos, las guías que, sobre dichas cuestiones, aprueben los organismos o comités internacionales activos en la regulación y supervisión bancarias.

Por lo tanto, el Banco de España emite sus propias guías, pero también adopta como propias las Directrices y Recomendaciones emitidas por la ABE, con el alcance y matizaciones que se especifican en cada una de ellas. Estas Directrices y Recomendaciones tienen la misma eficacia que las elaboradas por el Banco de España.

Dos de estas Directrices emitidas por la ABE y que ha adoptado como propias el BdE son las siguientes:

1. EBA/GL/2017/05 - Directrices sobre la evaluación del riesgo de TIC en el marco del proceso de revisión y evaluación supervisora (PRES) [81]

2. EBA/GL/2019/02 - Directrices sobre externalización [82]

Aunque este apartado del trabajo se va a centrar en la EBA/GL/2019/02 es conveniente introducir algunos detalles de la EBA/GL/2017/05, ya que tiene como objetivo no olvidar los riesgos derivados de la externalización de las TIC.

- **EBA/GL/2017/05**

Las Directrices recogidas en la EBA/GL/2017/05 especifican los criterios que las autoridades competentes deberían aplicar en la evaluación supervisora del gobierno y la estrategia en materia de TIC de las entidades y en la evaluación supervisora de las exposiciones al riesgo de TIC y los controles correspondientes de las entidades.

Según la EBA/GL/2017/05 se entiende por sistemas de TIC la configuración de los elementos de las TIC como parte de un mecanismo o una red de interconexión que sirve de soporte para las operaciones de una entidad. Y por servicios de TIC, los servicios prestados por sistemas de TIC a uno o más usuarios internos o externos. Por ejemplo, los servicios de entrada, almacenamiento y tratamiento de datos.

Se definen cinco grupos de riesgos a tener en cuenta:

1. Riesgo de disponibilidad y continuidad de las TIC: Riesgo de que el rendimiento y la disponibilidad de los sistemas de TIC y los datos se vean afectados negativamente, incluida la incapacidad para recuperar oportunamente los servicios de la entidad, debido a un fallo de los componentes de hardware o software de las TIC.

2. Riesgo de seguridad de las TIC: Riesgo de acceso no autorizado a los sistemas de TIC y a los datos dentro y fuera de la entidad.

3. Riesgo de cambio de las TIC: Riesgo derivado de la incapacidad de la entidad para gestionar de forma oportuna y controlada los cambios en los sistemas de TIC.

4. Riesgo de integridad de datos TIC: Riesgo de que los datos almacenados y procesados por los sistemas de TIC sean incompletos, inexactos o incoherentes en los diferentes sistemas de TIC.

5. Riesgo de externalización de las TIC: Riesgo de que la contratación de sistemas de TIC o servicios relacionados a un tercero u otra entidad del grupo (subcontratación intragrupo) tenga un efecto negativo en el desempeño de la entidad y la gestión de riesgos.

No hay que olvidar que el proveedor de servicios cloud, ya sea AWS, Azure o cualquier otro deben reducir al mínimo los riesgos de los cinco grupos definidos, pero a la entidad financiera que contrata los servicios de algún proveedor cloud le conviene poner el foco de manera interna en realizar un

análisis exhaustivo sobre los riesgos que conlleva el punto cinco. Se deben tener en cuenta las indicaciones de la ABE en el apartado 3.3.4.e Controles para la gestión de los riesgos materiales de externalización de las TIC, ya que tendrán que evidenciar su cumplimiento frente al regulador.

- Las autoridades competentes evaluarán si la estrategia de externalización de la entidad, se aplica adecuadamente a la externalización de las TIC, incluida la externalización intragrupo que presta servicios de TIC dentro del grupo.

- En particular, las autoridades competentes evaluarán si la entidad cuenta con un marco eficaz para identificar, entender y medir el riesgo de externalización de las TIC y, en particular, si dispone de controles y un entorno de control para mitigar los riesgos relacionados con los servicios de TIC externalizados que sean proporcionales al tamaño, las actividades y el perfil de riesgo de TIC de la entidad y que incluyan:

    - Una evaluación del impacto de la externalización de las TIC sobre la gestión de riesgos de la entidad en relación con el uso de proveedores de servicios (por ejemplo, proveedores de servicios en la nube) y sus servicios durante el proceso de adquisición, que se documenta y es tenido en cuenta por la alta dirección o el órgano de dirección a la hora de tomar una decisión sobre si externalizar los servicios o no. La entidad revisará las políticas de gestión de riesgos de TIC y el entorno de control y los controles de TIC del proveedor de servicios para asegurarse de que cumplen con los objetivos internos de gestión de riesgos de la entidad. Esta revisión se actualizará periódicamente durante el periodo contractual de la externalización, teniendo en cuenta las características de los servicios subcontratados.

    - Un seguimiento de los riesgos de TIC de los servicios externalizados durante el periodo contractual de la externalización como parte de la gestión de riesgos de la entidad, que sirva de base para la presentación de informes de gestión de riesgos de TIC de la entidad (por ejemplo, informes de continuidad del negocio, informes de seguridad, etc.).

    - Un seguimiento y comparación de los niveles de servicio recibidos con los niveles de servicio contractualmente acordados que deben formar parte del contrato de externalización o del acuerdo de nivel de servicio (SLA).

- **EBA/GL/2019/02**

Las Directrices recogidas en la EBA/GL/2019/02 especifican los sistemas de gobierno interno, incluida la adecuada gestión de los riesgos, que las entidades de crédito, las entidades de pago y las entidades de dinero electrónico deben aplicar cuando externalicen funciones, en particular, en relación con la externalización de las denominadas funciones esenciales o importantes.

Las directrices se distribuyen en cinco títulos, relativos al principio de proporcionalidad y la aplicación de las Directrices respecto de grupos y entidades que forman parte de un sistema institucional de protección, la evaluación de los acuerdos de externalización, el marco de gobernanza, el proceso de externalización y las directrices destinadas a las autoridades competentes.

Con la excepción del apartado 63, letra b), estas directrices serán de aplicación a partir del 30 de septiembre de 2019 a todos los acuerdos de externalización celebrados, revisados o modificados en esa fecha o con posterioridad. El apartado 63, letra b), es aplicable a partir del 31 de diciembre de 2021.

Las entidades y las entidades de pago deberían revisar y modificar en consecuencia los acuerdos de externalización existentes, con el fin de asegurarse de que estos cumplan con lo dispuesto en las presentes directrices.

A efecto de las directrices se aplican las siguientes definiciones:

Externalización: Acuerdo de cualquier forma entre una entidad, una entidad de pago o una entidad de dinero electrónico y un proveedor de servicios por el que dicho proveedor realiza un proceso, un servicio o una actividad que, de otro modo, serían realizados por la propia entidad, entidad de pago o entidad de dinero electrónico.

Proveedor de servicios: Tercera parte que realiza un proceso, servicio o actividad que se ha externalizado, o partes de los mismos, con arreglo a un acuerdo de externalización.

Servicios en la nube: Servicios prestados usando computación en la nube, es decir, un modelo que permite el acceso de red ubicuo, conveniente y bajo demanda, a un conjunto compartido de recursos informáticos configurables (por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios) que se pueden suministrar y desplegar rápidamente, requiriendo un esfuerzo de gestión o una interacción con el proveedor del servicio mínimos.

Nube pública: Infraestructura de nube disponible para el uso abierto del público en general.

Nube privada: Infraestructura de nube disponible para el uso exclusivo de una sola entidad o entidad de pago.

Nube comunitaria: Infraestructura de nube disponible para el uso exclusivo de una comunidad específica de entidades o de entidades de pago, incluido el caso de varias entidades de un mismo grupo.

Nube híbrida: Infraestructura de nube compuesta por dos o más infraestructuras de nube distintas.

A continuación se van a detallar las directrices más importantes de cada uno de los cincos títulos.

Título I – Proporcionalidad: aplicación a nivel de grupos y de sistemas institucionales de protección

- Proporcionalidad
    - Las entidades, las entidades de pago y las autoridades competentes, a la hora de cumplir o supervisar el cumplimiento de las presentes Directrices, deberían tener en cuenta el principio de proporcionalidad. El principio de proporcionalidad tiene por objeto garantizar que los sistemas de gobierno, en particular los relacionados con la externalización, sean coherentes con el perfil de riesgo individual, la naturaleza y el modelo de negocio de la entidad o la entidad de pago, y con la escala y complejidad de sus actividades, de manera que se alcancen eficazmente los objetivos de los requisitos regulatorios.
    - Las entidades de pago deberían remitirse también a las Directrices de la ABE emitidas con arreglo a la Directiva PSD2 sobre la información que debe facilitarse para la autorización de entidades de pago y de entidades de dinero electrónico y para el registro de proveedores de servicios de información sobre cuentas.
- Externalización por parte de grupos y entidades que forman parte de un sistema institucional de protección
    - Las entidades y las entidades de pago deberían asegurarse de que su órgano de administración sea debidamente informado de los cambios significativos previstos en relación con los proveedores de servicios controlados de forma centralizada y del impacto potencial de estos cambios sobre las funciones esenciales o importantes que se realicen, incluyendo un resumen del análisis de riesgos, que incluya los riesgos legales, el cumplimiento de los requisitos regulatorios y el impacto sobre niveles de servicio, a fin de que puedan valorar el impacto de estos cambios.

Título II – Evaluación de los acuerdos de externalización

- Externalización
    - Cuando el acuerdo con un proveedor de servicios abarque múltiples funciones, las entidades y las entidades de pago deberían considerar en su evaluación todos los aspectos del acuerdo; por ejemplo, si el servicio prestado incluye el suministro de hardware para el almacenamiento de datos y la copia de seguridad de los datos, ambos aspectos deberían analizarse conjuntamente.
    - No se debe considerar como externalización una función que legalmente debe realizarse por un proveedor de servicios, por

ejemplo, una auditoría legal; las infraestructuras de red globales de Visa y/o de Mastercard; los servicios de corresponsalía bancaria, etc.

- Funciones esenciales o importantes
    - Las entidades y las entidades de pago deberían considerar siempre que una función es esencial o importante en las siguientes situaciones:
        - Si una anomalía o fallo en su ejecución afectase considerablemente al cumplimiento continuado de sus condiciones de autorización o a sus otras obligaciones, a sus resultados financieros; o a la solidez o la continuidad de sus actividades bancarias y servicios de pago.
        - Cuando se externalicen tareas operativas de las funciones de control interno.
        - Cuando pretendan externalizar funciones relativas a actividades bancarias o servicios de pago en la medida que requeriría la autorización de una autoridad competente.
    - Al evaluar si un acuerdo de externalización afecta a una función esencial o importante, las entidades y las entidades de pago deberán tener en cuenta entre otras cosas las siguientes:
        - Si el acuerdo de externalización está directamente relacionado con la prestación de actividades bancarias o servicios de pago para los que están autorizadas.
        - El impacto potencial de cualquier interrupción de la función externalizada o la incapacidad del prestador de servicios para prestar el servicio con los niveles de servicio acordados y de forma continuada.
        - El impacto potencial sobre los servicios prestados a sus clientes.
        - La capacidad para transferir el acuerdo de externalización propuesto a otro proveedor de servicios, si fuera necesario o deseable, tanto desde el punto de vista contractual como en la práctica, incluidos los riesgos estimados, los impedimentos que afectan a la continuidad de las actividades, los costes y el plazo para dicha transferencia.

Título III – Marco de gobernanza

- Sistemas de gobierno adecuados y externalización

- La externalización de funciones no puede dar lugar a la delegación de las responsabilidades del órgano de administración. Las entidades y las entidades de pago son plenamente responsables y responden del cumplimiento de todas sus obligaciones regulatorias, incluida la capacidad para supervisar la externalización de funciones esenciales o importantes.

- Las entidades y las entidades de pago deben asignar claramente las responsabilidades relativas a la documentación, gestión y control de los acuerdos de externalización. Además, deberán destinar recursos suficientes para garantizar el cumplimiento de todos los requisitos legales y regulatorios, incluidas las presentes Directrices, y la documentación y seguimiento de todos los acuerdos de externalización.

- Planes de continuidad de negocio

  - Los planes de continuidad de negocio deberían tener en cuenta el posible escenario en el que la calidad del servicio relativo a la función esencial o importante externalizada se deteriore hasta llegar a niveles inaceptables o falle. Estos planes también deberían tener en cuenta el posible impacto de la insolvencia u otros incumplimientos por parte de los proveedores de servicios y, en su caso, los riesgos políticos en la jurisdicción del proveedor de servicios.

- Requisitos de documentación

  - Las entidades y las entidades de pago deberían poner a disposición de la autoridad competente, previa solicitud, el registro completo de todos los acuerdos de externalización existentes.

  - Las entidades y las entidades de pago deberían poner a disposición de la autoridad competente, previa solicitud, toda la información necesaria para que la autoridad competente pueda llevar a cabo la supervisión efectiva de la entidad o la entidad de pago, incluida, cuando se requiera, una copia del acuerdo de externalización.

Título IV – Proceso de externalización

- Análisis previo a la externalización

  - Las entidades y las entidades de pago deberían asegurarse de que las funciones relativas a las actividades bancarias o los servicios de pago, en la medida en que su realización requiera autorización o registro por parte de una autoridad competente en el Estado miembro en el que están autorizadas se externalicen a un proveedor de servicios ubicado en el mismo o en otro Estado

miembro exclusivamente si se cumple que el proveedor de servicios está autorizado o habilitado para llevar a cabo actividades bancarias o servicios de pago.

- Las entidades y las entidades de pago deberían evaluar el impacto potencial de los acuerdos de externalización en relación con su riesgo operacional, deberían tener en cuenta los resultados de la evaluación en el momento de decidir si la función se debe externalizar a un proveedor de servicios, y deberían tomar las medidas oportunas para evitar riesgos operacionales adicionales indebidos antes de suscribir dichos acuerdos de externalización. En el marco del análisis de escenarios, las entidades y las entidades de pago evaluarán el impacto potencial de que los servicios no sean adecuados o fallen, incluidos los riesgos causados por procesos, sistemas, personas o eventos externos.

- Cuando el acuerdo de externalización contemple la posibilidad de que el proveedor de servicios subcontrate funciones esenciales o importantes a otros proveedores de servicios, las entidades y las entidades de pago deberían tener en cuenta los riesgos asociados a la subcontratación.

- Cuando realicen la evaluación de riesgos previa a la externalización y durante el seguimiento continuado del desempeño del proveedor de servicios, las entidades y las entidades de pago deberían, como mínimo:

    - Identificar y clasificar las funciones pertinentes y los datos y sistemas relacionados en función de su sensibilidad y de las medidas de seguridad necesarias.

    - Llevar a cabo un análisis exhaustivo basado en el riesgo de las funciones y los datos y sistemas asociados cuya externalización se está considerando o que ya se han externalizado y abordar los riesgos potenciales, en particular los riesgos operacionales, incluidos los riesgos legales, de TIC, de cumplimiento y de reputación, y las limitaciones de la supervisión en los países en que se presten o puedan prestarse los servicios externalizados y en que se almacenen o probablemente se almacenen los datos.

    - Considerar las consecuencias del lugar en que se ubica el proveedor de servicios (dentro o fuera de la UE).

    - Definir y decidir el nivel apropiado de protección de la confidencialidad de la información, la continuidad de las actividades externalizadas, así como la integridad y trazabilidad de los datos y sistemas en el contexto de la

externalización de servicios prevista. Además, las entidades y las entidades de pago deberían considerar la adopción de medidas específicas cuando sean necesarias para proteger los datos en tránsito, los datos en memoria y los datos en reposo, como el uso de tecnologías de cifrado combinadas con una arquitectura de gestión de claves adecuada.

- Cuando la externalización conlleve el tratamiento de datos personales o confidenciales, las entidades y las entidades de pago deberían estar satisfechas de que el proveedor de servicios aplica medidas técnicas y organizativas adecuadas para proteger los datos.

- Los derechos y las obligaciones de la entidad, la entidad de pago y el proveedor de servicios deberían estar claramente asignados y establecidos en un acuerdo escrito.

- El acuerdo de externalización debería especificar si se permite la subcontratación de funciones esenciales o importantes, o partes significativas de ellas. Si se permite la subcontratación de funciones esenciales o importantes, el acuerdo escrito debería especificar cualquier tipo de actividad que esté excluido de la subcontratación, especificar las condiciones que han de cumplirse en caso de subcontratación, etc.

- Seguridad de los datos y sistemas

  - Las entidades y las entidades de pago deberían asegurarse de que los proveedores de servicios, en su caso, cumplen los estándares de seguridad informática oportunos.

  - Cuando proceda, por ejemplo en el contexto de servicios en la nube u otras externalizaciones TIC), las entidades y las entidades de pago deberían definir los requisitos de seguridad de los datos y sistemas dentro del acuerdo de externalización y realizar un seguimiento continuado del cumplimiento de estos requisitos.

  - En el caso de externalización a proveedores de servicios en la nube y otros acuerdos de externalización que impliquen el tratamiento o la transferencia de datos personales o confidenciales, las entidades y las entidades de pago deberían adoptar un enfoque basado en el riesgo en relación con las localizaciones del almacenamiento y el procesamiento de los datos (es decir, país o región) y con las cuestiones relativas a la seguridad de la información.

  - Las entidades y las entidades de pago deberían asegurarse de que el acuerdo de externalización incluya la obligación de que el proveedor de servicios proteja la información confidencial, personal o cualquier otro tipo de información delicada y cumpla

todos los requisitos legales en relación con la protección de datos aplicables a la entidad o la entidad de pago. Por ejemplo, que se cumplen las normas sobre la protección de los datos personales y el secreto bancario u obligaciones de confidencialidad similares que establezca la ley con respecto a la información de los clientes.

- Derechos de acceso, información y auditoría
    - Las entidades y las entidades de pago deberían asegurarse en el acuerdo escrito de externalización de que la función de auditoría interna sea capaz de revisar la función externalizada utilizando un enfoque basado en el riesgo.
    - En relación con la externalización de funciones esenciales o importantes, las entidades y las entidades de pago deberían asegurarse, en el acuerdo de externalización escrito, de que el proveedor de servicios les conceda a ellas y a sus autoridades competentes pleno acceso a todas las instalaciones pertinentes y derechos sin restricciones de inspección y auditoría en relación con el acuerdo de externalización (derechos de auditoría), para que puedan realizar un seguimiento del acuerdo de externalización y garantizar el cumplimiento de todos los requisitos regulatorios y contractuales aplicables.
    - Las entidades y las entidades de pago deberían ejercer sus derechos de acceso y de auditoría, determinar la frecuencia de las auditorías y las áreas que se van a auditar mediante un enfoque basado en el riesgo y ajustarse a las normas de auditoría nacionales e internacionales comúnmente aceptadas.
    - Las entidades y las entidades de pago podrán utilizar auditorías compartidas organizadas conjuntamente con otros clientes del mismo proveedor de servicios, y realizadas por ellas y dichos clientes o por un tercero designado por ellos, con el fin de utilizar los recursos de auditoría de una manera más eficaz y de reducir la carga organizativa que suponen para los clientes y para el proveedor de servicios. También podrán utilizar certificaciones externas e informes de auditoría internos o externos facilitados por el proveedor de servicios.
    - En línea con las Directrices de la ABE sobre la evaluación del riesgo de TIC en el marco del proceso de revisión y evaluación supervisora (PRES), las entidades deberían asegurarse, cuando proceda, de que pueden realizar pruebas de penetración de seguridad para evaluar la eficacia de las medidas y procesos de ciberseguridad y de seguridad tecnológica interna implementada.
    - Cuando el acuerdo de externalización conlleve un nivel elevado de complejidad técnica, por ejemplo, en el caso de externalización

de servicios en la nube, la entidad o la entidad de pago debería verificar que quien realiza la auditoría cuenta con capacidades y conocimientos apropiados y pertinentes para llevar eficazmente a cabo las auditorías o evaluaciones pertinentes.

- Derechos de resolución
    - El acuerdo de externalización debería contemplar expresamente la posibilidad de que la entidad o la entidad de pago resuelva el acuerdo, de conformidad con la legislación aplicable.
    - El acuerdo de externalización debería facilitar la transferencia de la función externalizada a otro proveedor de servicios o su reincorporación a la entidad o la entidad de pago.
- Supervisión de las funciones externalizadas
    - Las entidades y entidades de pago deberían realizar un seguimiento continuado del desempeño de los proveedores de servicios en lo que respecta a todos los acuerdos de externalización aplicando un enfoque basado en el riesgo y centrándose principalmente en la externalización de funciones esenciales o importantes, vigilando, en particular, que se garantiza la disponibilidad, integridad y seguridad de los datos y la información.
- Estrategia de salida
    - Las entidades y las entidades de pago deberían contar con una estrategia de salida documentada cuando externalicen funciones esenciales o importantes que esté en línea con su política de externalización y con los planes de continuidad de negocio.

Título IV – Directrices sobre externalización destinadas a autoridades competentes

Sobre este punto no se va a incluir ninguna directriz, ya que están destinadas a las autoridades competentes y no están enfocadas a las entidades de pago.

3.2 Payment Card Industry (PCI)

El PCI Security Standards Council (PCI SSC) es un foro global que reúne a las partes interesadas de la industria de pagos para desarrollar e impulsar la adopción de estándares y recursos de seguridad de datos para pagos seguros en todo el mundo. [83]

La misión de PCI SSC es mejorar la seguridad de los datos de los pagos mediante el desarrollo de estándares y servicios de apoyo que impulsen la educación, la concienciación y la implementación efectiva por parte de las partes interesadas.

El Consejo fue fundado en 2006 por American Express, Discover, JCB International, MasterCard y Visa Inc. Los miembros fundadores comparten por igual el gobierno y la ejecución del trabajo de la organización. Cada uno de ellos incorpora el Estándar de Seguridad de Datos PCI (en inglés, Data Security Standard PCI, PCI DSS) como parte de los requisitos técnicos para sus respectivos programas de cumplimiento de seguridad de datos. Los fundadores también reconocen a los Evaluadores de Seguridad Cualificados (QSA) y a los Proveedores de Escaneo Aprobados (ASV) calificados por el PCI SSC.

3.2.1 PCI - DSS

Introducción a PCI-DSS

El PCI-DSS [84] es un estándar promovido por un comité formado por las compañías de tarjetas de crédito más importantes con el objetivo de definir una guía de buenas prácticas sobre la protección de los datos personales y de autenticación de los usuarios de las tarjetas de pago (crédito y débito). Se aplica a todos los participantes en un pago, es decir, se aplica a los comerciantes, a los bancos que aceptan el pago, a los emisores de tarjetas, a las pasarelas de pago y a los proveedores de servicios relacionados.

Por lo tanto, la PCI DSS aplica a todas las entidades que almacenan, procesan o transmiten datos del titular de la tarjeta y/o datos confidenciales de autenticación.

Los datos del titular de la tarjeta y los datos de autenticación confidenciales se definen tal y como se muestra en la imagen 40:

Datos de cuentas	
Los datos de titulares de tarjetas incluyen:	**Los datos confidenciales de autenticación incluyen:**
▪ Número de cuenta principal (PAN) ▪ Nombre del titular de la tarjeta ▪ Fecha de vencimiento ▪ Código de servicio	▪ Contenido completo de la pista (datos de la banda magnética o datos equivalentes que están en un chip) ▪ CAV2/CVC2/CVV2/CID ▪ PIN/Bloqueos de PIN

Imagen 40.Clasificación datos PCI DSS.

La tabla de la imagen 41 ilustra los elementos de los datos de titulares de tarjetas y los datos de autenticación confidenciales que habitualmente se

utilizan y una primera aproximación a cómo debe ser el tratamiento de los mismos:

		Elemento de datos	Almacenamiento permitido	Datos almacenados ilegibles según el Requisito 3.4
Datos de cuentas	Datos del titular de la tarjeta	Número de cuenta principal (PAN)	Sí	Sí
		Nombre del titular de la tarjeta	Sí	No
		Código de servicio	Sí	No
		Fecha de vencimiento	Sí	No
	Datos confidenciales de autenticación[2]	Contenido completo de la pista[3]	No	No se pueden almacenar según el Requisito 3.2
		CAV2/CVC2/CVV2/CID[4]	No	No se pueden almacenar según el Requisito 3.2
		PIN/Bloqueo de PIN[5]	No	No se pueden almacenar según el Requisito 3.2

Imagen 41.Tratamiento datos sujetos a PCI DSS.

El cumplimiento de las medidas establecidas por PCI-DSS es de obligatorio cumplimiento para poder trabajar con las entidades de pago adheridas, si bien cada jurisdicción y legislación particular (regional, estatal, etc.) puede exigir la aplicación de diferentes medidas más restrictivas aunque pueden cubrir total o parcialmente las medidas propuestas por este estándar.

Los requisitos de seguridad de PCI DSS aplican a todos los componentes del sistema incluidos en el entorno de datos del titular de la tarjeta o conectados a este. El entorno de datos del titular de la tarjeta consta de personas, procesos y tecnologías que almacenan, procesan o transmiten datos de titulares de tarjetas o datos confidenciales de autenticación. El término componentes del sistema incluye dispositivos de red, servidores, dispositivos informáticos y aplicaciones.

Proceso de evaluación de PCI-DSS

El proceso de evaluación de PCI DSS se compone de los siguientes pasos:

1. Confirmar el alcance de la evaluación de PCI DSS.
2. Llevar a cabo la evaluación de las PCI DSS del entorno según los procedimientos de pruebas de cada requisito.
3. Completar el informe correspondiente de la evaluación (es decir, el SAQ, cuestionario de autoevaluación] o el ROC, informe sobre cumplimiento), que incluye la documentación de todos los controles de compensación, de acuerdo con la guía y las instrucciones de la PCI correspondientes.
4. Completar la declaración de cumplimiento para proveedores de servicios o comerciantes, según corresponda, en su totalidad.
5. Presentar el SAQ o el ROC y la atestación de cumplimiento junto con cualquier otro documento solicitado, como los informes de análisis de ASV (proveedores aprobados de escaneo) al adquirente (en el caso de

comerciantes), a la marca de pago o a otro solicitante (en el caso de proveedores de servicios).

6. Si es necesario, realizar la remediación para abordar los requisitos que no están implementados, y presentar un informe actualizado.

SAQ - Cuestionario de autoevaluación

El cuestionario de autoevaluación o SAQ [85] es un conjunto de controles PCI-DSS que están destinados a que sean evaluados por las entidades que quieran cumplir con el estándar, pero que no están obligados a presentar el informe ROC, mucho más difícil de cumplimentar. Esta autoevaluación tiene que demostrar claramente el cumplimiento de los requisitos PCI-DSS comentados anteriormente.

Los tipos de SAQ existentes son los siguientes:

- **A**: Aplicable a comercios que han subcontratado completamente todas las funcionalidades con datos del titular de la tarjeta a proveedores de servicios de terceros compatibles con PCI DSS, sin almacenamiento, procesamiento o transmisión electrónica de cualquier información del titular de la tarjeta. No aplicable a canales físicos.

- **A-EP**: Aplica a aquellos comercios que han delegado de forma parcial su canal de pago vía comercio electrónico a un tercero certificado en PCI DSS y que no almacena de forma electrónica, procesa o transmite ningún dato de tarjeta de pago en sus sistemas o instalaciones. Aplicable solo a canales de e-commerce.

- **B**: Aplicables a comercios que procesan datos tarjetas de pago únicamente por medio de máquinas impresoras o terminales independientes con disco externo. Pueden ser comercios que procesen transacciones presenciales o pagos por teléfono o correo (tarjeta no presente) y que no almacenan datos de tarjetas de pago en ningún sistema informático. No aplicable a canales de comercio electrónico.

- **B-IP**: Aplicable a comercios que procesan datos tarjetas de pago únicamente por medio de dispositivos de punto de interacción (point-of-interaction, POI) aprobados por PCI PTS y con una conexión IP a un procesador de pagos. Pueden ser comercios que procesen transacciones presenciales o pagos por teléfono o correo (tarjeta no presente) y que no almacenan datos de tarjetas de pago en ningún sistema informático. No aplicable a canales de comercio electrónico.

- **C**: Aplicable a comercios cuya aplicación de pago (por ejemplo, un sistema de punto de venta) está conectada a Internet. Los comercios que reporten el cumplimiento usando el SAQ C certifican que procesan datos de tarjeta de pago empleando una terminal de punto de venta (TPV/POS) u otros sistemas de aplicación para pagos conectados a Internet. Pueden ser comercios que procesen transacciones presenciales o pagos por teléfono o correo (tarjeta no presente) y que no

almacenan datos de tarjetas de pago en ningún sistema informático. No es aplicable a canales de comercio electrónico.

- **C-VT**: Aplicable a comercios que procesan datos de tarjetas de pago únicamente a través de una terminal de pago virtual aislado en un ordenador personal conectado a Internet. Aquellos comercios que reporten su cumplimiento a través de este SAQ deben ingresar manualmente una transacción a la vez empleando un teclado y una terminal virtual de pago conectada a Internet. Pueden ser comercios que procesen transacciones presenciales o pagos por teléfono o correo (tarjeta no presente) y que no almacenan datos de tarjetas de pago en ningún sistema informático. No es aplicable a canales de comercio electrónico.

- **P2PE**: Aplicable a todos aquellos comercios que están empleando terminales de pago de hardware incluidos y gestionados por un proveedor certificado P2PE, sin almacenamiento electrónico de datos de tarjetas de pago.

- **D**:

    - Comerciantes: Aplicable a todos aquellos comercios elegibles que no concuerdan con ninguno de los criterios descritos en los anteriores tipos de SAQ.

    - Proveedor de servicios: Aplicable a todos aquellos proveedores de servicio definidos por las marcas de pago como elegibles para reportar su cumplimiento empleando un SAQ.

Requisitos de PCI-DSS

El estándar básicamente define un listado de 12 requisitos principales, organizados en 6 secciones, que definen a alto nivel las medidas de seguridad a tomar por cualquier entidad relacionada con pagos mediante tarjetas de pago:

- Desarrollar y mantener las redes y los sistemas seguros

    1. Instalar y mantener una configuración de firewall para proteger los datos del titular de la tarjeta.

        Los firewalls son dispositivos que controlan el tráfico entre las redes (internas) y las redes no confiables (externas) de una entidad, así como el tráfico de entrada y salida a áreas más sensibles dentro de las redes internas confidenciales de una entidad.

        Todos los sistemas debe estar protegidos contra el acceso no autorizado desde redes no confiables, ya sea que ingresen al sistema a través de Internet como comercio electrónico, del acceso a Internet desde los ordenadores de los empleados, del

acceso al correo electrónico de los empleados, de conexiones dedicadas como conexiones mediante redes inalámbricas o a través de otras fuentes.

2. No usar los valores predeterminados suministrados por el proveedor para las contraseñas del sistema y otros parámetros de seguridad.

   Las personas malintencionadas (externas e internas a una empresa), por lo general, utilizan las contraseñas predeterminadas por los proveedores y otros parámetros que el proveedor predetermine para comprometer los sistemas. Estas contraseñas y parámetros son conocidos entre las comunidades de hackers y se determinan fácilmente por medio de información pública.

- Proteger los datos del titular de la tarjeta

3. Proteger los datos del titular de la tarjeta que sean almacenados.

   Los métodos de protección como el cifrado, el truncamiento, el ocultamiento y la función de hash son importantes componentes para proteger los datos de los titulares de tarjetas. Si un intruso viola otros controles de seguridad y obtiene acceso a los datos cifrados, sin las claves de cifrado adecuadas, no podrá leer ni utilizar esos datos.

   Guardar las claves secretas y privadas utilizadas para cifrar/descifrar los datos del titular de la tarjeta en una (o más) de las siguientes formas:

   a. Cifradas con una clave de cifrado de claves que sea, al menos, tan sólida como la clave de cifrado de datos y que se almacene separada de la clave de cifrado de datos.

   b. Dentro de un dispositivo seguro criptográfico como un HSM.

   c. Como, al menos, dos claves o componentes de la clave completos de acuerdo con los métodos aceptados por la industria

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

   La información confidencial se debe cifrar durante su transmisión a través de redes a las que delincuentes puedan acceder fácilmente. Por ejemplo, utilizando TLS versión 1.2 o superior.

- Mantener un programa de administración de vulnerabilidades

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

    6. Desarrollar y mantener sistemas y aplicaciones seguros.

        Muchas vulnerabilidades pueden subsanarse mediante parches de seguridad proporcionados por los proveedores. Las entidades que administran los sistemas deben instalar estos parches.

        También es vital la separación de funciones entre entornos de desarrollo, entornos de pruebas y entornos de producción. Los datos de producción (PAN activos) no se deben utilizar para la realización de las pruebas ni para los desarrollos.

- Implementar medidas sólidas de control de acceso

    7. Restringir el acceso a los datos del titular de la tarjeta según la necesidad de saber que tenga la empresa.

        A efectos de asegurar que el personal autorizado sea el único que pueda acceder a los datos importantes, se deben implementar sistemas y procesos que limiten el acceso conforme a la necesidad de conocer y conforme a la responsabilidad del cargo. Por ejemplo, se debe implementar una negación por defecto en el acceso a los datos e ir permitiendo sólo a aquellos roles que deben tener acceso de los datos.

    8. Identificar y autenticar el acceso a los componentes del sistema.

        Al asignar una identificación exclusiva a cada persona que tenga acceso se garantiza que cada una se hará responsable de sus actos. Cuando se ejerce dicha responsabilidad, las medidas implementadas en datos y en sistemas críticos están a cargo de procesos y usuarios conocidos y autorizados y, además, se puede realizar un seguimiento.

        Se recomienda eliminar o inhabilitar las cuentas de usuario inactivas, al menos, cada 90 días. También es recomendable limitar el número de accesos fallidos al sistema por parte de un usuario. Por otro lado, es interesante que para el acceso a los datos importantes se implementen solución que pidan un segundo factor de autenticación (2FA).

        Implementar una buena política de contraseñas también es vital para tener un acceso robusto al sistema. Debe definir la longitud, el contenido y la rotación de las mismas.

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

   Cualquier acceso físico a datos o sistemas que alojen datos de titulares de tarjetas permite el acceso a dispositivos y datos, así como también permite la eliminación de sistemas o copias en papel, y se debe restringir correctamente. Por lo tanto, se deben utilizar controles a la entrada de la empresa apropiados para limitar y supervisar el acceso físico a los sistemas en el entorno de datos del titular de la tarjeta.

- Supervisar y evaluar las redes con regularidad

10. Rastrear y supervisar todos los accesos a los recursos de red y a los datos del titular de la tarjeta.

    Los mecanismos de registro y la posibilidad de rastrear las actividades del usuario son críticos para la prevención, detección o minimización del impacto de los riesgos de datos. Determinar la causa de un riesgo es muy difícil, sino imposible, sin los logs de la actividad del sistema.

    Se deben implementar pistas de auditoría para vincular todo acceso a componentes del sistema con usuarios específicos. Se debe utilizar tecnología de sincronización como, por ejemplo, el NTP (protocolo de tiempo de red) para que los sistemas tengan un horario uniforme y correcto.

11. Probar con regularidad los sistemas y procesos de seguridad.

    Las vulnerabilidades son descubiertas continuamente por personas malintencionadas e investigadores y son introducidas mediante software nuevo. Los componentes del sistema, los procesos y el software personalizado deben evaluarse con frecuencia para garantizar que los controles de seguridad continúen reflejando un entorno dinámico.

- Mantener una política de seguridad de información

12. Mantener una política que aborde la seguridad de la información para todo el personal.

    Una política de seguridad sólida establece el grado de seguridad para toda la entidad e informa al personal sobre lo que se espera de ellos. Todo el personal debe estar al tanto de la confidencialidad de los datos y de sus responsabilidades para protegerlos.

Para obtener un análisis exhaustivo de los requisitos para cumplir con PCI-DSS se recomienda consultar la bibliografía especificada en esta sección. En concreto la referencia [84].

Controles de compensación

Hay que cumplir con todos los requisitos anteriores para cumplir con PCI DSS. No obstante, cuando una entidad no pueda cumplir con alguno de los requisitos anteriores tal y como están definidos en el estándar, por causa de limitaciones técnicas o prácticas bien documentadas y razonables, puede mitigar el riesgo del incumplimiento mediante el establecimiento de controles de compensación.

Cuando una entidad no cumple en su totalidad con alguno de los 12 requisitos de PCI-DSS, por causa justificada (bien por una limitación técnica o un práctica bien documentada), se hace necesario presentar un conjunto de medidas, llamado controles de compensación, que permitan mitigar el riesgo del incumplimiento del requisito. Un control de compensación, para que sea aceptable, debe de cumplir los siguiente requisitos:

- Cumplir con el propósito del requisito original de PCI-DSS.
- Proporcionar un nivel de seguridad similar con la aplicación del control de compensación, del que proporciona el requisito original, o como mínimo que compense el riesgo.
- El cumplimiento de otros requisitos no exime de aplicar medidas compensatorias para el requisito no cumplido en su totalidad.
- Conocer absolutamente el riesgo que conlleva no poder cumplir con un requisito obligatorio.

La información necesaria que debe incluir un control compensatorio es la siguiente:

- Limitaciones o restricciones. Razonar las limitaciones o restricciones que hacen que no se pueda cumplir con el requisito original.
- Objetivo. Definir el objetivo del control original e identificar claramente el objetivo que cumple la medida compensatoria.
- Riesgo. Identificar cualquier riesgo relacionado que implique no cumplir con el requisito.
- Definición. Definir detalladamente el control o controles de compensación, con sus objetivos y sus riesgos, comparándolos con el original.
- Validación. Se debe de probar que los controles compensatorios se han validado y probado de forma satisfactoria.
- Mantenimiento. Definir los procesos de actualización

3.2.2 PCI - DSS y AWS

Amazon Web Services (AWS) está certificado como proveedor de servicios de Nivel 1 PCI DSS 3.2, el nivel más alto de evaluación disponible. La evaluación de conformidad fue realizada por Coalfire Systems Inc., un asesor de seguridad cualificado (QSA) independiente. La Declaración de conformidad (AOC) y el resumen de responsabilidades de PCI DSS están disponibles para clientes mediante AWS Artifact, visto en el apartado 2.5.4.5 Conformidad.

AWS no almacena, transmite ni procesa directamente ningún dato del titular de la tarjeta del cliente . Sin embargo, permite crear entornos propios de datos de titulares de tarjetas , capaces de almacenar, transmitir y procesar datos de titulares de tarjetas mediante el uso de los productos de AWS.

AWS aparece en el registro global de proveedores de servicios de Visa [86] y en la lista de proveedores de servicios en conformidad con MasterCard [87], esto demuestra que AWS ha validado correctamente el cumplimiento de PCI DSS e implementó todos los requisitos correspondientes de los programas de Visa y MasterCard.

La lista de los servicios de AWS que logran el cumplimiento con PCI DSS es prácticamente interminable. [88]

Aunque AWS es una solución multitenant, es decir, el entorno de AWS es un entorno virtualizado con varios clientes. AWS implementó los requisitos de PCI DSS y otros controles compensatorios que asignan de manera segura a cada cliente su propio entorno protegido.

En abril del 2020, los centros de datos de AWS de las siguientes ubicaciones cumplen con el estándar PCI DSS: EE.UU. Este (Norte de Virginia), EE.UU. Este (Ohio), EE.UU. Oeste (Oregón), EE.UU. Oeste (Norte de California), AWS GovCloud (EE.UU.), Canadá (Central), Europa (Irlanda), Europa (Fráncfort), Europa (Londres), Europa (París), Asia Pacífico (Singapur), Asia Pacífico (Sídney), Asia Pacífico (Tokio), Asia Pacífico (Osaka), Asia Pacífico (Seúl), Asia Pacífico (Mumbai) y América del Sur (São Paulo).

AWS incluye varias referencias a documentos [89][90][91] que ayudan al cliente a ser PCI Compliance en sus arquitecturas desplegadas en AWS y una guía de inicio rápido (Quick Start Guide) [92] que proporciona una arquitectura estandarizada para el cumplimiento del estándar PCI DSS. Quick Start Guide [93] proporciona plantillas que configuran automáticamente los recursos de AWS.

Para obtener más detalle sobre la arquitectura desplegada haciendo uso de Quick Start Guide PCI DSS se recomienda consultar el apartado Arquitectura de PCI DSS en AWS que contiene imágenes y explicaciones de la arquitectura desplegada haciendo uso de estas plantillas de inicio rápido. AWS detalla la arquitectura principal, la arquitectura de registro centralizado, la arquitectura de bases de datos y la arquitectura de aplicaciones web. Todas las arquitecturas desplegadas son PCI DSS Compliance, es decir, cumplen con estándar PCI DSS.

3.2.3 PCI - PIN

El documento Payment Card Industry PIN Security Requirements and Testing Procedures [94] define 33 requerimientos de seguridad para la gestión, procesamiento y transmisión del número de identificación personal (PIN, del inglés Personal Identification Number) durante transacciones online y offline relacionadas con tarjetas de pago en cajeros (ATM, del inglés Automatic Teller Machine) y terminales de punto de venta (POS, del inglés point-of-sale) atendidos y desatendidos.

Estos requerimientos se encuentran organizados en 7 grupos denominados Objetivos de Control que deben ser cumplidos por aquellas entidades adquirentes y agentes responsables del procesamiento de PIN en conjunción con otros estándares de la industria aplicables.

Por lo tanto, el estándar PCI PIN es de obligatorio cumplimiento para todas las instituciones adquirientes y agentes responsables del procesamiento de transacciones con PIN de las tarjetas de las marcas del PCI SSC (VISA, MasterCard, AMEX, Discover y JCB) y debe ser usado en conjunción con otros estándares aplicables de la industria como PCI DSS.

Los objetivos de este estándar son:

- Identificar los requerimientos mínimos de seguridad para transacciones de intercambio basadas en PIN.
- Describir los requisitos mínimos aceptables para asegurar el dato del PIN y las claves de cifrado.
- Asistir a todos los participantes del sistema de pago minorista en el establecimiento de garantías de que los datos del PIN de los titulares de tarjetas no se vean comprometidos.

Dado que actualmente, abril 2020, AWS CloudHSM no se puede utilizar para realizar la traducción en bloque del número de identificación personal (PIN) o cualquier otra operación de cifrado que se utilice con las transacciones de pago no se va a entrar en más detalle sobre el estandar PCI PIN. AWS destaca en las FAQs de AWS CloudHSM [42] que en el futuro es posible que ofrezcan funciones de pago.

3.3 Directiva de servicios de pago revisada (PSD2)

PSD 2 es la Directiva de Servicios de Pago revisada, proviene del inglés PSD, Payment Service Providers. El número dos se corresponde con la revisión.

La primera Directiva de Servicios de Pago, Directiva 2007/64/EC [95], surgió en 2007 con el objetivo de contribuir al desarrollo de un mercado de pagos único en la Unión Europea (UE).

En 2013, la Comisión Europea (CE) propuso una revisión, Directiva (UE) 2015/2366 [96], para mejorar la protección del consumidor, impulsar la competencia del sector financiero y reforzar la seguridad en el mercado de pago.

También es importante tener en cuenta el REGLAMENTO DELEGADO (UE) 2018/389 [97] por el que se complementa la Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo en lo relativo a las normas técnicas de regulación para la autenticación reforzada de clientes y unos estándares de comunicación abiertos comunes y seguros.

La principal novedad de la Directiva es la apertura por parte de los bancos de sus servicios de pagos a terceras empresas, los denominados TPP (Third Party Providers).

PSD2 regula dos clases de servicios que ya existían cuando se adoptó la primera PSD en 2007 pero que se estaban popularizando en los últimos años: por un lado los servicios de iniciación de pagos (PIS, Payment Initiation Service) y por otro los servicios de información de cuenta (AIS, Account Information Services).

El servicio de información de cuenta (AIS) consiste en recoger y almacenar la información de las distintas cuentas bancarias de un cliente en un solo lugar, permitiendo a los clientes tener una visión global de su situación financiera y analizar fácilmente sus gastos y sus necesidades financieras.

Por su parte, en el servicio de iniciación de pagos (PIS), terceros proveedores facilitan el uso de la banca online para realizar pagos por internet. PSD2 también posibilita al cliente la realización de pagos a terceros desde la aplicación de una entidad bancaria utilizando cualquiera de sus cuentas (pertenezcan o no a esa entidad).

En los últimos años, se han popularizados los llamados "*Agregadores Financieros*" en la mayoría de entidades financieras más importantes, así como en soluciones de terceros. El ejemplo más conocido de servicios de agregación de un tercero ajeno a las entidades financieras es Fintonic [98].

Los servicios anteriores es básicamente lo que ofrecen los agregadores financieros, posibilitan al cliente tener todas las cuentas que posean en distintas entidades en una única aplicación, ya sea de una de las entidades financieras de las que es cliente o en una aplicación de terceros como, por ejemplo, Fintonic. Además, Fintonic y las entidades bancarias con sus agregadores financieros, permiten el iniciar pagos como una transferencia nacional desde una cuenta de la entidad X en la aplicación de la entidad Y.

Todo esto provee la entrada de nuevos jugadores en el sector financiero que antes no había tal y como se vió en el apartado 1.1 Contexto y justificación del Trabajo.

La otra gran novedad de la PSD2 es la introducción de nuevos requisitos de seguridad, lo que se conoce como Autenticación Reforzada de Clientes (SCA, Strong Customer Authentication). Esto implica el uso de dos factores de autenticación en operaciones bancarias que antes no lo requerían, así como una definición más estricta de lo que puede servir como factor de autenticación.

Para ofrecer este tipo de servicios, antes de PSD2, se utilizaban y aún se utilizan técnicas como el *Web scraping* [99], técnica utilizada para extraer información de sitios web mediante aplicaciones software.

Esto cambia con PSD2, ya que las entidades financieras tienen que proveer a las otras entidades financieras y a terceros la información necesaria para ofrecer los servicios de información de cuentas y de iniciación de pagos a través de API. Estas API están sujetas a las condiciones del escenario PSD2, donde los TPP pueden hacer uso de ellas.

Todo esto desemboca en el concepto de banca abierta u Open Banking promovido por Reino Unido y ajeno a la Unión Europea. No obstante, está basado en un modelo de negocio en el que se permite el intercambio de datos en el ecosistema financiero. El marco legal para todo ello, como no podía ser de otra manera, es la PSD2. En resumen, se establece que la información de los clientes en las entidades bancarias les pertenece a ellos y no a las propias entidades, y que por lo tanto la banca ha de permitir el acceso de terceros a sus sistemas, siempre con el consentimiento de los clientes. Como se ha visto, los TPP, que no necesariamente tienen que ser entidades financieras, pueden acceder a los datos y el comportamiento financiero de sus usuarios siempre que estos lo autoricen expresamente.

A continuación se van a ilustrar a alto nivel mediante una serie de imágenes los actores que intervienen en PSD2, así como una posible arquitectura de referencia de cualquier entidad financiera (ASPSP, Account Servicing Payment Service Provider). [100]

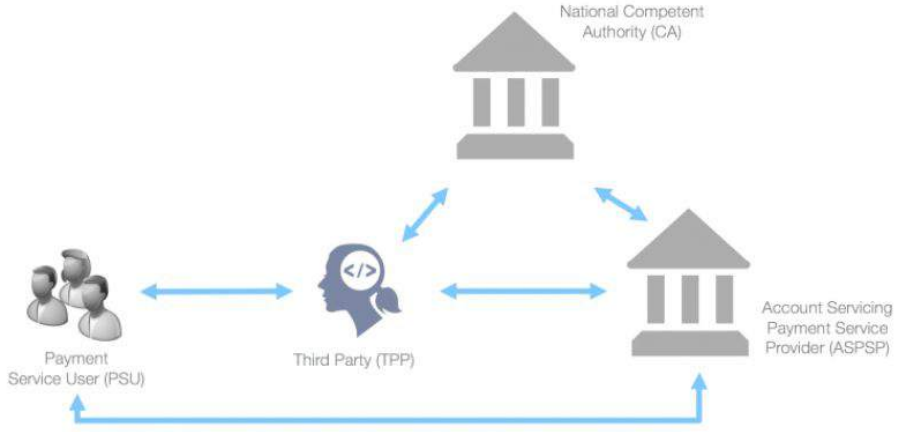

Imagen 42. Actores principales PSD2. [100]

Los actores principales de PSD2 reflejados en la imagen 42 son:

- El usuario como cliente de la entidad financiera (ASPSP) y del TPP.
- El tercero, TPP, por ejemplo Fintonic.
- La entidad financiera, ASPSP, por ejemplo BBVA, Santander, CaixaBank, etc.
- La entidad competente nacional o europea que regule los TPP.

Un ejemplo de realización de pago desde una cuenta de una entidad financiera (ASPSP) en un servicio de un tercero (TPP) con la autorización expresa del cliente se refleja en la imagen 43.

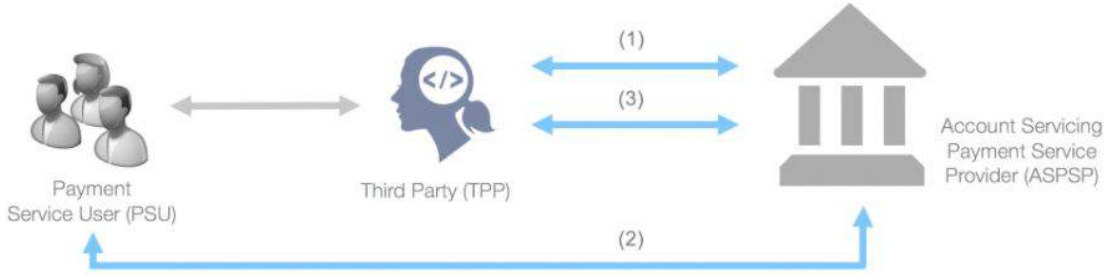

Imagen 43. Realización de pago a través de TPP. [100]

El flujo sería el siguiente:

1. El TPP le pide a la entidad financiera que realice una acción en nombre del cliente, por ejemplo, iniciar un pago.
2. La entidad financiera autentica al cliente, haciendo que el cliente “firme” la acción solicitada por el TPP.
3. Si la respuesta es satisfactoria, El TPP desencadena la ejecución de la acción.

Desde el punto de vista de la seguridad, el enfoque más interesante para administrar estas interacciones es aprovechar OAuth 2.0, en particular el llamado OAuth 2.0 de 3 patas (3-legged OAuth), donde actúan el TPP, el propietario de los datos (el cliente) y la entidad financiera que expone la API.

Por último, antes de pasar a ver la relación entre AWS y la PSD2, una arquitectura de referencia de una entidad financiera tradicional podría ser la siguiente para el cumplimiento de PSD2:

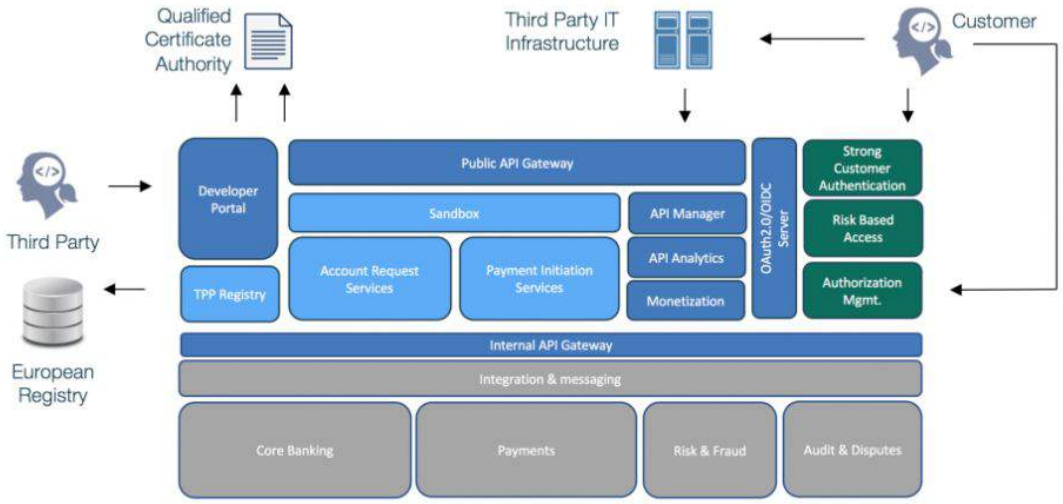

Imagen 44. Arquitectura orientativa ASPSP. [100]

AWS indica que la banca abierta es más que el cumplimiento de una regulación. Considera que la banca abierta crea mejores experiencias para los clientes.

AWS considera que aporta valor a las entidades financieras que crean API en su infraestructura porque con AWS las instituciones financieras pueden cumplir con los requisitos regulatorios mediante el desarrollo de nuevos modelos de negocio, al construir una plataforma segura, escalable e innovadora para la banca abierta en la nube haciendo uso de los servicios de AWS.

AWS lleva años alentando a la industria financiera a sumarse a su plataforma para ofrecer los servicios de API necesarias para el cumplimiento de las directivas. Además, estas directivas ya son una tendencia global como se observar en la imagen 45:

Imagen 45. Open Banking a nivel mundial. [101]

Todo este aumento de estándares de open banking está produciendo el desarrollo de API a gran escala por las diferentes empresas de la industria financiera tal y como refleja la imagen 46.

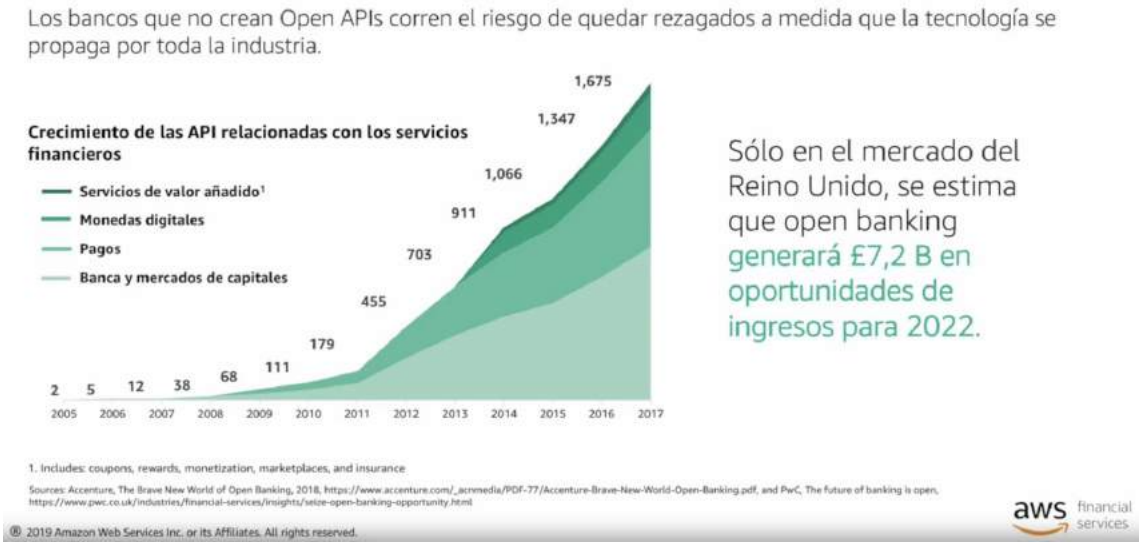

Imagen 46. Crecimiento API servicios financieros en AWS. [101]

En relación con la imagen 44, AWS proporciona su visión a alto de nivel de lo que sería la unión de una solución de banca abierta en AWS en convivencia con un CPD tradicional (on premise) de cualquier entidad financiera. La visión de arquitectura de AWS se puede observar en la imagen 47.

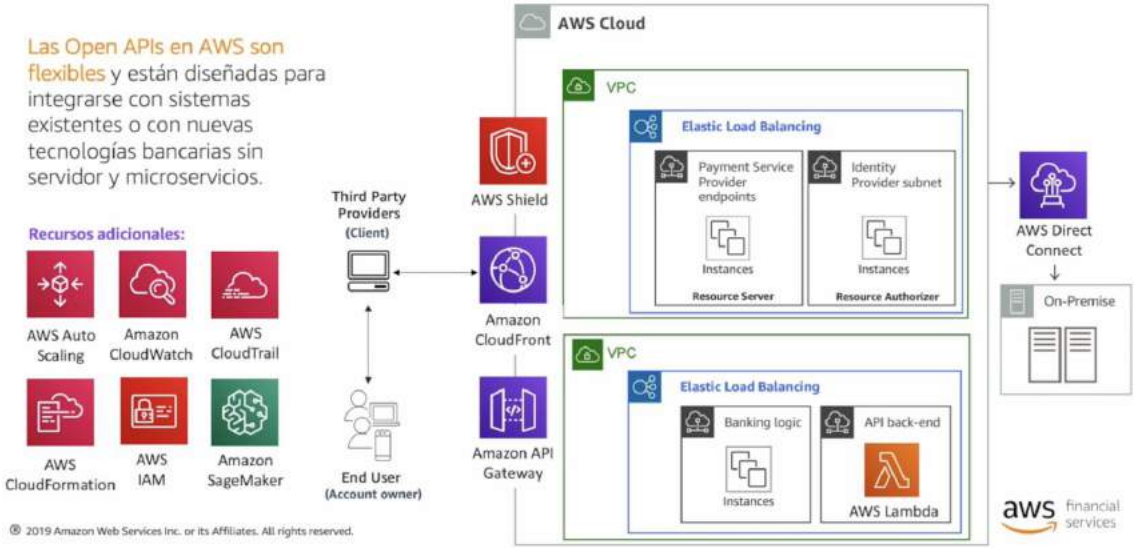

Imagen 47. AWS Open Banking - CPD tradicional on premise. [101]

Para finalizar este apartado se va a enunciar un servicio de AWS que no se ha visto anteriormente en este trabajo y cobra especial relevancia para el cumplimiento de PSD2, ya que facilita toda la gestión de las API.

- **Amazon API Gateway**: [102][103] Es un servicio completamente administrado que facilita a los desarrolladores la creación, la publicación, el mantenimiento, la monitorización y la protección de API a cualquier escala. Ofrece dos opciones para crear las API RESTful, las API HTTP y las API REST, así como una opción para crear las API WebSocket.

  Todas las API creadas con Amazon API Gateway solo exponen los puntos de enlace HTTPS. Amazon API Gateway no soporta puntos de enlace no cifrados (HTTP).

  Con Amazon API Gateway, se tiene la opción de configurar los métodos del API para que exijan autorización.

  Además, Amazon API Gateway se integra con AWS CloudTrail para proporcionar un historial totalmente auditable de los cambios en las API REST. Todas las llamadas a las API efectuadas a las API de Amazon API Gateway para crear, modificar, eliminar o implementar las API de REST se registran en CloudTrail en la cuenta de AWS.

3.4 Reglamento General de Protección de datos (RGPD - GDPR)

El Reglamento General de Protección de Datos (RGPD, del inglés General Data Protection Regulation - GDPR) [104] es el reglamento europeo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). [105]

Entró en vigor el 25 de mayo de 2016 y fue de aplicación el 25 de mayo de 2018, dos años durante los cuales las empresas, las organizaciones, los organismos y las instituciones se fueron adaptando para su cumplimiento. Es una normativa a nivel de la Unión Europea (UE), por lo que cualquier empresa de la unión, o aquellas empresas que tengan negocios en la UE, que manejen información personal de cualquier tipo, deberán acogerse a la misma.

En España, el RGPD dejó obsoleta la Ley Orgánica de Protección de Datos de Carácter Personal (LOPD) de 1999 [106], siendo sustituida el 6 de diciembre de 2018 por la Ley Orgánica 3/2018 [107], de Protección de Datos Personales y garantía de los derechos digitales, acorde con el RGPD.

La Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPD-GDD) es una ley orgánica aprobada por las Cortes Generales de España que tiene por objeto adaptar el Derecho interno español al Reglamento General de Protección de Datos.

Dado que la Ley Orgánica 3/2018 es una Ley Orgánica que trata de adaptar el Derecho interno español a RGPD, en este apartado se van a revisar los puntos más interesantes del propio RGPD. Al final se introduce como AWS provee mecanismos para el cumplimiento del RGPD que también se aplica así mismo, ya que como se ha visto el modelo de seguridad es un modelo de responsabilidad compartida entre el cliente y AWS.

- **Definiciones del RGPD**: El artículo 4 del RGPD proporciona una serie de definiciones que aplican a todo el Reglamento. Se incluyen a continuación las más interesantes en el ámbito de este trabajo:

    - Datos personales: Toda información sobre una persona física identificada o identificable (el interesado); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.

    - Tratamiento: Cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de

habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción;

- Elaboración de perfiles: Toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física.

- Seudonimización: Tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyen a una persona física identificada o identificable.

- Fichero: Todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica.

- Responsable del Tratamiento (RT) o Responsable: La persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros.

- Encargado del Tratamiento (ET) o Encargado: La persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento.

- Consentimiento del interesado: Toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen.

- Violación de la seguridad de los datos personales: Toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

- Datos biométricos: Datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que

permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos.

- Datos relativos a la salud: Datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud.

- Empresa: Persona física o jurídica dedicada a una actividad económica, independientemente de su forma jurídica, incluidas las sociedades o asociaciones que desempeñen regularmente una actividad económica.

- Grupo empresarial: Grupo constituido por una empresa que ejerce el control y sus empresas controladas.

- **Principios del RGPD**: El RGPD además de mantener los principales principios de la LOPD, los refuerza. Los principios del RGPD están recogidos en el Capítulo II, desde el artículo 5 al artículo 11, ambos inclusive.

  - Principios relativos al tratamiento (artículo 5): Los datos personales serán:

    - tratados de manera lícita, leal y transparente en relación con el interesado (licitud, lealtad y transparencia). (art. 5.1 a) RGPD)

    - recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines. (art. 5.1 b) RGPD)

    - adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados (minimización de datos). (art. 5.1 c) RGPD)

    - exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan (exactitud); (art. 5.1 d) RGPD)

    - tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas (integridad y confidencialidad).

- El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo (responsabilidad proactiva). (art. 5.2 RGPD)

Los dos últimos puntos son muy importantes para cualquier empresa porque implican poner mucho esfuerzo en realizar un buen tratamiento del dato, incluido el cifrado de los mismos ya sea en el CPD tradicional on premise o en un sistema de nube pública como puede ser AWS. Además, como dicta el artículo 5.2, la empresa debe ser capaz de demostrar que lo está haciendo.

- Licitud del tratamiento (artículo 6): Los datos personales serán tratados de manera lícita. Para que un tratamiento sea lícito los datos deberán ser tratados con el consentimiento del interesado o sobre alguna otra base legítima establecida en el RGPD. Por lo tanto, tal y como se indica en artículo 6.1 del RGPD, el tratamiento sólo será lícito si se cumple al menos una de las siguientes condiciones (sólo se indican algunas):

  - el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos. (art. 6.1 a) RGPD)

  - el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales. (art. 6.1 b) RGPD)

  - el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento. (art. 6.1 c) RGPD)

  - el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física. (art. 6.1 d) RGPD)

- Condiciones para el consentimiento (artículo 7):

  - art. 7.1: Cuando el tratamiento se base en el consentimiento del interesado, el responsable deberá ser capaz de demostrar que aquel consintió el tratamiento de sus datos personales.

  - art. 7.2: Si el consentimiento del interesado se da en el contexto de una declaración escrita que también se refiera a otros asuntos, la solicitud de consentimiento se presentará de tal forma que se distinga claramente de los demás asuntos, de forma inteligible y de fácil acceso y utilizando un lenguaje claro y sencillo.

  - art. 7.3: El interesado tendrá derecho a retirar su consentimiento en cualquier momento. La retirada del

consentimiento no afectará a la licitud del tratamiento basada en el consentimiento previo a su retirada. Antes de dar su consentimiento, el interesado será informado de ello. Será tan fácil retirar el consentimiento como darlo.

Por lo tanto, el consentimiento debe darse mediante un acto afirmativo claro que refleje una manifestación de voluntad libre, específica, informada, e inequívoca del interesado de aceptar el tratamiento de los datos personales que le conciernen. A diferencia de la legislación anterior el RGPD no contempla el consentimiento tácito o por omisión.

Las formas de otorgar el consentimiento podrían incluir: marcar una casilla de un sitio web en internet, escoger parámetros técnicos para la utilización de servicios de la sociedad de la información, o cualquier otra declaración o conducta que indique claramente en este contexto que el interesado acepta que sus datos personales sean tratados.

En ningún caso se entenderá otorgado el consentimiento cuando aparezcan las casillas premarcadas, el silencio o la inacción.

El consentimiento debe darse para todas las actividades de tratamiento realizadas con el mismo fin o fines. Por tanto, cuando el tratamiento tenga varios fines deberá darse el consentimiento para todos ellos.

El RT deberá ser capaz de demostrar que el interesado ha dado su consentimiento al tratamiento de sus datos personales.

- Condiciones aplicables al consentimiento de los niños (artículo 8): El tratamiento de los datos personales de un niño se considerará lícito cuando tenga como mínimo 16 años. Si el niño es menor de 16 años, tal tratamiento únicamente se considerará lícito si el consentimiento lo dio o autorizó el titular de la patria potestad o tutela sobre el niño, y solo en la medida en que se dio o autorizó. Los Estados miembros podrán establecer por ley una edad inferior a tales fines, siempre que esta no sea inferior a 13 años. (art. 8.1 RGPD).

- Tratamiento de categorías especiales de datos personales (artículo 9): Una de las novedades del RGPD respecto a la normativa anterior es la introducción de nuevas categorías especiales de datos. Estas son los datos biométricos dirigidos a identificar de manera unívoca a una persona física y los datos genéticos.

    - Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical,

y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física. (art. 9.1 RGPD)

- El art. 9.1 no será de aplicación cuando, por ejemplo, el interesado dio su consentimiento explícito para el tratamiento de dichos datos personales con uno o más de los fines especificados, excepto cuando el Derecho de la UE o de los Estados miembros establezca que la prohibición mencionada en el apartado 1 no puede ser levantada por el interesado. (art. 9.2 a) RGPD)

- Tratamiento que no requiere identificación (artículo 11): Si los fines para los cuales un responsable trata datos personales no requieren o ya no requieren la identificación de un interesado por el responsable, este no estará obligado a mantener, obtener o tratar información adicional con vistas a identificar al interesado con la única finalidad de cumplir el presente Reglamento. (art. 11.1 RGPD).

  La identificación incluye la identificación digital del interesado, por ejemplo, las credenciales empleadas por el interesado para abrir una sesión en el servicio en línea ofrecido por el RT.

- **Derechos del interesado**: El RGPD contempla los conocidos como derechos ARCO [108] recogidos en la legislación anterior y añade dos nuevos derechos: limitación del tratamiento y portabilidad. Además, establece la diferencia entre el derecho de rectificación y el derecho de supresión (derecho al olvido). Los derechos del interesado en el RGPD están recogidos en el Capítulo III, desde el artículo 12 al artículo 23, ambos inclusive divididos en varias secciones.

  - Transparencia de la información (artículo 12): Se incrementa la información que el RT deberá facilitar a los interesados en el momento de la recogida de los datos personales respecto a LOPD. En la LOPD está recogido en el artículo 5, mientras que el RGPD está indicado en los artículos 13 y 14.

    - El RT tomará las medidas oportunas para facilitar al interesado toda información indicada en los artículos 13 y 14, así como cualquier comunicación con arreglo a los artículos 15 a 22 y 34 relativa al tratamiento, en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo, en particular cualquier información dirigida específicamente a un niño. La información será facilitada por escrito o por otros medios, inclusive, si procede, por medios electrónicos. Cuando lo solicite el interesado, la información podrá facilitarse

verbalmente siempre que se demuestre la identidad del interesado por otros medios. (art. 12.1 RGPD)

- El responsable del tratamiento facilitará al interesado información relativa a sus actuaciones sobre la base de una solicitud con arreglo a los artículos 15 a 22, y, en cualquier caso, en el plazo de un mes a partir de la recepción de la solicitud. (art. 12.3 RGPD)

- Información que debe facilitarse al interesado cuando los datos se obtengan del interesado (artículo 13) y cuando no se obtengan del interesado (artículo 14).

  - Cuando se obtengan de un interesado datos personales relativos a él, el responsable del tratamiento, en el momento en que estos se obtengan, le facilitará toda la información indicada a continuación (art. 13.1 RGPD) y cuando los datos personales no se hayan obtenidos del interesado, el responsable del tratamiento le facilitará la siguiente información (art. 14.1 RGPD):

    - La identidad y los datos de contacto del responsable y, en su caso, de su representante. (art. 13.1 a) RGPD) (art. 14.1 a) RGPD)

    - Los datos de contacto del delegado de protección de datos, en su caso. (art. 13.1 b) RGPD) (art. 14.1 b) RGPD)

    - Los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento. (art. 13.1 c) RGPD) (art. 14.1 c) RGPD)

    - Etcétera

  - Además de la información mencionada en el apartado 1, el responsable del tratamiento facilitará al interesado, en el momento en que se obtengan los datos personales, la siguiente información necesaria para garantizar un tratamiento de datos leal y transparente (art. 13.2 RGPD) (art. 14.2 RGPD):

    - El plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo. (art. 13.2 a) RGPD) (art. 14.2 a) RGPD)

    - La existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, o a oponerse al

tratamiento, así como el derecho a la portabilidad de los datos. (art. 13.2 b) RGPD) (art. 14.2 c) RGPD)

- Etcétera

- Derecho de acceso del interesado (artículo 15): Derecho de los interesados a obtener del responsable del tratamiento confirmación de si se están tratando o no sus datos personales y, en el primer caso, tiene derecho a acceder a la siguiente información (art.15 RGPD):

  - Los fines del tratamiento. (art. 15.1 a) RGPD)
  - Las categorías de datos personales de que se trate. (art. 15.1 b) RGPD)
  - Los destinatarios o las categorías de destinatarios a los que se comunicaron o serán comunicados los datos personales, en particular destinatarios en terceros u organizaciones internacionales. (art. 15.1 c) RGPD)
  - El plazo previsto de conservación de los datos personales o, de no ser posible, los criterios utilizados para determinar este plazo. (art. 15.1 d) RGPD)
  - Etcétera.

  Cuando se transfieran datos personales a un tercer país o a una organización internacional, el interesado tendrá derecho a ser informado de las garantías adecuadas en virtud del artículo 46 relativas a la transferencia. (art. 15.2 RGPD)

  El responsable del tratamiento facilitará una copia de los datos personales objeto de tratamiento. El responsable podrá percibir por cualquier otra copia solicitada por el interesado un canon razonable basado en los costes administrativos. Cuando el interesado presente la solicitud por medios electrónicos, y a menos que este solicite que se facilite de otro modo, la información se facilitará en un formato electrónico de uso común. (art. 15.3 RGPD)

- Derecho de rectificación (artículo 16): El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la rectificación de los datos personales inexactos que le conciernan. Teniendo en cuenta los fines del tratamiento, el interesado tendrá derecho a que se completen los datos personales que sean incompletos, inclusive mediante una declaración adicional.

- Derecho de supresión (artículo 17): También conocido como derecho al olvido, el interesado tendrá derecho a obtener sin

dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan, el cual estará obligado a suprimir sin dilación indebida los datos personales cuando concurra alguna de las circunstancias siguientes (art. 17.1 RGPD):

- Los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo. (art. 17.1 a) RGPD)

- El interesado retire el consentimiento en que se basa el tratamiento de conformidad con el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), y este no se base en otro fundamento jurídico. (art. 17.1 b) RGPD)

- Derecho a la limitación del tratamiento (artículo 18): Supone que a solicitud del interesado el responsable del tratamiento deberá dejar de tratar los datos personales del interesado. La limitación del tratamiento consiste en el marcado de los datos de carácter personal conservados con el fin de limitar su tratamiento en el futuro.

- Obligación de notificación relativa a la rectificación o supresión de datos personales o la limitación del tratamiento (artículo 19): El responsable del tratamiento comunicará cualquier rectificación o supresión de datos personales o limitación del tratamiento efectuada con arreglo al artículo 16, al artículo 17, apartado 1, y al artículo 18 a cada uno de los destinatarios a los que se hayan comunicado los datos personales, salvo que sea imposible o exija un esfuerzo desproporcionado. El responsable informará al interesado acerca de dichos destinatarios, si este así lo solicita.

- Derecho a la portabilidad de los datos (artículo 20): Permite a los interesados recibir sus datos personales en formato estructurado, de uso común, de lectura mecánica e interoperable y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado.

- Derecho de oposición (artículo 21): El interesado tendrá derecho a oponerse en cualquier momento, por motivos relacionados con su situación particular, a que datos personales que le conciernan sean objeto de un tratamiento basado en lo dispuesto en el artículo 6, apartado 1, letras e) o f), incluida la elaboración de perfiles sobre la base de dichas disposiciones. El responsable del tratamiento dejará de tratar los datos personales, salvo que acredite motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del interesado, o para la formulación, el ejercicio o la defensa de reclamaciones.

Cuando el tratamiento de datos personales tenga por objeto la mercadotecnia directa, el interesado tendrá derecho a oponerse en todo momento al tratamiento de los datos personales que le conciernan, incluida la elaboración de perfiles en la medida en que esté relacionada con la citada mercadotecnia. (art. 21.2 RGPD)

- Decisiones individuales automatizadas (artículo 22): Todo interesado tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar. (art. 22.1 RGPD)

  El art. 22.1 no aplicará si es necesaria para la celebración o la ejecución de un contrato entre el interesado y un responsable del tratamiento. (art. 22.2 a) RGPD)

  Este tipo de tratamiento también se refiere a la elaboración de perfiles consistentes en cualquier forma de tratamiento de los datos personales que evalúe aspectos personales relativos a una persona física, especialmente cuando se analice o prediga aspectos relacionados con el rendimiento en el trabajo, la situación económica, la salud, las preferencias o intereses personales, la fiabilidad o el comportamiento, la situación o los movimientos del interesado, siempre que produzcan efectos jurídicos en él o le afecte de manera significativamente de manera similar.

  En ningún caso las decisiones automatizadas podrán afectar a los menores. Las decisiones automatizadas y la elaboración de perfiles sobre la base de las categorías especiales de datos únicamente podrán autorizarse en condiciones específicas.

- Limitaciones de los derechos del interesado (artículo 23): El RGPD indica que se puedan imponer limitaciones en el ejercicio de los derechos establecidos en el mismo. Dichas limitaciones deberán establecerse por el Derecho de la UE o de los Estados miembros mediante una ley que deberá respetar los derechos y libertades fundamentales, además deberá ser una medida necesaria y proporcionada.

  Por ejemplo, se podrán limitar los derechos de los interesados para salvaguardar la seguridad del Estado, la defensa y la seguridad pública. (art. 23.1 a) b) y c) RGPD)

- **Responsable del tratamiento (RT) y encargado del tratamiento (ET)**: El capítulo 4 del RGPD, hace alusión al responsable del tratamiento y al encargado del tratamiento, entre los artículos que van desde el 23 hasta el 43, ambos inclusive.

La primera sección indica las obligaciones generales. La segunda sección, a partir del artículo 32, trata sobre la seguridad de los datos personales. La tercera sección incide en la evaluación de impacto relativa a la protección de datos y consulta previa. La cuarta sección define la figura del Delegado de Protección de Datos (DPD, del inglés Data Protection Officer - DPO). Por último, la quinta sección establece las directrices en cuanto a códigos de conducta y certificación.

Lo más interesantes en el ámbito de este trabajo son los siguientes:

- Responsabilidad del responsable del tratamiento (artículo 24): Teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario. (art. 24.1 RGPD)

  Cuando sean proporcionadas en relación con las actividades de tratamiento, entre las medidas mencionadas en el apartado 1 se incluirá la aplicación, por parte del responsable del tratamiento, de las oportunas políticas de protección de datos. (art. 24.2 RGPD)

- Protección de datos desde el diseño y por defecto (artículo 25): El responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados. (art. 25.1 RGPD)

  El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, sólo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas. (art. 25.2 RGPD)

- Encargado del tratamiento (artículo 28): Cuando se vaya a realizar un tratamiento por cuenta de un responsable del

tratamiento, este elegirá únicamente un encargado que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, de manera que el tratamiento sea conforme con los requisitos del presente Reglamento y garantice la protección de los derechos del interesado. (art. 28.1 RGPD)

El encargado del tratamiento no recurrirá a otro encargado sin la autorización previa por escrito, específica o general, del responsable. En este último caso, el encargado informará al responsable de cualquier cambio previsto en la incorporación o sustitución de otros encargados, dando así al responsable la oportunidad de oponerse a dichos cambios. (art. 28.2 RGPD)

El tratamiento por el encargado se regirá por un contrato u otro acto jurídico con arreglo al Derecho de la Unión o de los Estados miembros, que vincule al encargado respecto del responsable y establezca el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable. Dicho contrato o acto jurídico estipulará, en particular, que el encargado:

- Tratará los datos personales únicamente siguiendo instrucciones documentadas del responsable, inclusive con respecto a las transferencias de datos personales a un tercer país o una organización internacional, salvo que esté obligado a ello en virtud del Derecho de la Unión o de los Estados miembros que se aplique al encargado; en tal caso, el encargado informará al responsable de esa exigencia legal previa al tratamiento, salvo que tal Derecho lo prohíba por razones importantes de interés público. (art. 28.3 a) RGPD)

- Garantizará que las personas autorizadas para tratar datos personales se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación de confidencialidad de naturaleza estatutaria. (art. 28.3 b) RGPD)

- Tomará todas las medidas necesarias de conformidad con el artículo 32. (art. 28.3 c) RGPD)

- Asistirá al responsable, teniendo cuenta la naturaleza del tratamiento, a través de medidas técnicas y organizativas apropiadas, siempre que sea posible, para que este pueda cumplir con su obligación de responder a las solicitudes que tengan por objeto el ejercicio de los derechos de los interesados establecidos en el capítulo III. (art. 28.3 e) RGPD)

- Ayudará al responsable a garantizar el cumplimiento de las obligaciones establecidas en los artículos 32 a 36, teniendo en cuenta la naturaleza del tratamiento y la información a disposición del encargado. (art. 28.3 f) RGPD)

- A elección del responsable, suprimirá o devolverá todos los datos personales una vez finalice la prestación de los servicios de tratamiento, y suprimirá las copias existentes a menos que se requiera la conservación de los datos personales en virtud del Derecho de la Unión o de los Estados miembros. (art. 28.3 g) RGPD)

- Pondrá a disposición del responsable toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas en el presente artículo, así como para permitir y contribuir a la realización de auditorías, incluidas inspecciones, por parte del responsable o de otro auditor autorizado por dicho responsable. (art. 28.3 h) RGPD)

  En relación con lo dispuesto en la letra h), el encargado informará inmediatamente al responsable si, en su opinión, una instrucción infringe el presente Reglamento u otras disposiciones en materia de protección de datos de la Unión o de los Estados miembros.

Cuando un encargado del tratamiento recurra a otro encargado para llevar a cabo determinadas actividades de tratamiento por cuenta del responsable, se impondrán a este otro encargado, mediante contrato u otro acto jurídico establecido con arreglo al Derecho de la Unión o de los Estados miembros, las mismas obligaciones de protección de datos que las estipuladas en el contrato u otro acto jurídico entre el responsable y el encargado, en particular la prestación de garantías suficientes de aplicación de medidas técnicas y organizativas apropiadas de manera que el tratamiento sea conforme con las disposiciones del RGPD. Si ese otro encargado incumple sus obligaciones de protección de datos, el encargado inicial seguirá siendo plenamente responsable ante el responsable del tratamiento por lo que respecta al cumplimiento de las obligaciones del otro encargado. (art. 28.4 RGPD)

Este es el artículo que principalmente debe cumplir el proveedor de servicios cloud cuando es contratado por una empresa para tratamiento de sus datos, ya sean departamentales, confidenciales, etc. AWS debe mostrar que cumple con lo expuesto en el artículo 28 para ser GDPR Compliance.

- Registro de las actividades del tratamiento (artículo 30): Ya no es necesario inscribir los ficheros en el Registro General de

Protección de datos de la AEPD. Sin embargo, ahora es necesario que el responsable del tratamiento y el encargado del tratamiento tengan registros escritos, inclusive en formato electrónico, de las actividades de tratamiento de los datos que llevan a cabo.

No se aplica a ninguna empresa ni organización que emplee a menos de 250 personas, a menos que el tratamiento que realice pueda entrañar un riesgo para los derechos y libertades de los interesados, no sea ocasional, o incluya categorías especiales de datos personales indicadas en el artículo 9, apartado 1, o datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10. (artículo 30.5 RGPD)

Cada registro debe contener la siguientes información (artículo 30.1 RGPD):

- El nombre y los datos de contacto del responsable y, en su caso, del corresponsable, del representante del responsable, y del delegado de protección de datos.
- Los fines del tratamiento.
- Una descripción de las categorías de interesados y de las categorías de datos personales.
- Las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales.
- En su caso, las transferencias de datos personales a un tercer país o una organización internacional, incluida la identificación de dicho tercer país u organización internacional.
- Cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos.
- Cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad a que se refiere el artículo 32, apartado 1.

Tanto los RT como los ET están obligados a cooperar con la autoridad de control y a poner a disposición de esta los registros, de modo que puedan supervisar las operaciones. (artículo 31)

- Seguridad del tratamiento (artículo 32): A diferencia de la normativa anterior, el RGPD no recoge ni prevé desarrollar un catálogo de medidas de seguridad concretas. Únicamente hace referencia a la seudonimización y al cifrado de los datos, pero sin

especificar nada más. Respecto a la metodología del análisis de riesgos a utilizar, el RGPD no menciona nada.

Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:

- La seudonimización y el cifrado de datos personales.
- La capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.
- La capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico.
- Un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

La adhesión a un código de conducta aprobado a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrá servir de elemento para demostrar el cumplimiento de los requisitos establecidos en el apartado 1 del presente artículo. (art. 32.3)

El responsable y el encargado del tratamiento tomarán medidas para garantizar que cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales sólo pueda tratar dichos datos siguiendo instrucciones del responsable, salvo que esté obligada a ello en virtud del Derecho de la Unión o de los Estados miembros. (art. 32.4)

- Notificación de una violación de la seguridad de los datos personales a la autoridad de control (artículo 33): En caso de violación de la seguridad de los datos personales, el responsable del tratamiento la notificará a la autoridad de control competente de conformidad con el artículo 55 sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Si la notificación a la autoridad de control no tiene lugar en el plazo de 72 horas,

deberá ir acompañada de indicación de los motivos de la dilación.

El encargado del tratamiento notificará sin dilación indebida al responsable del tratamiento las violaciones de la seguridad de los datos personales de las que tenga conocimiento. (art. 33.2)

La notificación contemplada en el apartado 1 deberá, como mínimo (art. 33.3):

- La naturaleza de la violación de seguridad y las categorías de datos y el número de interesados afectados.
- Los datos del delegado de protección de datos.
- Descripción de las posibles consecuencias de la violación.
- Descripción de las medidas adoptadas o propuestas para remediar la violación y mitigar las consecuencias.

Si no fuera posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se facilitará de manera gradual sin dilación indebida. (art. 33.4 RGPD)

- Comunicación de una violación de la seguridad de los datos personales al interesado (artículo 34): Si la violación de seguridad puede comportar alto riesgo para los derechos de los interesados, el RT deberá comunicarlo sin dilación indebida al interesado.

  La comunicación al interesado describirá en un lenguaje claro y sencillo la naturaleza de la violación de la seguridad de los datos personales y contendrá como mínimo la información y las medidas a que se refiere el artículo 33, apartado 3, letras b), c) y d). (art. 34.2 RGPD)

  La comunicación al interesado no será necesaria si se cumple alguna de las condiciones indicadas en el artículo 34.3.

- Evaluación de impacto relativa a la protección de datos (artículo 35): Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales.

  El RGPD prevé que la autoridad de control como la AEPD o la APDCAT pueda elaborar listas de tratamientos que requieran una evaluación de impacto relativa a la protección de datos. (art. 35.4)

  La autoridad de control podrá asimismo establecer y publicar la

lista de los tipos de tratamiento que no requieren evaluaciones de impacto relativas a la protección de datos. (art. 35.5)

La evaluación deberá incluir como mínimo (art. 35.6)

- Una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento, inclusive, cuando proceda, el interés legítimo perseguido por el responsable del tratamiento.
- Una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad.
- Una evaluación de los riesgos para los derechos y libertades de los interesados.
- Las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales, y a demostrar la conformidad con el RGPD, teniendo en cuenta los derechos e intereses legítimos de los interesados y de otras personas afectadas.

- Consulta previa (artículo 36): El responsable consultará a la autoridad de control antes de proceder al tratamiento cuando una evaluación de impacto relativa a la protección de los datos en virtud del artículo 35 muestre que el tratamiento entrañaría un alto riesgo si el responsable no toma medidas para para mitigarlo.

- Delegado de Protección de Datos (DPD, del inglés Data Protection Officer - DPO): Se trata de una figura que surge con el RGPD. Se trata de una persona que posee conocimientos especializados en derecho y práctica en materia de protección de datos. Los DPD podrán ser o no empleados del RT o ET. En cualquier caso, deben desempeñar sus funciones de manera independiente.

  Del artículo 39.1, se desprende que el delegado de protección de datos tendrá como mínimo las siguientes funciones:

  - Informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del presente Reglamento y de otras disposiciones de protección de datos de la Unión o de los Estados miembros. (art. 39.1 a) RGPD)
  - Supervisar el cumplimiento de lo dispuesto en el RGPD, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección

de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes. (art. 39.1 b) RGPD)

- Ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación de conformidad con el artículo 35. (art. 39.1 c) RGPD)
- Cooperar con la autoridad de control. (art. 39.1 d) RGPD)
- Actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36, y realizar consultas, en su caso, sobre cualquier otro asunto. (art. 39.1 e) RGPD)

- Certificación (artículo 42): Los Estados miembros, las autoridades de control, el Comité y la Comisión promoverán, en particular a nivel de la Unión, la creación de mecanismos de certificación en materia de protección de datos y de sellos y marcas de protección de datos a fin de demostrar el cumplimiento de lo dispuesto en el RGPD en las operaciones de tratamiento de los responsables y los encargados. Se tendrán en cuenta las necesidades específicas de las microempresas y las pequeñas y medianas empresas.

  La certificación será voluntaria y estará disponible a través de un proceso transparente. (art. 42.3 RGPD)

  La certificación se expedirá a un responsable o encargado de tratamiento por un período máximo de tres años y podrá ser renovada en las mismas condiciones, siempre y cuando se sigan cumpliendo los requisitos pertinentes. (art. 42.7 RGPD)

- Organismo de certificación (artículo 43): Los organismos de certificación que tengan un nivel adecuado de pericia en materia de protección de datos expedirán y renovarán las certificaciones una vez informada la autoridad de control.

- **Transferencias de datos personales a terceros países u organizaciones internacionales**: Una de las novedades que introduce el RGPD en cuanto a las transferencias internacionales de datos es la posibilidad de que el encargado del tratamiento pueda realizar transferencia de este tipo.

  Se produce una transferencia internacional de datos cuando se transfieren datos personales desde la UE a países terceros, es decir a países situados fuera del Espacio Económico Europeo (EEE). (art. 44)

Sólo se permiten este tipo de transferencias si existe una decisión de adecuación (art. 45 - Transferencias basadas en una decisión de adecuación) o, no habiendo una decisión de adecuación, se ofrecen las garantías adecuadas para llevarla a cabo (art. 46 -Transferencias mediante garantías adecuadas).

Hay cuestiones en las que el RGPD se queda escueto y no proporciona suficiente detalle en algunos de los artículos. Por eso se recomienda consultar también las publicaciones del Grupo de trabajo del artículo 29. Este Grupo de trabajo (GT Art. 29 o en inglés Art. 29 WG) es el grupo de trabajo europeo independiente que se ha ocupado de cuestiones relacionadas con la protección de la privacidad y los datos personales hasta el 25 de mayo de 2018 (entrada en aplicación del RGPD). Las publicaciones del GT Art. 29 están accesibles para su consulta de manera pública [109]. En concreto, se recomienda consultar el apartado de *Guidelines* [110].

La AEPD también ha elaborado una serie de guías para aterrizar los expuesto en el RGPD haciendo referencia a este y a algunas de las publicaciones del Grupo de Trabajo del Artículo 29. Algunas de estas guías son las siguientes:

- Guía para clientes que contraten servicios de Cloud Computing. [111]
- Orientaciones para prestadores de servicios de Cloud Computing. [112]
- Guía Práctica de análisis de riesgos en los tratamientos de datos personales sujetos al RGPD. [113]
- Guía práctica para las Evaluaciones de Impacto en la Protección de los datos sujetas al RGPD. [114]

3.4.1 RGPD y AWS

Por último, en este apartado del trabajo se va a introducir cómo AWS provee mecanismos para el cumplimiento del RGPD que también se aplica así mismo, ya que como se ha visto el modelo de seguridad es un modelo de responsabilidad compartida entre el cliente y AWS. [115] [116]

Por ejemplo, se ha visto que el artículo 25 del RGPD, establece la necesidad de implementar medidas técnicas apropiadas para garantizar que, por defecto, se protege el dato desde el diseño, así como se garantiza que se cumple con el procesamiento de datos mínimo e imprescindible.

Para ello, AWS pone a disposición de los cliente servicios como:

- AWS IAM para toda la gestión de acceso al dato.
- AWS Security Token Service (AWS STS) para proporcionar accesos temporales a los datos necesarios.
- Autenticación basada en múltiples factores (MFA) para robustecer el acceso a los datos.
- Acceso restringido a los recursos incluso de manera interna a otros servicios de AWS.

- AWS Secrets Manager para la gestión de secretos.
- Restricciones en el acceso en función de la ubicación del origen de la petición.
- AWS Cognito para controlar el acceso a los datos a través de aplicaciones móviles y aplicaciones web.
- Cloud Formation, servicio enfocado a la infraestructura como código (IaC, Infrastructure as code), proporciona un lenguaje común para describir y aprovisionar todos los recursos de la infraestructura, incluidas las políticas de seguridad.

El artículo 30 del RGPD indica que, tanto el responsable del tratamiento como el encargado del tratamiento deben contar con un registro de las actividades del tratamiento. Para cumplir con esto, AWS ofrece servicios de monitorización y trazabilidad. Por ejemplo:

- AWS Config ofrece al cliente una vista detallada de la configuración de los recursos de su cuenta de AWS. Esto incluye cómo se relacionan entre sí y cómo fueron configurados.
- AWS CloudTrail, permite monitorizar continuamente la actividad de la cuenta de AWS.

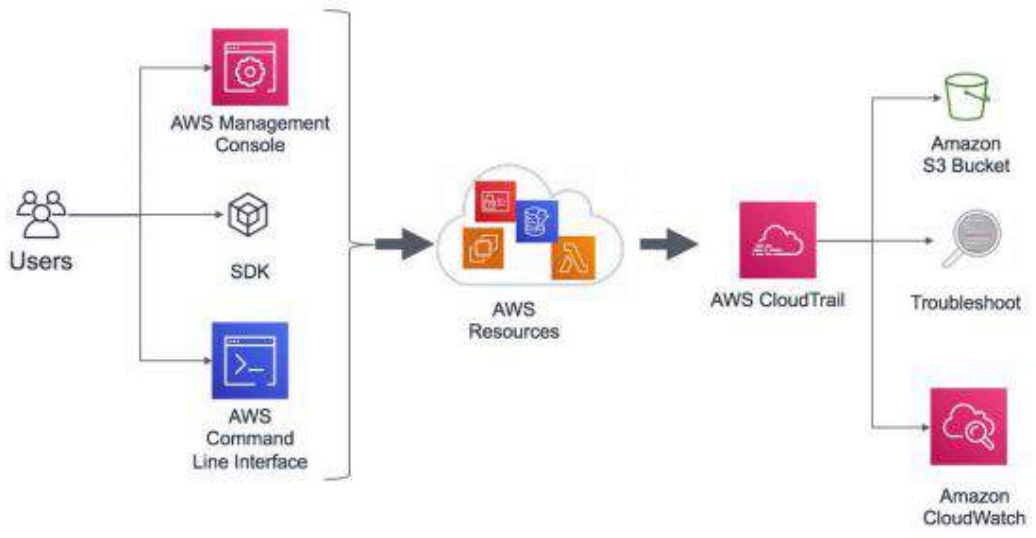

Imagen 48. Ejemplo de arquitectura para auditoría de cumplimiento y análisis de seguridad con AWS CloudTrail.

El artículo 32 del RGPD, exige que las organizaciones implementen medidas técnicas y organizativas para garantizar un nivel de seguridad apropiado, incluyendo la seudonimización y el cifrado de datos personales. Adicionalmente, las organizaciones deben protegerse contra la divulgación no autorizada o el acceso a los datos personales.

Por lo tanto, AWS recomienda el cifrado de los datos puesto que reduce los riesgos asociados al almacenamiento de datos personales porque los datos son ilegibles mientras no se descifren. Una estrategia de cifrado completa puede ayudar a mitigar el impacto de posibles brechas de seguridad. Como se

ha visto en el apartado 2.5.3.1 - Servicios de cifrado en AWS, AWS provee servicios para el cifrado de los datos en reposo (at rest) y para el cifrado de los datos en tránsito (in transit), así como herramientas para el cifrado de los datos como pueden ser AWS KMS, AWS CloudHSM, AWS Encryption SDK, etc.

4. Cloud Access Security Broker (CASB) - Agentes de seguridad de acceso a la nube

4.1 Introducción a los CASB

Según la Cloud Security Alliance (CSA) [40], un CASB es un producto que intercepta las comunicaciones que se dirigen a un servicio en la nube o que se conectan directamente al servicio a través de una API con el fin de monitorizar la actividad, aplicar políticas y detectar y/o prevenir problemas de seguridad.

Los CASB también pueden conectarse a herramientas on premise del cliente para ayudar a una entidad a detectar, evaluar y potencialmente bloquear el uso de la nube y de servicios no aprobados en la entidad. Si bien hay opciones de CASB en las instalaciones on premise del cliente, a menudo también se ofrece como un servicio alojado en la nube.

Algunos CASB incluyen características básicas de DLP para los servicios específicos que protegen. Obviamente la eficiencia del CASB viene determinada, en gran medida, en cómo el producto está integrado para realizar la monitorización.

Algunos CASB también pueden enrutar tráfico a plataformas dedicadas de DLP para un análisis más robusto que el que típicamente está disponible en el CASB cuando ofrece características de DLP.

Según Gartner [120], los CASB son productos/servicios que cubren *gaps* de las organizaciones en el uso de servicios en la nube en lo que a la seguridad respecta. Consideran que esta tecnología resulta necesaria para securizar los servicios en la nube.

Los CASB proporcionan un punto central para el gobierno del uso de los servicios en la nube de una organización y sería la ubicación donde aplicar políticas sobre los mismos, teniendo una visión granular que permite tener el control de las actividades del usuario, así como de los datos sensibles.

La cobertura de los CASB se aplica a todos los modelos de prestación de servicios en la nube de software como servicio (SaaS), plataforma como servicio (PaaS) e infraestructura como servicio (IaaS).

Los CASB proporcionan las funcionalidades basados en cuatro pilares:

- Visibilidad: proporcionan el descubrimiento en la organización del denominado *shadow IT*, es decir, todo software o hardware no censado en la organización. Proporciona además una vista consolidada de los servicios en la nube de una organización y detalles sobre los usuarios que acceden a los datos de los servicios en la nube, así como desde qué dispositivo y desde qué ubicación.

- Seguridad de los datos: Ofrecen la posibilidad de aplicar políticas de seguridad centradas en los datos para evitar actividades no deseadas basadas en la clasificación de los datos, en el descubrimiento de datos y en la supervisión de la actividad de los usuarios en lo que respecta al

acceso a datos confidenciales o la escalada de privilegios para el acceso a estos.

Algunos CASB ofrecen la posibilidad de cifrar, *tokenizar* o marcar el contenido a nivel de campo y de archivo en los servicios en la nube. No obstante, esto puede hacer perder funcionalidades en los servicios de nube.

- Protección de amenazas: Los CASB impiden que los dispositivos, los usuarios y las versiones de aplicaciones no deseadas accedan a los servicios de la nube, proporcionando controles de acceso adaptativos (AAC, Adaptive Access Controls).

  También algunos CASB pueden proporcionar un análisis de comportamiento de los usuarios y de las entidades (UEBA, User and Entity Behavior Analytics) para identificar comportamientos anómalos, *sandboxing* de redes e identificación y reparación de malware.

- Cumplimiento (*compliance*): A través de sus capacidades de visibilidad y control, los CASB ayudan a cumplir los requisitos de ubicación de datos y de cumplimiento normativo. Por ejemplo, para cumplir con el RGPD, visto en 3.4 Reglamento General de Protección de Datos, salvo alguna excepción, es requisito que los datos estén ubicados y se traten en la Unión Europea.

  Muchos proveedores de CASB han añadido capacidades de CSPM (Cloud Security Posture Management) a sus productos. CSPM evalúa y gestiona la configuración de seguridad en la nube, sobre todo para IaaS y cada vez más para SaaS. A grandes rasgos, son herramientas que buscan evitar configuraciones incorrectas que puedan conducir a la fuga de datos.

Para lograr estos objetivos los CASB se integran en un CPD corporativo o en un modo híbrido que involucra el CPD y la plataforma de servicio de nube, pero la mayoría de las empresas eligen un CASB que opera exclusivamente desde la nube.

Las tres formas principales en las que puede operar un CASB son:

- Proxy inverso (Reverse proxy)
- Proxy de reenvío (Forward proxy)
- Modo API

Tras el estudio realizado por Gartner, publicaron un cuadrante mágico como el mostrado en la imagen 8 para el uso del los cloud público, pero en este caso enfocado a los CASB. Este cuadrante se puede observar en la imagen 49.

Imagen 49. Gartner Magic Quadrant estudio sobre CASB.

Para Gartner, los líderes demuestran un progreso y esfuerzo equilibrados en todas las categorías de ejecución y visión. Además producen productos que incorporan todas las capacidades y opciones arquitectónicas de CASB. En el siguiente apartado se van a introducir algunos de ellos.

4.2 Principales CASB

A continuación se van a introducir algunos de los principales CASB, basados en el estudio de Gartner [120]:

- Microsoft Cloud App Security: [121] Microsoft Cloud App Security (MCAS) es un CASB de proxy inverso más API. Se trata de un CASB que funciona en varias nubes. Recomendado por Microsoft principalmente para cubrir los siguientes fines [122]:
    - Detección y evaluación de aplicaciones en la nube
    - Aplicación de directivas de gobernanza de la nube
    - Limitación de la exposición de datos compartidos y aplicación de directivas de colaboración
    - Detección, clasificación, etiquetado y protección de datos regulados y confidenciales almacenados en la nube
    - Aplicación de directivas de cumplimiento y de DLP para datos almacenados en la nube
    - Detección de amenazas en la nube, cuentas en peligro, colaboradores malintencionados y ransomware
    - Servicios de IaaS seguros y aplicaciones personalizadas

  Aunque la integración es mejor con Microsoft Azure y el resto de la suite de SaaS de Microsoft como, por ejemplo, Office 365, OneDrive, etc, ya se apoya en Azure Active Directory [123], también ofrece para algunos fines integración con Dropbox, G Suite, Salesforce, WebEx e incluso, Amazon Web Services (AWS) [124].

- Netskope: [125][126][127] Permite identificar y administrar rápidamente el uso de aplicaciones en la nube, independientemente de si se administran o no. Evita que los datos confidenciales se filtren más allá del entorno del cliente. Como principales casos de uso indican los siguientes:
    - Encontrar servicios en la nube en uso y evaluar el riesgo
    - Proteger los datos en miles de servicios en la nube y sitios web
    - Detener la filtración de datos de servicios en la nube administrados y no administrados
    - Proteger la nube de las amenazas web
    - Control granular de dispositivos que acceden a los servicios en la nube

Netskope Security Cloud proporciona visibilidad y protección de datos y amenazas en tiempo real al acceder a servicios en la nube.

Los modos de trabajo del CASB de Netskope se puede observar en la imagen 50.

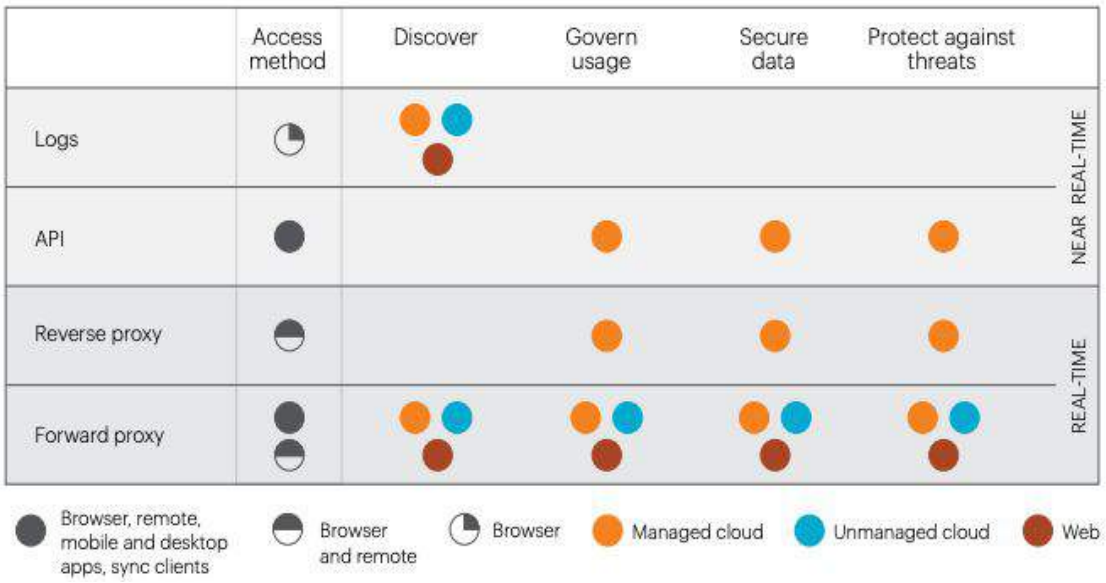

Imagen 50. Netskope - Cómo trabaja.

Algunas características de Netskope Security Cloud [126] son:

- Cifrado de datos estructurados: Cifrado de datos estructurados en reposo (at rest) o en tiempo real en servicios gestionados a través de un cifrado que conserva el formato origen con un cifrado AES-256, un KMS con certificación FIPS 140-2 de nivel 3 y la opción de utilizar el HSM on premise del cliente.

- Cifrado de datos estructurados a través de BYOK: Permite aprovechar las integraciones preconstruidas con las capacidades de que el cliente lleve su propia clave (BYOK) con cifrado AES-256, un KMS con certificación FIPS 140-2 Nivel 3 y la opción de usar el HSM on premise del cliente.

- Cifrado de datos no estructurados: Cifrado de datos no estructurados en reposo en los servicios gestionados o en en tiempo real con cifrado AES-256 y un KMS con certificación FIPS 140-2 Nivel 3 y a opción de usar el HSM on premise del cliente.

Permite integración con multitud de plataformas, software, etc. Algunos de ellos son Amazon Web Services (AWS), Google Cloud Platform, Microsoft Azure, ServiceNow, Slack, Salesforce, Splunk, etc.

Por último, destacar que se puede encontrar en el propio Marketplace de AWS [128].

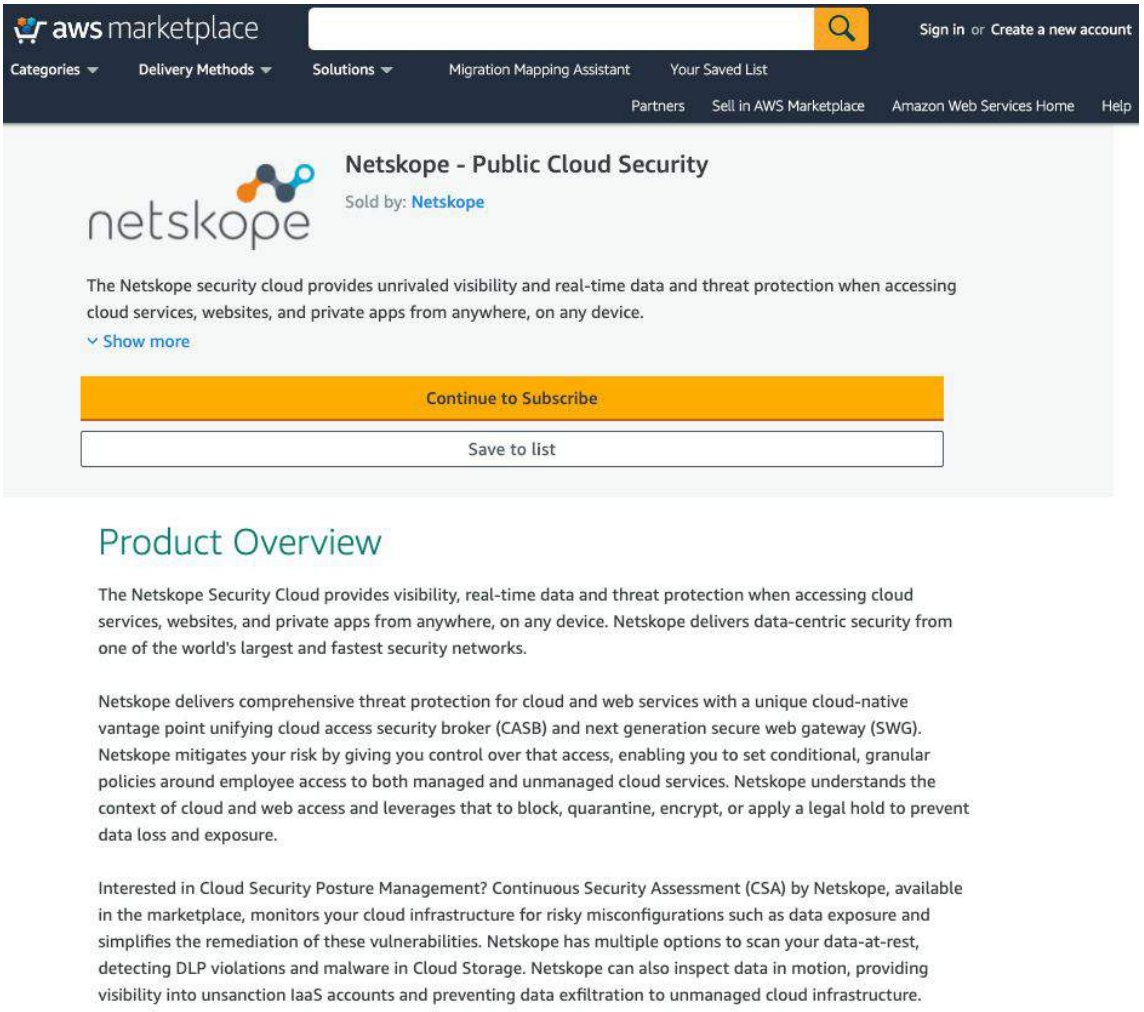

Imagen 51. Netskope - AWS Marketplace.

- McAfee MVISION Cloud: [129] [130] En enero de 2018, McAfee cerró la adquisición de Skyhigh Networks. McAfee MVISION Cloud fue uno de los primeros productos CASB en crear conciencia sobre el *shadow IT*.

  Como funcionalidades principales McAfee destaca:

  - Detectar: Visibilidad completa de los datos, el contexto y el comportamiento de los usuarios en todos los servicios de nube y dispositivos.
  - Proteger: Desarrollado de forma nativa en la nube y para la nube, MVISION Cloud protege de forma persistente la información confidencial donde quiera que se transmita, dentro o fuera de la nube.

- Corregir: Actuar en tiempo real sobre los servicios en la nube para corregir las infracciones de directivas y detener las amenazas a la seguridad.

En febrero de 2020, por tercer año consecutivo, McAfee fue nombrada "Elección de los clientes de 2020 Gartner Peer Insights para corredores de seguridad de acceso a la nube (CASB)" por su solución MVISION Cloud [131]. Es compatible con AWS, con Google Cloud y con Azure. [132]. Destacar que se encuentran en AWS Marketplace tanto McAfee MVISION Cloud for AWS [133] como Skyhigh Networks CASB for Custom Application [134].

En la imagen 52, se muestran algunos ejemplos de compatibilidad del CASB de McAfee:

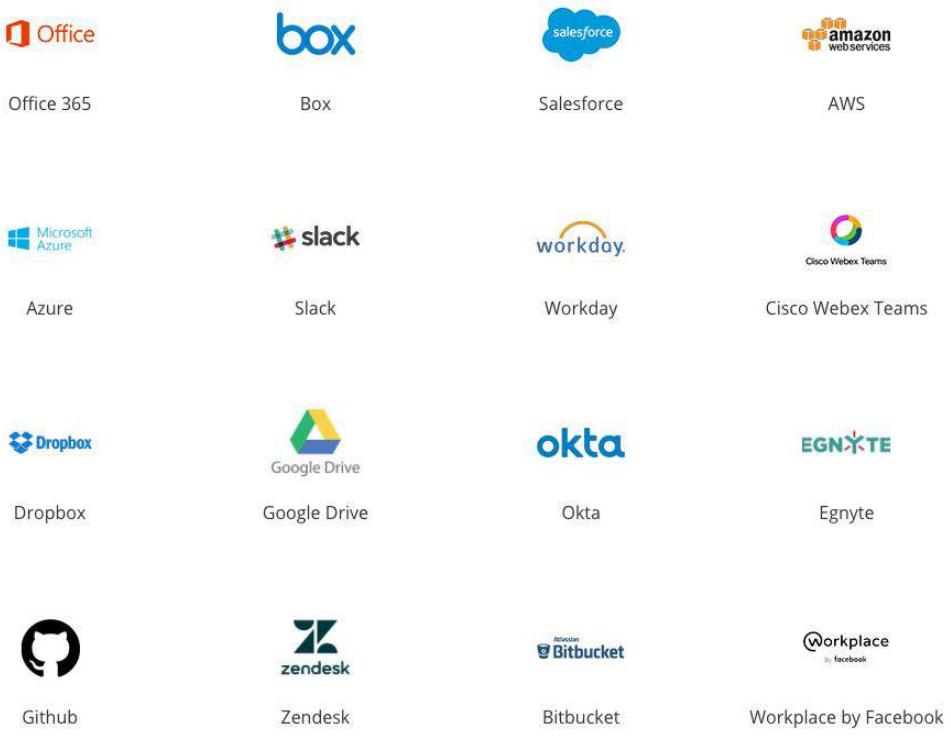

Imagen 52. McAfee compatibilidad.

Por último, aunque no ha resultado como un CASB líder en el estudio de Gartner [120], se va a introducir CipherCloud porque obtuvo muy buenos resultado, en dicho estudio, respecto al cifrado y tokenizado, tal y como se observa en la imagen 53:

Critical Capabilities	Bitglass	CipherCloud	Forcepoint	McAfee	Microsoft	Netskope	Palo Alto Networks	Proofpoint	Symantec
Data Loss Prevention	4.5	4.5	4.0	4.5	4.5	5.0	2.5	4.5	4.5
User and Entity Behavior Analytics	3.5	4.5	4.0	3.0	4.5	2.5	3.0	4.5	4.5
Adaptive Access Control	5.0	4.0	3.0	5.0	5.0	4.5	4.0	3.5	4.5
Cloud Security Posture Management	3.5	4.0	2.5	5.0	4.0	4.5	5.0	1.5	4.0
Encryption and Tokenization	5.0	5.0	2.0	4.0	3.0	4.0	1.5	1.0	4.0
Enterprise App/Service Integration	4.5	4.5	4.0	4.0	4.0	4.5	3.0	2.0	4.0

Source: Gartner (October 2019)

Imagen 53. Clasificación de productos/servicios en capacidades críticas.

- CipherCloud: [135][136] Más allá de los objetivos principales de un CASB ya comentados en este apartado, CipherCloud ha dedicado muchos esfuerzos al cifrado a nivel de campo y la tokenización de datos estructurados en servicios en la nube empresarial a través de un dispositivo local.

  Proporciona protección total de datos de extremo a extremo. El cifrado en reposo y al vuelo puede abordar los requisitos de seguridad más estrictos y, al mismo tiempo, proporcionar transparencia al usuario para las funciones típicas de las aplicaciones, como la búsqueda, la elaboración de informes, la clasificación, etc. En esta línea, se hace hincapié en la seguridad de los datos proporcionando una administración de claves completa, cifrado y tokenización, anonimización automatizada de la información personal y compatibilidad con HSM.

  También se integra con Azure, Google Cloud, AWS y varios productos SaaS más como Box, Office 365, Dropbox, etc.

  Un ejemplo de arquitectura híbrida propuesta por CipherCloud para que el cliente cumpla con las funcionalidades y los objetivos descritos en esta sección se muestra en la imagen 54:

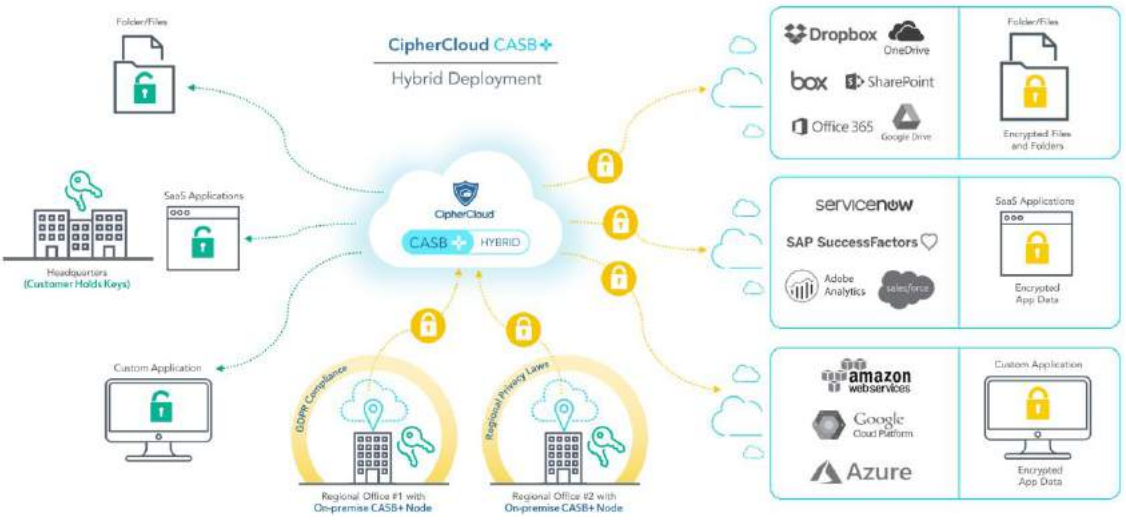

Imagen 54. Despliegue híbrido CipherCloud.

Se han introducido los cuatro CASB anteriores teniendo en cuenta el resultado del estudio de Gartner respecto a los casos de uso principales de estos productos, tal y como se muestra en la imagen 55:

Use Cases	Bitglass	CipherCloud	Forcepoint	McAfee	Microsoft	Netskope	Palo Alto Networks	Proofpoint	Symantec
Discovering Cloud Services; Assessing Cloud Risk	4.10	4.28	3.38	4.45	4.25	4.40	3.70	2.73	4.20
Identifying and Protecting Sensitive Information	4.33	4.35	3.48	4.38	4.40	4.35	3.25	3.43	4.35
Detecting and Mitigating Threats	4.15	4.28	3.28	4.33	4.40	4.05	3.60	3.20	4.33
Attaining Valuable Cloud Governance and Compliance	4.23	4.35	3.28	4.38	4.25	4.28	3.38	3.00	4.28

Source: Gartner (October 2019)

Imagen 55. Puntuación de los CASB por casos de uso.

No obstante, existen muchos más proveedores de CASB, algunos de ellos con soluciones de nicho que quizás en algunos casos se deberían tener en cuenta a la hora de elegir un CASB en una organización.

En tal caso, habría que hacer una exploración (*scouting*) teniendo en cuenta la necesidad de la entidad y, valorando las ventajas y las desventajas de cada solución, tomar una decisión adecuada en función del caso de uso que se pretenda cubrir.

5. Buenas prácticas de seguridad en entornos cloud

Antes de presentar una serie de buenas prácticas o recomendaciones de seguridad en entornos en la nube, se van a presentar algunos de los riesgos más importantes a los que se enfrenta cualquier organización a la hora de tener sus sistemas en los sistemas de los proveedores de nube.

Para ello, el siguiente listado está basado en el TOP 10 OWASP Cloud Security Risk.

OWASP (acrónimo de Open Web Application Security Project, en inglés 'Proyecto abierto de seguridad de aplicaciones web') es un proyecto de código abierto dedicado a determinar y combatir las causas que hacen que el software sea inseguro. [137]

La Fundación OWASP es un organismo sin ánimo de lucro que apoya y gestiona los proyectos e infraestructura de OWASP. La comunidad OWASP está formada por empresas, organizaciones educativas y particulares de todo mundo. Juntos constituyen una comunidad de seguridad informática que trabaja para crear artículos, metodologías, documentación, herramientas y tecnologías que se liberan y pueden ser usadas gratuitamente por cualquiera.

El top 10 de los riesgos de seguridad en la nube serían los siguientes, agrupados en categorías: [138]

- Responsabilidad y riesgo de los datos (Accountability and Data Risk): En esta categoría se cubren los riesgos de pérdida de los datos y lo relacionado con el tratamiento de los mismos. Al delegar los datos en las instalaciones del tercero, la organización que lo contrata debe saber bien qué está contratando y qué mecanismos de seguridad soporta el tercero para la protección de sus datos. Por ejemplo, cifrado, tokenizado, cómo pueden gestionarse las claves de cifrado, etc.

  También debe estar claro si cuentan con Plan de Recuperación de Desastres (Disaster Recovery Plan).

  Cómo es el borrado de los datos una vez finaliza la relación contractual. Qué aislamiento proporcionan entre clientes, si se comparte infraestructura o si es dedicada para cada cliente, etc.

- Federación de identidad del usuario (User Identity Federation): El principal riesgo de esta categoría es el robo de cuentas o credenciales que han sido comprometidas.

  Este caso lo ideal es revisar que opciones tiene el proveedor de integraciones con directorios activos *on premises* u on cloud. Qué opciones de delegación de autenticación soporta (por ejemplo, SAML 2.0). Si el proveedor soporta OAuth 2.0 para lo relacionado con la autorización y si cuenta con soluciones que requieran múltiples factores de autenticación (Multiple Factor Authentication - MFA).

Si cuenta con opciones para tener comunicaciones punto a punto cifradas como puede ser una solución de VPN. O incluso, si es posible conexiones dedicadas que no vayan a través de Internet.

- Cumplimiento normativo: Riesgo de no cumplir con la regulación. Como se ha visto las entidades financieras en particular deben cumplir con muchas regulaciones para no ser penalizadas por el organismo competente. Lo necesario como punto de partida para que un proveedor de servicios en la nube pueda prestar servicios a una entidad financiera es que cumple con el RGPD y con el PCI DSS en el caso de ser utilizado para cualquier cosa relacionada con datos de tarjetas.

  En este punto también es conveniente revisar con detalle la ubicación y desde dónde se va a realizar el tratamiento de los datos para no incumplir con la regulación.

- Continuidad de negocio (Business Continuity): Según el procedimiento que se tenga externalizado en un proveedor de servicios en la nube es posible que no se pueda permitir indisponibilidad del servicio en ningún momento. Por ello, deben estar perfectamente identificados y firmados los acuerdos de nivel de servicio (SLA, Service Level Agreement).

  Recomendable que el proveedor este certificado en la ISO 22301 [139] que hace referencia a lo relacionado con continuidad de negocio.

- Privacidad del usuario y uso secundario de los datos: En esta categoría principalmente existen dos riesgos, en primer lugar el acceso indebido a los datos por parte de algún empleado de la organización o por parte de algún empleado de la empresa que provee el servicio en la nube. En segundo lugar, el riesgo de usar los datos para un fin para el cual el cliente no ha dado su consentimiento explícito, requisito al que obliga el RGPD.

  En este punto es importante que se parta de la privacidad por diseño, se apoyen en rutinas de cifrado y *tokenizados* para que si se produce un acceso indebido los datos sean ilegibles.

  Por otro lado, para tratar de prevenir los acceso por parte de empleados que no deben tener acceso a los datos, es útil poner el foco en las opciones que tiene el proveedor para la gestión de usuarios haciendo hincapié en la autenticación, la autorización y el perfilado de los mismos.

- Integridad de los datos: Riesgo en la transmisión de datos hacia y desde proveedores en la nube con los sistemas *on premises* e incluso con otros proveedores cloud si ha optado por una solución multiproveedor. Para tratar de mitigar este riesgo se recomienda el cifrado en tránsito.

- Seguridad física y servicios multicliente (*multi tenant*): El ahorro de costes para el proveedor de servicios en la nube implica, en general, que los servidores y resto de infraestructura en la nube se usan en una configuración de arrendamiento múltiple.

  Esto significa que los recursos se comparten con más compañías. La seguridad en entornos de arrendamiento múltiple (*multi tenant*) se centra en la segregación lógica de recursos, más que en la física. El objetivo es evitar que otros inquilinos afecten la confidencialidad, integridad y disponibilidad de datos.

  Por ello, las medidas más importantes en esta categoría sería el cifrado de los datos incluso haciendo uso de claves propias almacenadas en algún otro proveedor o en sistemas *on premises* (BYOK - Bring Your Own Key) e incluso solicitar al proveedor instancias dedicadas para almacenar según que datos.

  En esta categoría también destacar la seguridad física del proveedor, ya que un acceso no autorizado a sus instalaciones podría ser catastrófico.

- Análisis de incidentes y análisis forense: Riesgo de que el proveedor no realice una buena monitorización de los servicios y no genere unos logs que puedan ser de utilidad en caso de un incidente de seguridad. También es importante tener detallado el acceso a dichos logs, tanto en tiempo como en forma.

- Seguridad de la infraestructura: De la misma manera que cuando se define una topología de red o un diseño de arquitectura en sistemas *on premises* existe un riesgo de no realizarlo correctamente y dejar expuestos servidores o cualquier otro punto del sistema que posibilite un ataque, una fuga de información, etc.

  Por ello, es recomendable realizar una separación de deberes desde la planificación, *hardening*[10] y actualización de todos los sistemas (parches de seguridad incluido), hasta realizar auditorías periódicas que verifiquen que todo es correcto.

- Exposición de entornos no productivos: Los riesgos y medidas que los mitiguen se tienen que tener en cuenta en todos los ciclos de vida del desarrollo, de los datos, de los despliegues, etc. Si no se hace correctamente existe un riesgo de diseñar sistemas de entornos previos que sean más laxos en lo que a seguridad se refiere que los productivos. Por ello, además de que sean prácticamente iguales, se debería trabajar con el principio de privacidad por diseño y destacar que en los sistemas no productivos nunca debería haber datos de producción.

[10] Asegurar un sistema reduciendo sus vulnerabilidades o agujeros de seguridad

A continuación se recuerdan las imágenes del segundo apartado que reflejaban los modelos de seguridad compartida de los proveedores de servicios en la nube.

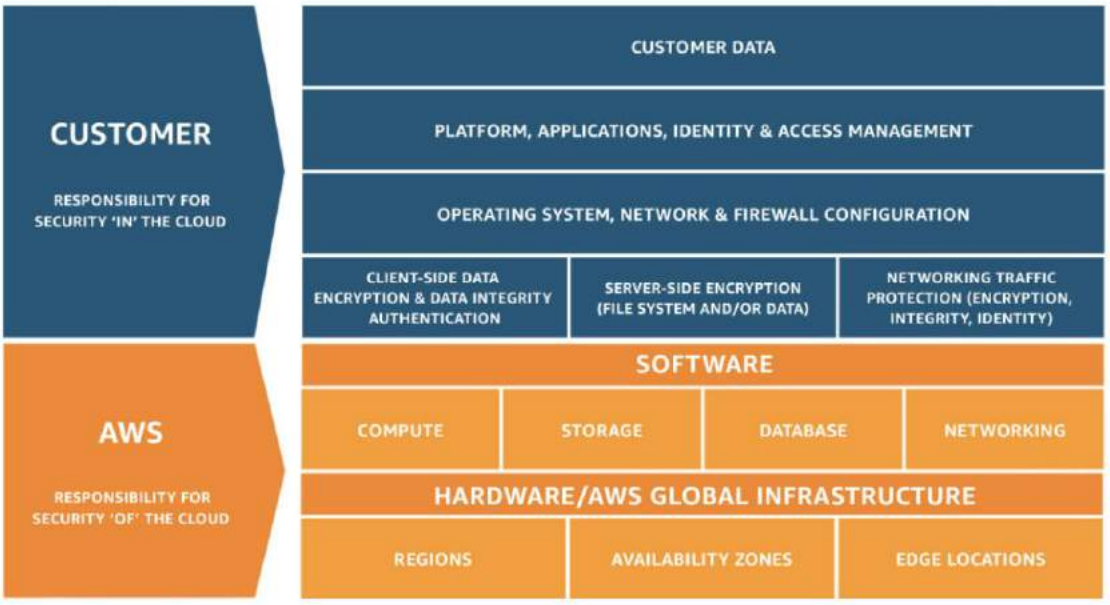

Imagen 5. Modelo de responsabilidad compartida de AWS.

Imagen 6. Modelo de responsabilidad compartida de Microsoft Azure.

El proveedor de servicio en la nube como AWS o Azure, es responsable de la seguridad de la nube y de la infraestructura subyacente de la misma, y los clientes son responsables de la seguridad en la nube, para cualquier cosa que pongan, y construyan encima de la infraestructura del proveedor.

Los conceptos tratados en este apartado son extrapolables a cualquier proveedor de servicios cloud tal y como se expuso en el apartado 2.6. La única diferencia será la nomenclatura del propio proveedor de servicios, pero el concepto y la esencia de la idea es la misma.

En este caso se van enfocar al proveedor AWS por ser el líder del sector y por afinidad con el entorno.

En la nube, hay una serie de principios que pueden ayudar a fortalecer la seguridad de los sistemas: [140] [141]

- Implementar una fuerte base de identidad: Implementar el principio del menor privilegio y cumplir con la separación de funciones añadiendo la autorización apropiada para cada interacción con los recursos de la nube. Centralizar la gestión de privilegios y reducir o incluso eliminar la dependencia de las credenciales a largo plazo.

- Habilitar la trazabilidad: Monitorizar, alertar y auditar acciones y cambios en el entorno en tiempo real. Integrar registros y métricas con sistemas para responder y tomar medidas automáticamente.

- Aplicar la seguridad en todas las capas: En lugar de centrarse en la protección de la capa exterior, aplicar un enfoque de defensa en profundidad con otros controles de seguridad en todas las capas.

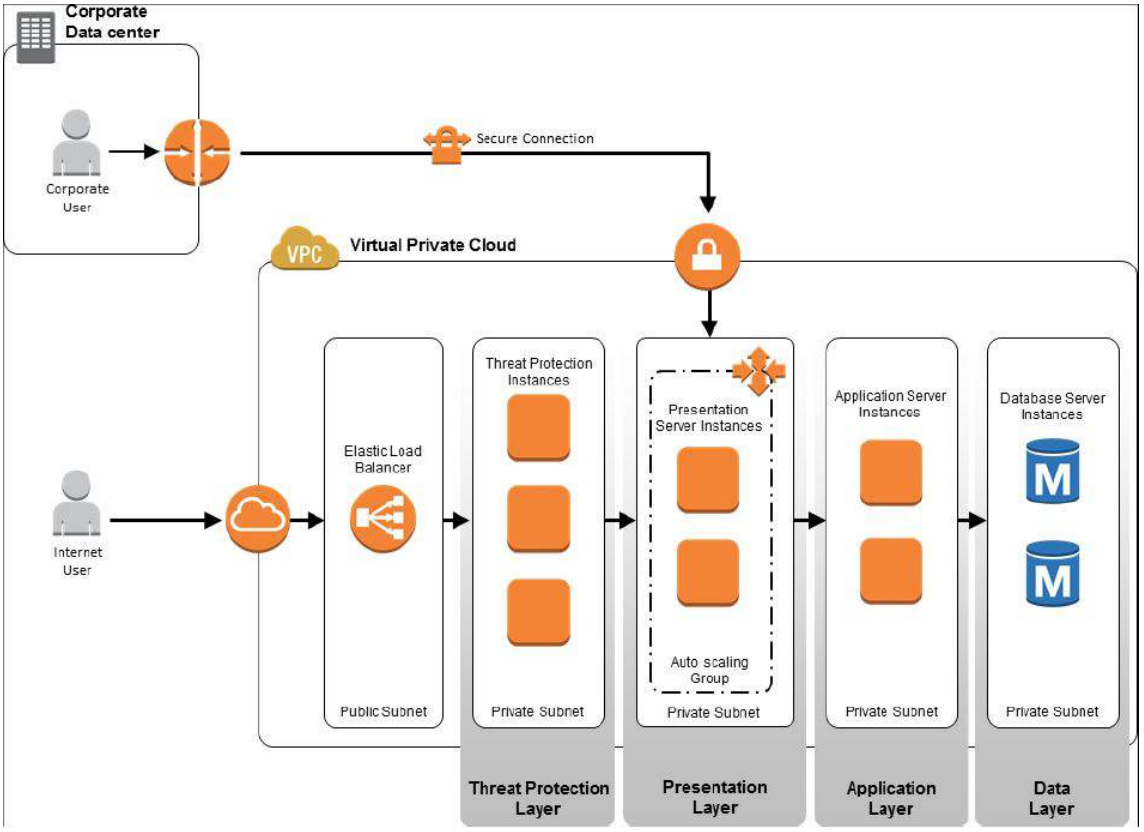

Imagen 56. Defensa implementando seguridad en todas las capas.

- Automatizar las mejores prácticas de seguridad: Los mecanismos de seguridad automatizados basados en software mejoran su capacidad para escalar de forma segura con mayor rapidez. Crear arquitecturas seguras, incluyendo la implementación de controles que se definen y gestionan como código en plantillas controladas por versiones ayuda a evitar en gran medida los fallos humanos.

- Proteger los datos en tránsito y en reposo: Clasificar los datos en niveles de sensibilidad y utilizar mecanismos como el cifrado y el control de acceso.

- Mantener alejada a la gente de los datos: Crear mecanismos y herramientas para reducir o eliminar la necesidad de acceso directo o procesamiento manual de los datos. Esto reduce el riesgo de pérdida o modificación, así como el error humano al manejar datos sensibles.

- Estar preparado para los incidentes de seguridad: Ponerse en el peor caso teniendo un proceso de gestión de incidentes que se ajuste a los requisitos de la organización. Se deben ejecutar simulaciones de respuesta ante incidentes y utilizar procesos automatizados para aumentar la velocidad de detección, investigación y recuperación.

Las consideraciones se van a dividir en cinco áreas [140][141]:

1. Gestión de accesos e identidades
2. Controles de detección
3. Protección de la infraestructura
4. Protección de los datos
5. Respuesta a incidentes

5.1 Gestión de accesos e identidades

Parte fundamental de un programa de seguridad, ya debe garantizar que sólo los usuarios autorizados y autenticados puedan acceder a sus recursos, y sólo de la manera que se haya permitido. Para ello, se deben definir los usuarios, los grupos, etc. que tienen acceso, elaborar políticas que se ajusten a lo definido y aplicar una gestión de credenciales adecuada. Estos elementos de gestión de privilegios constituyen el núcleo de la autenticación y la autorización.

En AWS, IAM (2.5.4.1) proporciona un control de acceso seguro al entorno de AWS para interactuar con los recursos de AWS de forma controlada.

Algunas prácticas recomendadas para hacer uso de este servicio correctamente son:

- Eliminar las claves de acceso del usuario root: Una cuenta de root es una cuenta que tiene no restricciones de acceso a todos los recursos de AWS en la cuenta. Se recomienda borrar las claves de acceso, las identificaciones de las claves de acceso y la clave secreta de acceso para el root para que no puedan ser mal utilizadas. En su lugar, se debe crear un usuario con los permisos deseados y llevar a cabo las tareas con este usuario.

  Por lo tanto, quedaría prohibido el uso del usuario root de las cuentas de AWS, a excepción de las operativas que no pueden ser realizadas de otra forma. También se debe prohibir la generación de claves de pares (access key, secret key) para este usuario.

- Configurar el MFA: Añadir una capa adicional de seguridad configurando el MFA para todos los usuarios y especialmente para aquellos que tienen acceso a recursos críticos o sensibles.

- Usar roles en lugar de usuarios sobre todo para aquellos que sean temporales. Los roles son gestionados por AWS y las credenciales para los roles son administradas por AWS. Un ejemplo muy claro del uso de roles es el proveer un acceso temporal a un auditor. El usuario del auditor estará autorizado para asumir el *role* auditor dado de alta en AWS con los permisos estrictamente necesarios y con la temporalidad determinada. Así se evita dar credenciales a un usuario y que se queden en el olvido.

  Otro caso especialmente importante para el uso de roles es el caso de llamadas entre recursos en la propia nube, se hará uso de los roles antes que de la creación de un usuario en IAM. Para ello, el rol creado será asignado al servicio consumidor siempre bajo la política de mínimo privilegio posible.

- Roles con mínimo privilegio posible: Una rol de IAM es asumido por un usuario u otro servicio de AWS y se le asignan credenciales temporales con un alcance limitado de permisos.

Como se ha indicado, a la hora de generar roles IAM, para el perfilado de permisos que asumirán los usuarios, siempre usará la política de los menos permisos posibles para poder realizar su función.

La organización debe definir las funciones y responsabilidades de los usuarios y aplicaciones que interactúan con los servicios de AWS e implementar una autorización detallada para el cumplimiento de estas funciones.

- Uso de grupos: Los usuarios IAM de AWS, siempre sea posible, deben de estar contenidos dentro de grupos organizativos. Se recomienda asignar los usuarios a grupos y conceder los permisos sobre grupos en lugar de sobre los usuarios directamente.

- Delegación de autenticación en el directorio de usuarios corporativo: Hacer uso de identidades existentes utilizando la federación (a través de SAML 2.0 o de identidades web) en el proveedor de identidad de la organización. El uso de la federación reduce la necesidad de crear usuarios en IAM, a la vez que aprovecha las identidades, las credenciales y el acceso basado en funciones existentes que ya podría haber establecido en la organización.

  Por lo tanto, se deberá delegar siempre que sea posible la gestión de cuentas de usuario en un Directorio Activo/LDAP con el fin de gestionar de manera más efectiva las altas y bajas de las cuentas de usuario de manera centralizada.

- Política de contraseñas: Además del MFA, se deben aplicar las políticas de contraseñas adecuadas para cumplir con una autenticación robusta. La política de contraseñas en la cuenta de AWS debe requerir una longitud y complejidad mínimas para las contraseñas asociadas a los usuarios de IAM.

  También debe establecer una política de rotación obligatoria que exija a los usuarios de IAM que cambien sus contraseñas a intervalos regulares.

  Por ejemplo, una política de contraseñas podría ser la siguiente:

  - La contraseña debe de estar formada por un mínimo de 10 caracteres.
  - La contraseña debe de contener letras mayúsculas y minúsculas, números y caracteres especiales.
  - La contraseña debe de ser cambiada con una periodicidad mínima de 30 días.
  - La contraseña debe ser diferente a las 10 anteriores que se hayan utilizado.

- Usuarios inactivos o innecesarios: No pueden existir usuarios IAM inactivos en las cuentas de AWS. Cualquier usuario con más de 3

meses sin uso debe ser deshabilitado de forma automática. De igual manera, aquellos usuarios que no sean necesarios para el funcionamiento del servicio deberán ser eliminados.

- Almacenamiento de credenciales: Prohibido el almacenamiento de contraseñas dentro del propio código del aplicativo. En caso de que la solución no haga uso ya de métodos de almacenamiento de claves seguros (como es el caso de los secretos en contenedores Docker), estas claves deberán alojarse en el servicio AWS Secrets Manager, que protege las claves cifradas o, en su defecto, el AWS Parameter Store usando, en todo caso, el cifrado con KMS.

- Organización centralizada de las cuentas de una empresa: Las organizaciones de AWS deben utilizarse para gestionar de forma centralizada las cuentas de AWS. AWS Organizations (apartado 2.5) permite agrupar las cuentas en unidades organizativas (OU). Las políticas de control de servicio (SCP) se pueden utilizar para aplicar políticas de forma centralizada sobre los servicios de AWS a través de múltiples cuentas de AWS.

La imagen 57 muestra que se han realizado unos controles mínimos en IAM sobre la cuenta de AWS.

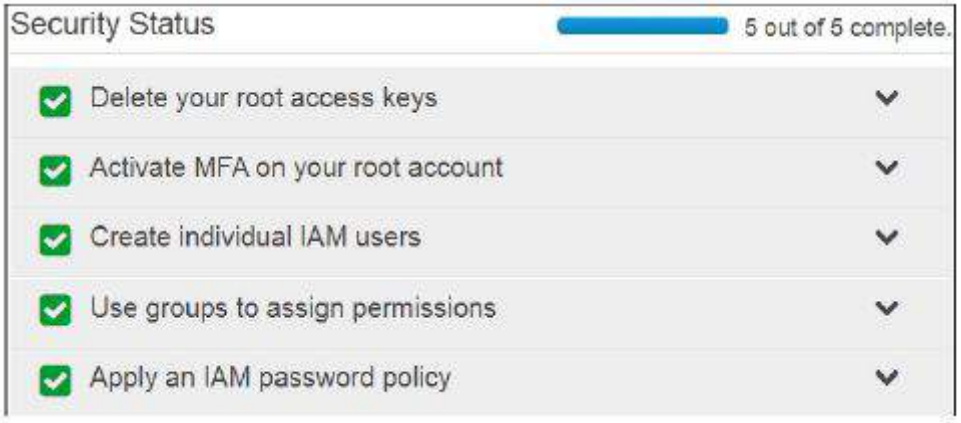

Imagen 57. Configuración inicial IAM AWS.

Por último, en la imagen 58 se puede ver cómo trabaja IAM. Dado que es una “base de datos de usuarios” la integración con el resto de servicios es total además de ser global.

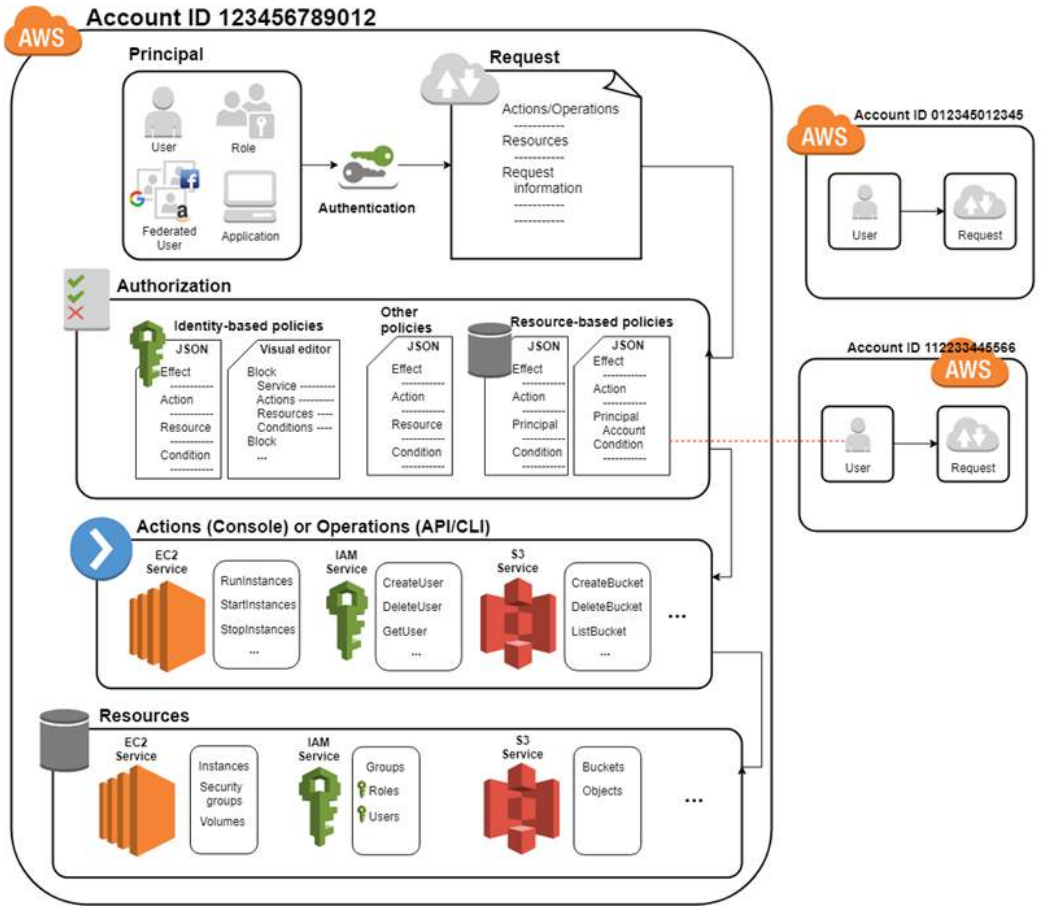

Imagen 58. Cómo trabaja IAM AWS.

5.2 Controles de detección

Realizar una configuración adecuada de los distintos sistemas de identificación de amenazas a distintos niveles puede ser muy útil para identificar amenazas o incidentes de seguridad (casi) en tiempo real. Además, dichos sistemas pueden ser muy beneficiosos desde el punto de visto del gobierno de los sistemas e incluso desde la visión de cumplimiento normativo.

Los equipos de operaciones de seguridad se basan en la recopilación de logs y en el uso de herramientas de búsqueda de patrones de comportamiento para descubrir posibles acontecimientos de interés, que pueden indicar una actividad no autorizada o un cambio no intencionado.

En AWS, hay una serie de enfoques a considerar cuando se abordan este tipo de controles:

- Cómo capturar y analizar los logs

- Cómo integrar los controles de auditoría con las notificaciones y los flujos de trabajo (workflows)

Algunas de las mejores prácticas en este sentido son las siguientes:

- Registrar todo: AWS proporciona AWS CloudTrail (2.5.4.6) que registra todas las actividades de la API para la cuenta del cliente de AWS. Da capacidades para recoger, almacenar y registrar cualquier proceso de la infraestructura como los VPC Flow Logs, los servicios de AWS, etc. Se recomienda utilizar los logs de CloudWatch para procesar todos los logs, y S3 para almacenarlos.

  Por lo tanto, se debe considerar como obligatorio que CloudTrail este activo en todas las regiones de todas las cuentas que utilice la empresa en AWS. Adicionalmente habrá que activar el check de “registrar las acciones globales” para registrar también las acciones que afectan a todas las regiones.

  Todos los logs de CloudTrail deben de centralizarse en un repositorio único con el fin de consolidar y poder explotar esta información. Esta ubicación debe estar aislada de otros servicios y aplicaciones en una cuenta de AWS dedicada a la supervisión y la auditoría.

  Cloudtrail debe de tener activa la opción de “habilitar checksum de verificación”, con el fin de garantizar la integridad del mismo.

  Se hará uso de los servicios CloudWatch y CloudTrail para trazar los accesos de los distintos usuarios (tanto nominales como no nominales) a los distintos recursos de AWS.

- Habilitar AWS CloudWatch: Ya se indica en el anterior control de seguridad, pero se debe asegurar que se hace uso de CloudWatch con el objetivo de monitorizar todos los recursos en la nube, incluyendo datos, servicios, servidores y otros servicios de AWS como son los balanceadores de carga de red y de aplicación, grupos de auto escalado, etc.

  Se deben utilizar métricas, dashboards, gráficos y alarmas para crear soluciones preventivas para los incidentes de seguridad que puedan surgir.

  Para la detección inteligente de amenazas, se puede utilizar un servicio como GuardDuty (2.5.4.2) de Amazon para monitorizar continuamente los eventos de AWS CloudTrail, los registros de flujo de Amazon VPC y los registros de DNS.

- Cumplimiento continuo: Utilizar AWS Trusted Advisor para comprobar proactivamente cuestiones relacionadas con la configuración de seguridad de sus recursos de AWS. Este servicio avisa al cliente si considera que tiene alguna configuración incorrecta a nivel de seguridad.

  Usar AWS Config para notificar al usuario en tiempo real sobre los cambios en la configuración predefinida de recursos. Ya se indicó anteriormente, pero AWS Config ofrece al cliente una vista detallada de la configuración de los recursos de su cuenta de AWS. Esto incluye cómo se relacionan entre sí y cómo fueron configurados.

- Automatizar el cumplimiento y la auditoría: Se recomienda usar combinaciones de AWS CloudTrail, AWS SNS, AWS Lambda, AWS Config Rules, CloudWatch logs, alertas de CloudWatch, Amazon Inspector, etc. para automatizar el cumplimiento y la auditoría de todos los recursos desplegados en la cuenta de AWS.

Por resumir, para configurar y aplicar las recomendaciones expuestas los servicios de AWS que van a ayudar al cliente son:

AWS CloudTrail: Soporta la captura de actividades y proporciona detalles sobre las llamadas API realizadas en la cuenta de AWS.

Amazon GuardDuty: Servicio de detección de amenazas administrado por AWS que monitoriza continuamente el comportamiento malicioso o no autorizado.

AWS Config: Proporciona un inventario de recursos de AWS, un historial de configuración y notificaciones de cambios de configuración para permitir la seguridad y el gobierno de la infraestructura.

Amazon CloudWatch Logs: permite centralizar los logs en flujos, integrándose de forma nativa con servicios como Amazon VPC Flow Logs y CloudTrail.

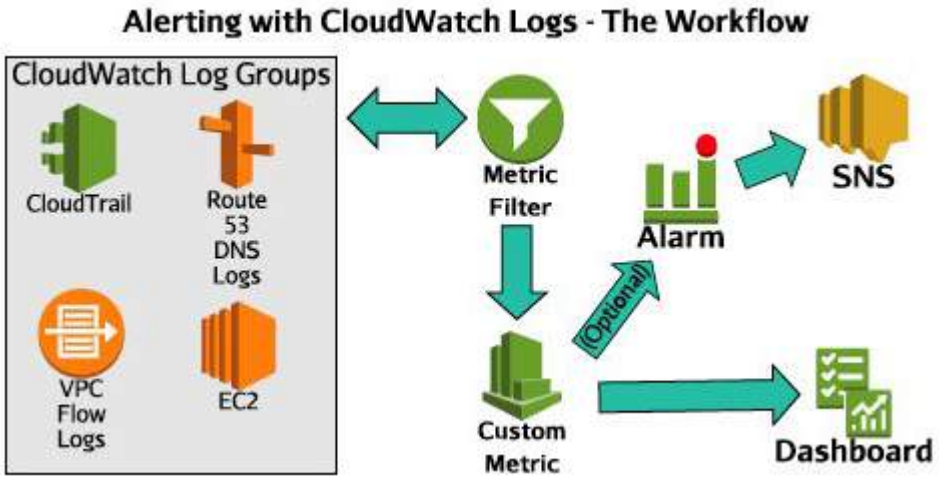

Imagen 37. Flujo CloudWatch Logs y Events.

Amazon S3 - Amazon Glacier: pueden utilizarse para centralizar el almacenamiento y el archivo a largo plazo de los logs, especialmente Glacier por su bajo coste.

Amazon Athena: puede utilizarse para analizar logs, como los de CloudTrail, para ayudar a identificar tendencias y aislar aún más la actividad por atributo, como la dirección IP de la fuente o el usuario.

CloudWatch Events: Provee integración de los controles de auditoría con los sistemas de notificación. Permite enrutar los eventos a un motor de reglas. Las reglas examinan los eventos entrantes, analizan los valores entrantes y dirigen el evento a cualquier número de objetivos, tales como correo electrónico, dispositivos móviles, etc. Amazon CloudWatch y CloudWatch Logs deben estar habilitados para facilitar la recolección de eventos y el enrutamiento con CloudWatch Events.

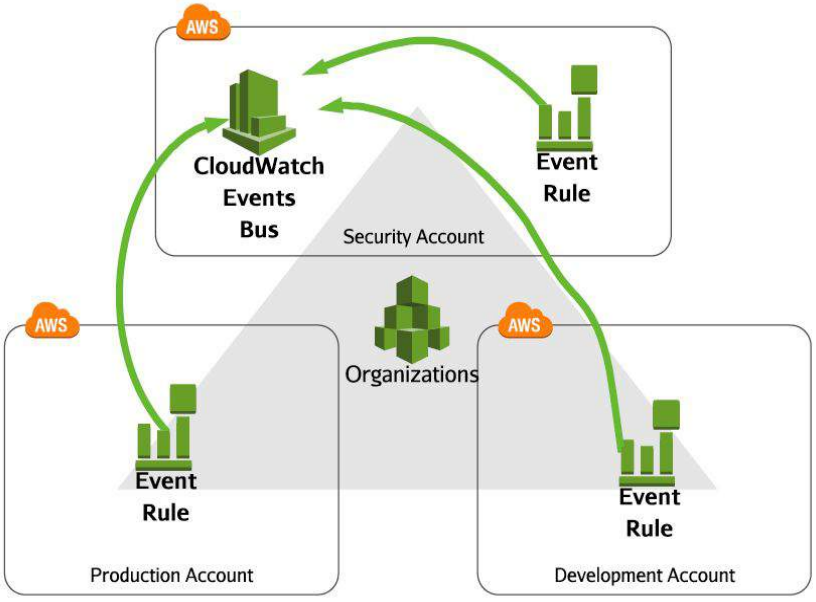

Imagen 38. Cloudwatch Bus.

Amazon Inspector: monitoriza los CVE, comprueba políticas de hardening, comportamientos de ejecución y mejores prácticas.

De la mayoría de los servicios anteriores se han dado más detalles en el apartado correspondiente de la segunda sección de este trabajo.

Se proporcionan un par de ejemplos de diagramas de arquitecturas para la implementación de estos servicios:

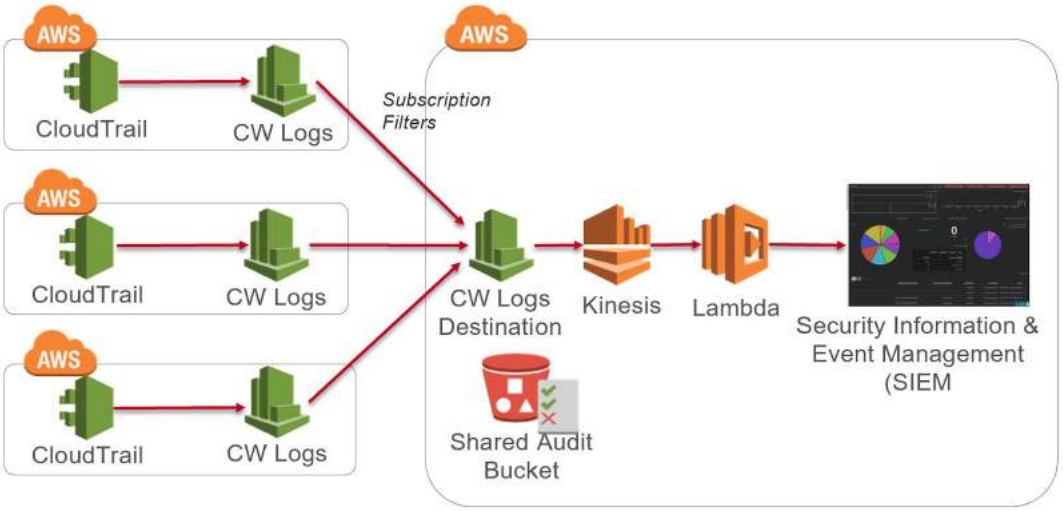

Imagen 59. Análisis de eventos. [142]

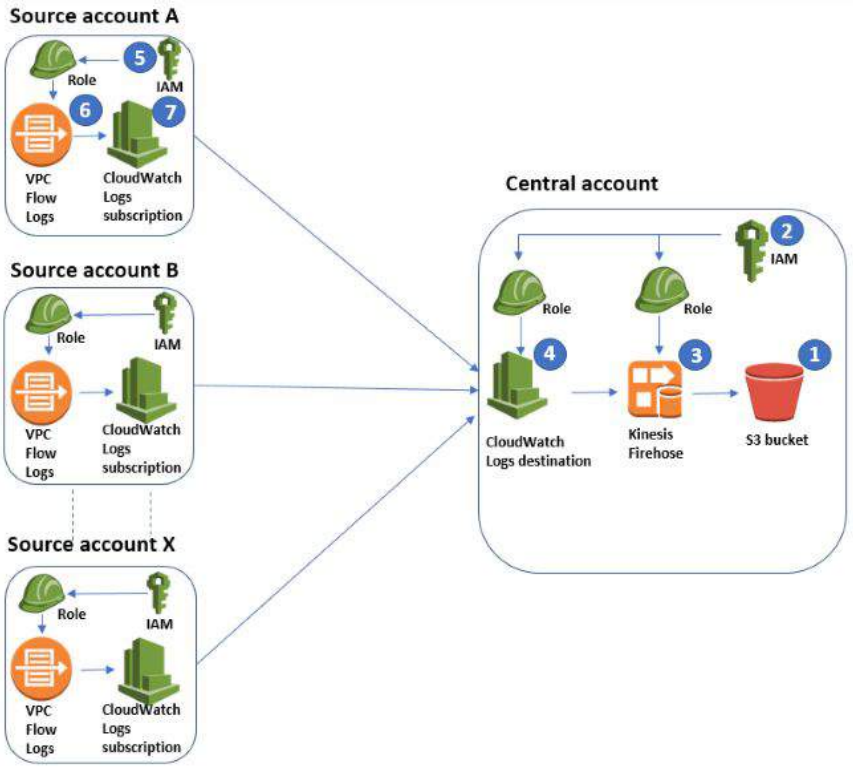

Imagen 60. Análisis de datos flujo centralizado. [143]

5.3 Protección de la infraestructura

La protección de la infraestructura es una parte esencial en un programa de seguridad de la información. Es vital asegurar que los sistemas y servicios estén protegidos contra el acceso no intencionado, no autorizado y contra posibles vulnerabilidades.

El diseño y la gestión de la topología de red forma la base de cómo se proporciona el aislamiento y los límites de los recursos dentro del entorno. Debido a que los recursos colocados dentro del entorno pueden heredar las propiedades de seguridad de la red subyacente, es fundamental establecer un diseño de red apropiado que asegure que sólo se permiten las rutas de red deseadas. Esto se puede hacer aprovechando las múltiples capas de protección para proporcionar redundancia a los controles y mitigar el impacto de una mala configuración en una sola capa que podría derivar en un acceso inadecuado.

Cuando se define la topología de la red, hay que tener en cuenta qué componentes del sistema deben ser públicos. Además, cuando se diseña la conectividad, se debe considerar si se necesita conectividad entre el centro de datos *on premise* y el proveedor cloud.

En el caso de AWS, se deben aplicar las configuraciones apropiadas a la nube privada virtual (VPC), a las subredes, a las tablas de enrutamiento, a las listas de control de acceso a la red (NACL), a las puertas de enlace (*gateways*) y a los grupos de seguridad para lograr el enrutamiento de red correcto, así como la protección a nivel de host.

Cuando se diseñan las reglas NACL, hay que considerar que es un cortafuegos sin estado (*stateless*) y, por lo tanto, tanto las reglas de salida como las de entrada tienen que ser definidas para permitir el tráfico entrante y saliente si así se requiere. Hay que adoptar un enfoque de mínimos privilegios por defecto como, por ejemplo, abrir únicamente los puertos necesarios para la comunicación.

Cuando una máquina se lanza dentro de un VPC, por ejemplo una instancia EC2, tiene su propio grupo de seguridad que es como un *firewall* con estado *(statefull)*. Este cortafuegos está fuera de la capa del sistema operativo y puede ser usado para definir mediante reglas el tráfico permitido.

También se pueden definir relaciones entre grupos de seguridad. Por ejemplo, las instancias dentro de un grupo de seguridad de nivel de base de datos sólo aceptan el tráfico de las instancias dentro del nivel de aplicación y, a su vez, las instancias de la aplicación sólo aceptan peticiones del servidor web. Esto viene representado en la imagen 61, relacionado con lo mostrado en la imagen 56 - defensa implementando seguridad en todas las capas.

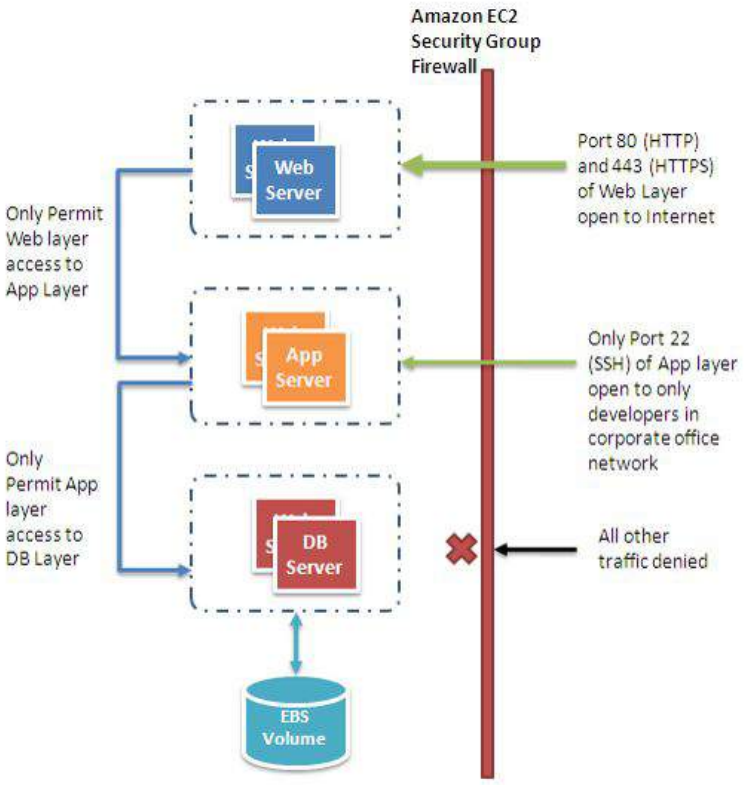

Imagen 61. Grupos de seguridad en AWS. [144]

Se deben automatizar los despliegues y el mantenimiento de la infraestructura, y eliminar el acceso de los equipos de operaciones para reducir el riesgo operativo.

Algunos controles específicos para la protección de la infraestructura son los siguientes:

Respecto a las VPC (Virtual Private Cloud) de AWS:

- Crear una VPC personalizada: Se recomienda crear una VPC propia y no utilizar la VPC por defecto, ya que tiene una configuración predeterminada para permitir tráfico de entrada y salida.
- Control de acceso: Usar IAM para controlar el acceso a la VPC y a los recursos que son parte de la VPC. Se puede crear un control de acceso de grano fino utilizando IAM para los recursos en las VPC.
- Monitorizar la actividad de la VPC: Como se ha visto en apartados anteriores de esta sección, es una buena práctica el crear VPC Flow Logs para monitorizar el flujo de todo el tráfico IP en la VPC.
- Utilizar un NAT (Network Address Translation): Los recursos que no necesitan estar expuestos a Internet deben mantenerse en una subred privada. En el caso que dichos recursos necesiten salida a Internet para

actualizaciones o actualizaciones de seguridad, esta salida deberá realizarse a través de un NAT Gateway situado en la subred pública.

- Subredes privadas sin IP pública: En ningún caso deben de existir instancias EC2 dentro de subredes privadas de una VPC que contengan IP con direccionamiento público. De igual manera, en la tabla de rutas de la red privada no podrá definirse el Internet Gateway como objetivo.

- Tablas de rutas en subredes: Todas las subredes, tanto públicas como privadas, contarán con su tabla de rutas propia. En ningún momento las subredes deberán heredar la tabla de rutas de la VPC creada por defecto.

- Aislamiento entre entornos: crear VPC separadas para los entornos de desarrollo, pruebas y producción.

- Uso de Direct Connect (DX): Si se requiere de conexión continua con el CPD *on premise* del cliente y siempre que la infraestructura lo permita, se deberá establecer una conexión Direct Connect con el CPD a través del cual deberá circular todo el tráfico entre AWS y el CPD.

Respecto a los servidores - instancias EC2:

- Parcheado de las máquinas: Se debe mantener actualizado el SO en servicios IaaS cuya responsabilidad cae del lado del cliente. Se aconseja el uso de servicios de detección de vulnerabilidades como AWS Inspector el cual se basa en estándares de seguridad de mercado.

- Copias de seguridad y recuperación: Se recomienda utilizar las *snapshots* para hacer copias de seguridad de todos los datos y configuración almacenada en los servidores de manera periódica.

  Por otra parte, para automatizar la creación de servidores, se recomienda crear las máquinas de la organización a través de una AMI (Amazon Machine Image) que haya sido revisada y esté actualizada con las últimas recomendaciones y parches de seguridad. Esto proporciona poder crear máquinas basadas todas en una misma imagen con la configuración correcta y, por otro lado, ante un incidente de seguridad poder levantar la misma máquina en minutos.

- Utilizar roles IAM: Se ha comentado anteriormente, pero se recalca la utilización de roles de IAM en vez de usuarios de IAM. Por ejemplo, se asigna un rol a una instancia de EC2 para acceder a otros servicios de AWS como S3. De esta forma, las credenciales del rol no se almacenarán en la instancia de EC2 como en el caso de un usuario de IAM. El funcionamiento de asumir un rol por una instancia EC2 para obtener unos objetos de un *bucket* de S3 se muestra en la imagen 62.

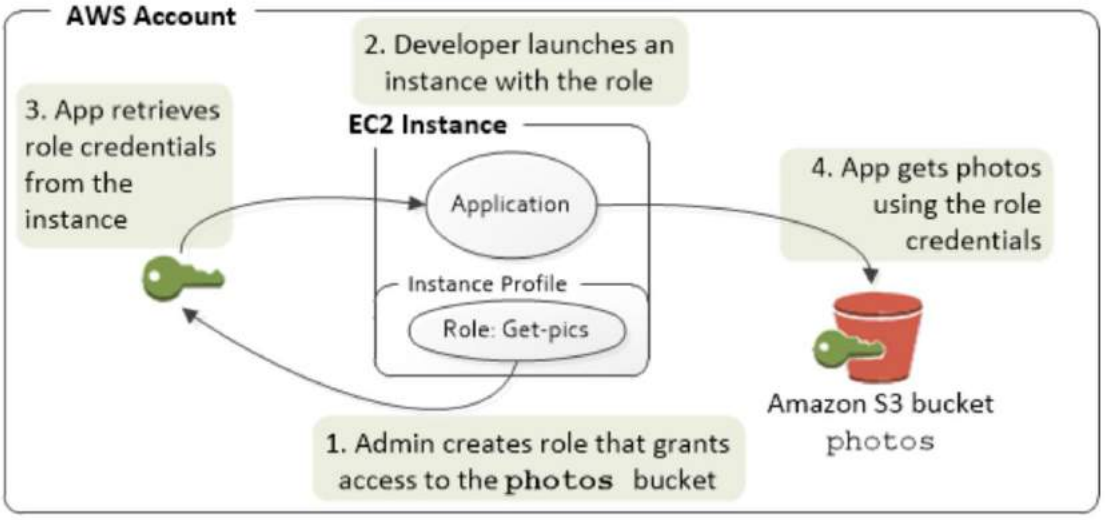

Imagen 62. Rol IAM para instancia EC2. [145]

- Utilizar balanceadores de carga (Elastic Load Balancer - ELB): Se deben poner cuando corresponda las instancias EC2 detrás del balanceador para proteger a las instancias de recibir tráfico directamente de Internet y recibir tráfico sólo del balanceador aplicando correctamente los Security Groups de manera análoga a como se ha visto en la imagen 61.

- Configuración de los Security Groups: En ningún caso deben existir grupos de seguridad de AWS expuestos a Internet (que permitan el acceso desde cualquier CIDR ó 0.0.0.0/0) salvo en el caso de servicios públicos que se presten abiertamente en Internet como pudiera ser una página o servicio web. En dicho caso, sólo estarán abiertos los puertos HTTP (80) y HTTPS (443).

- Web Application Firewall (WAF): En caso de que se publiquen servicios web se debe hacer uso del servicio WAF de AWS.

- Denegación de servicio distribuida (DDoS): Utilizar AWS Shield en su versión normal o avanzada para prevenir ataques de denegación de servicio.

- Acceso seguro: En el caso de que se necesite acceso a los servidores, se recomienda utilizar el Servicio de Token Seguro (STS) para conceder credenciales temporales en lugar de usar las credenciales de usuario de IAM.

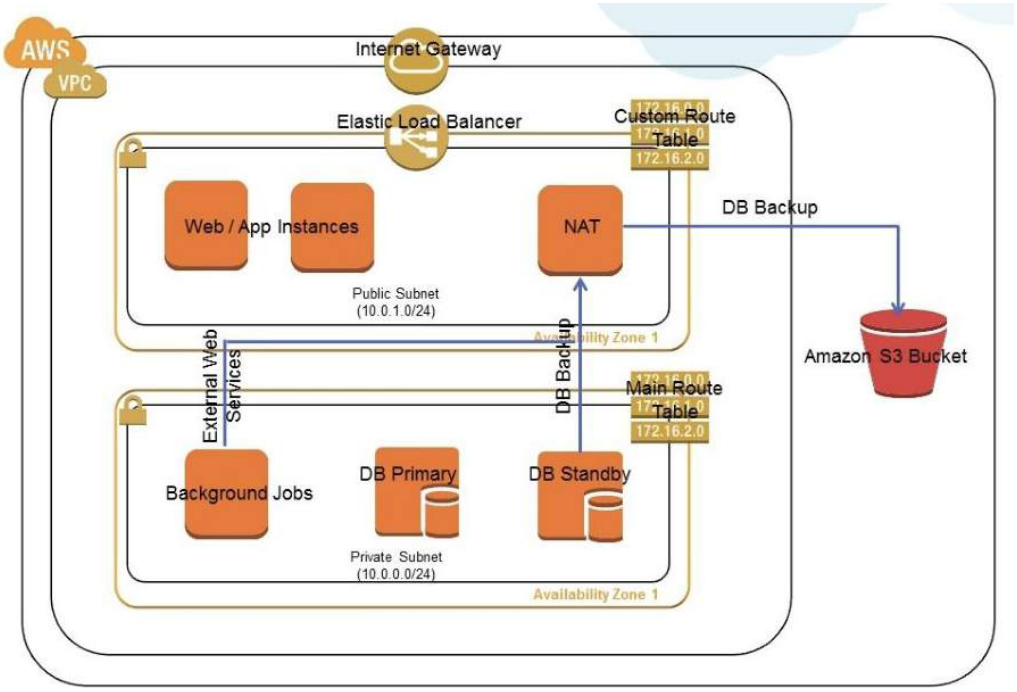

Imagen 63. Ejemplo arquitectura NAT, balanceadores, IGW aplicación web.

Respecto a las aplicaciones desplegadas en los servidores, además del uso del WAF, de Amazon Inspector, de los grupos de seguridad, listas de control de acceso, etc. se recomienda realizar test de *pentesting.* AWS permite realizar pruebas de vulnerabilidades y *pentesting* para todas las instancias de EC2, pero se debe avisar a AWS con anterioridad.

Para concluir el apartado, los servicios que pone AWS a disposición del cliente para configurar y aplicar las recomendaciones expuestas son los siguientes:

Amazon VPC Security Groups: Proporcionan un cortafuegos con estado por cada host, permitiendo especificar las reglas de tráfico y definir las relaciones con otros grupos de seguridad.

AWS Shield: Servicio administrado de protección frente a la denegación de servicio distribuido (DDoS).

AWS WAF: Cortafuegos de aplicaciones web que ayuda a proteger las aplicaciones web de exploits web comunes que podrían afectar a la disponibilidad de las aplicaciones, comprometer la seguridad o consumir recursos excesivos.

AWS Firewall Manager: Servicio que facilita la configuración y gestión centralizada de las reglas de AWS WAF en todas sus cuentas y aplicaciones.

AWS VPN: Permite establecer una conexión punto a punto privada y cifrada a través de Internet para conectar el centro de datos *on premises* a la VPC en AWS.

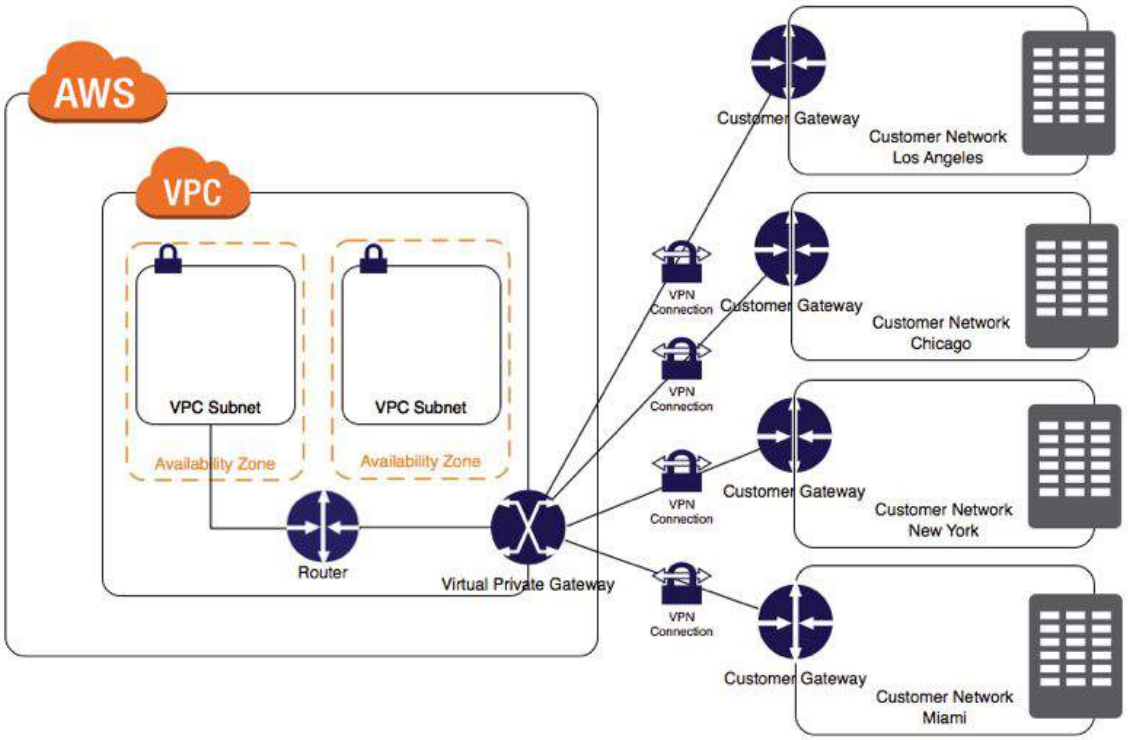

Imagen 64. Múltiples VPN.

AWS Direct Connect: Permite establecer conectividad propia y directa desde el centro de datos *on premises* a la VPC en AWS.

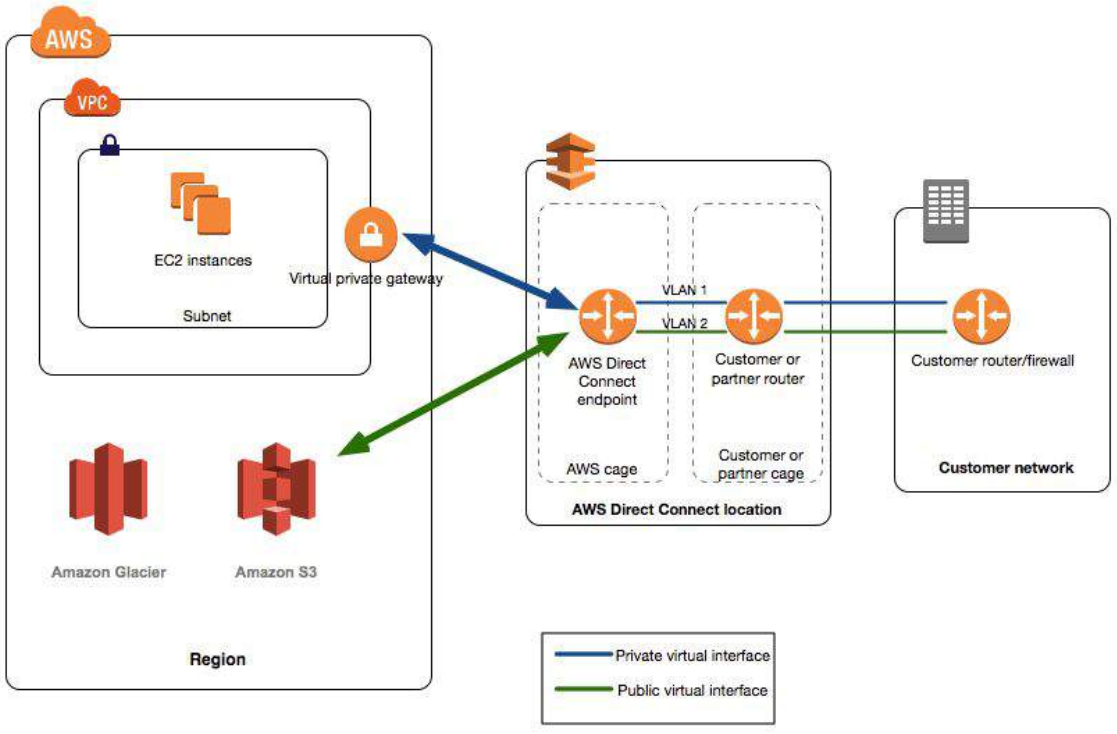

Imagen 65. Direct Connect.

Amazon Inspector: Puede utilizarse para identificar vulnerabilidades o posibles mejores prácticas en los sistemas operativos y aplicaciones desplegadas.

AWS CloudFormation: Puede utilizarse para crear y gestionar la infraestructura de manera automatizada. Permite definir plantillas (*templates*) en JSON o YAML para desplegar infraestructura de manera muy rápida y automática. Se pueden combinar plantillas y se conoce como un servicio de IaC (Infrastructure as Code).

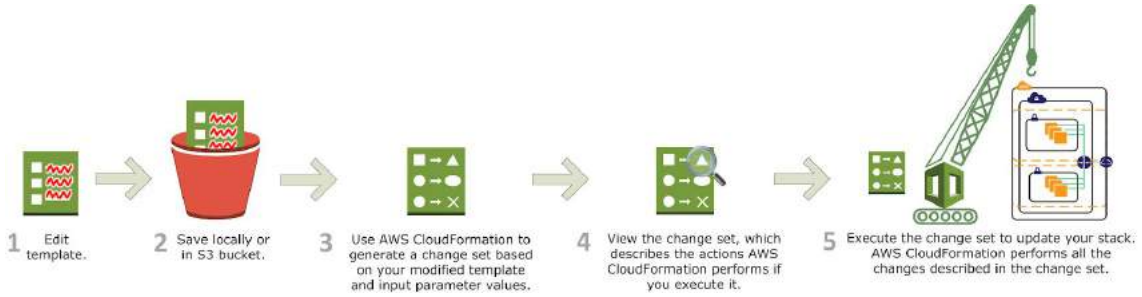

Imagen 66. Flujo CloudFormation.

La imagen 66 muestra el flujo de desplegar infraestructura con CloudFormation. El paso 5 deja intuir que se pueden desplegar infraestructura complejas. En la imagen 67 se muestran algunos de los posibles servicios que se pueden lanzar desde CloudFormation.

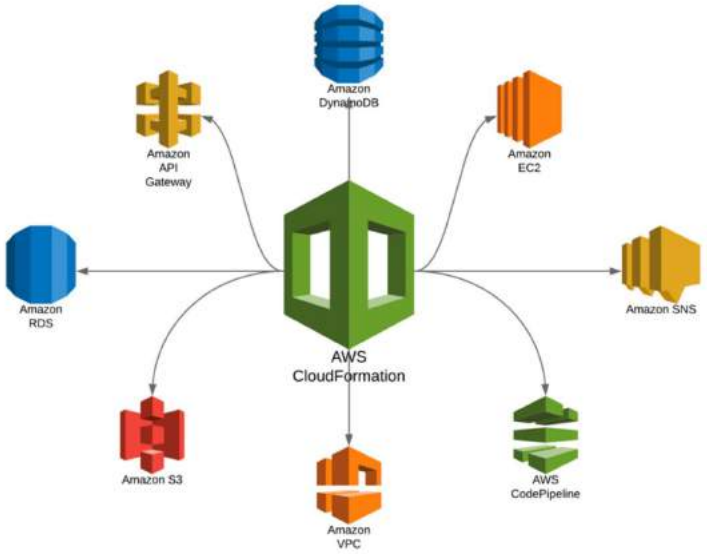

Imagen 67. CloudFormation posibles servicios desplegados.

5.4 Protección de los datos

Antes de diseñar cualquier sistema en la organización, se debe realizar la clasificación de los datos de forma que se categoricen los datos de la organización en función de los niveles de sensibilidad y criticidad. Tras esto se debe revisar qué tratamiento se les va a dar para protegerlos haciéndolos ininteligibles para el acceso no autorizado o ante una fuga de información. Este tratamiento va a ser esencial, más si cabe para los datos que sean considerados sensibles, ya que por un lado evitará el impacto reputacional o las pérdidas financieras ante una brecha de seguridad y, por otro lado, ayudará a cumplir con las regulaciones vigentes.

Tanto en sistemas *on premises* como en los sistemas de la nube se deberían tener en consideración los siguientes puntos:

- Clasificación de los datos
- Cifrado/Tokenización de los datos
- Protección de los datos en reposo (at rest)
- Protección de los datos en tránsito (in transit)
- Copias de seguridad (backups), réplica de los datos y recuperación de datos

5.4.1 Clasificación de los datos

La clasificación de los datos proporciona una forma de categorizar los datos de la organización en función de los niveles de sensibilidad de los mismos. Esto incluye la comprensión de los tipos de datos disponibles, el lugar donde se encuentran los datos, los niveles de acceso y la protección de los datos. [146]

Mediante la gestión cuidadosa de un sistema de clasificación de datos apropiado, junto con los requisitos a nivel de protección, se pueden trazar los controles y el nivel de acceso/protección apropiado para los datos. Por ejemplo, el contenido destinado al público general estará disponible para que cualquier persona tenga acceso a él, mientras que el contenido importante se cifra y se almacena de manera protegida, lo que requiere el acceso autorizado a una clave para descifrar el contenido.

El concepto de clasificación del dato en un enfoque holístico incluye la taxonomía, los esquemas y la categorización de los datos en aras de la confidencialidad, la integridad y la disponibilidad.

Por lo tanto, como se ha indicado en la introducción, independientemente de que los datos se procesen o almacenen en los sistemas *on premises* o en la nube, la clasificación de los datos es un punto de partida básico para determinar el nivel apropiado de los controles de la confidencialidad, la integridad y la disponibilidad de los datos en función del riesgo para la organización.

Las organizaciones de normalización, como la Organización Internacional de Normalización (ISO) y el Instituto Nacional de Normalización y Tecnología

(NIST), recomiendan planes de clasificación de datos para que la información se pueda gestionar y asegurar eficazmente en función de su riesgo relativo y su carácter crítico, aconsejando que no se apliquen prácticas que traten todos los datos por igual. Cada nivel de clasificación de datos debe asociarse a un conjunto básico recomendado de controles de seguridad que ofrezca una protección contra las vulnerabilidades, las amenazas y los riesgos proporcional al nivel de protección designado.

El proceso de clasificación de datos podría asemejarse al siguiente:

1. Establecer un catálogo de datos: Realizar un inventario de los diversos tipos de datos que existen en la organización, cómo se utilizan y si alguno de ellos se rige por un reglamento o política de cumplimiento. Una vez completado el inventario, se deben agrupar los tipos de datos en uno de los niveles de clasificación de datos que la organización haya adoptado.

2. Evaluar las funciones críticas de las empresas y realizar una evaluación del impacto: Un aspecto importante para determinar el nivel adecuado de seguridad de los conjuntos de datos es comprender el carácter crítico de esos datos para la empresa. Tras una evaluación de las funciones críticas para la empresa, se puede llevar a cabo una evaluación del impacto para cada tipo de datos.

3. Etiquetado de los datos: Someterse a una evaluación de garantía de calidad para asegurar que los bienes y los conjuntos de datos estén debidamente etiquetados en sus respectivos conjuntos de clasificación. Además, puede ser necesario crear etiquetas secundarias para los subtipos de datos a fin de diferenciar determinados conjuntos de datos dentro de un nivel debido a la privacidad u otros problemas de cumplimiento. El uso de servicios como AWS Glue para la creación del catálogo de datos [147] y Amazon SageMaker [148] para el etiquetado puede servir de apoyo en las actividades de clasificación y etiquetado de datos.

4. Manejo de activos: Cuando a los conjuntos de datos se les asigna un nivel de clasificación, los datos se manejan de acuerdo con las directrices de manejo apropiadas para ese nivel, que incluyen controles de seguridad específicos. Estos procedimientos de manipulación deben formalizarse, pero también ajustarse a medida que cambia la tecnología.

5. Monitorización continua: Seguir vigilando las pautas de seguridad, utilización y acceso de los sistemas y datos. Esto puede hacerse mediante procesos automatizados (preferiblemente) o manuales para identificar amenazas externas, mantener las operaciones normales del sistema, instalar actualizaciones y seguir los cambios en el entorno.

Existen diferentes modelos de clasificación de datos, con distintos nombres para los conjuntos de datos. Por ejemplo, el gobierno de Estados Unidos

identifica tres niveles en la clasificación de los datos y les asigna unos valores de organización como bajo, medio y alto.

Por otro lado, el gobierno de Reino Unido utiliza también tres niveles y los denomina como datos oficiales, datos secretos o altos secretos (*top secret*).

Aunque lo ideal es no tener mucha granularidad en las categorías principales, la ciudad de Washington D.C., implementó una clasificación de cinco niveles: datos abiertos, datos públicos, datos de uso gubernamental, datos confidenciales y datos confidenciales restringidos.

Por lo tanto, se recomienda tener entre tres y cinco categorías en los que incluir absolutamente todos los datos de la organización.

Es importante señalar que las organizaciones que aplican un nivel de clasificación general alto a todos los datos no reflejan un enfoque de la seguridad basado en los riesgos. La protección de los datos clasificados en niveles más altos requiere un nivel de atención más elevado, lo que se traduce en que la organización gaste más recursos en asegurar, vigilar, medir, remediar y notificar los riesgos. No es práctico destinar muchos recursos para gestionar de forma segura los datos de mayor repercusión en el caso de los datos no alcancen los umbrales requeridos. Además, los controles adicionales que se aplican a los datos de los niveles de clasificación más altos pueden afectar negativamente a la disponibilidad, integridad o entrega de esos datos al personal en general y a los clientes. Es decir, en este caso, no siempre más es mejor.

La clasificación de los datos es particularmente importante, ya que las nuevas leyes y reglamentos sobre la privacidad otorgan a los consumidores derechos de acceso, eliminación y otros controles sobre los datos personales. Por ejemplo, como se vio en apartado 3.4, en virtud del RGPD, las organizaciones están obligadas a responder a determinadas solicitudes de los consumidores en el plazo de un mes a partir de su recepción. A fin de responder adecuadamente, las organizaciones deben, por lo general, verificar la identidad del solicitante, localizar sus datos personales, asegurarse de que los datos devueltos sólo contienen los datos personales del solicitante y, posiblemente, rechazar una solicitud si es incompatible con la legislación aplicable. Las organizaciones que adoptan políticas sólidas de clasificación de datos están en mejores condiciones de dar respuestas oportunas a esas solicitudes. Un marco de clasificación de datos, junto con un etiquetado adecuado, ayudará a proteger estos datos personales.

5.4.2 Cifrado y tokenización

El cifrado y el tokenizado son dos procedimientos de protección de datos importantes pero distintos. La tokenización es un proceso que permite definir un token para representar un elemento de información que de otro modo sería sensible (por ejemplo, un token para representar el número de la tarjeta de crédito de un cliente). Un token debe carecer de sentido por sí mismo. El cifrado es una forma de transformar el contenido de manera que sea ilegible sin una clave secreta necesaria para descifrar el contenido de nuevo en texto

plano. Tanto la tokenización como el cifrado pueden utilizarse para asegurar y proteger la información según corresponda.

Al definir el enfoque de tokenización, se puede proporcionar una protección adicional para el contenido y puede asegurarse de que se cumple con los requisitos de cumplimiento. Por ejemplo, se puede reducir el alcance de un sistema de procesamiento de tarjetas de crédito si aprovecha un token en lugar de un número de tarjeta de crédito.

Al definir el enfoque de cifrado, se puede proporcionar protección para el contenido contra los usuarios no autorizados y contra la exposición innecesaria a los usuarios autorizados. AWS KMS ayuda a gestionar las claves de cifrado y se integra con muchos servicios de AWS. Se pueden definir alias de clave así como políticas de nivel de clave. Las políticas ayudan a definir los administradores de las claves así como los usuarios de las mismas. Por ejemplo, un sistema de gestión de secretos puede ser el único sistema que tenga acceso a la clave maestra que cifra los secretos para su almacenamiento.

Además, AWS CloudHSM es un módulo de seguridad de hardware que permite generar y utilizar fácilmente claves propias de cifrado en la nube de AWS. Ayuda a cumplir con los requisitos corporativos, contractuales y de cumplimiento normativo en materia de seguridad de los datos mediante el uso de HSM validados por el FIPS 140-2 nivel 3.

Al definir el enfoque de cifrado/tokenización, se debe considerar el modelo de clasificación de datos que se ha definido previamente y los niveles de acceso necesarios para cada contenido.

Se indican a continuación algunas recomendaciones particulares para cumplir con lo expuesto:

- Política de menor privilegio posible: Siempre que se trabaje con claves de cifrado, debe utilizarse una política de otorgar los menos permisos posibles y mínimo acceso por parte de los usuarios. Por ejemplo, si una aplicación necesita escribir datos cifrados pero nunca los lee, solo se le asignará el permiso para cifrar, revocando el de descifrar.

- Rotación de claves de cifrado: Las claves de cifrado que se usen deben rotar, preferiblemente y siempre que sea posible de forma automática y con una periodicidad mínima anual. En caso de sospecha de que las claves de cifrado hayan podido ser expuestas será necesario realizar un rotado manual de las mismas. Cuanto más tiempo tenga una clave, mayor es el riesgo de haber sido comprometida.

- Etiquetado de claves de cifrado: Todas las claves de cifrado que se utilicen deben de estar etiquetadas con una etiqueta lo suficientemente descriptiva del uso que se le está dando a la clave. [149]

- Asignación de claves a recursos, no a personas: Siempre que sea posible, se limitará el acceso y uso de las claves de cifrado a roles IAM

asignados a servicios, evitando conceder el permiso de lectura y uso de las claves de cifrado a usuarios individuales.

- No reutilización de claves: Se deben generar claves individuales para cada aplicación o funcionalidad con un contexto específico de acceso a datos, quedando prohibido la reutilización de las mismas claves de cifrado.

- MFA para acciones específicas: Las operaciones más sensibles sobre el servicio de custodia de claves serán protegidas mediante el uso de un dispositivo de autenticación multifactor. Se consideran sensibles las operaciones de asignación de políticas sobre la clave maestra y borrado de claves tanto maestras como de aplicación. Algunas de las llamadas al API que deben protegerse son: PutKeyPolicy, ScheduleKeyDeletion, DeleteAlias, DeleteImportedKeyMaterial.

- Registro del repositorio de claves: Todas las acciones sobre el repositorio de claves deben quedar registradas para su posterior inspección en caso de ser necesario. En AWS esto queda integrado dentro del servicio CloudTrail.

5.4.3 Protección de los datos en reposo (at rest)

Los datos en reposo (at rest) representan cualquier dato que persista durante cualquier duración. Esto incluye el almacenamiento en bloque, el almacenamiento de objetos, las bases de datos, los archivos y cualquier otro medio de almacenamiento en el que persistan los datos. La protección de los datos en reposo reduce el riesgo de acceso no autorizado, cuando se implementa el cifrado y los controles de acceso apropiados.

Al implementar un método de protección basado en el cifrado en reposo, hay que tener en cuenta el modelo de clasificación de datos de la organización para asegurar que la protección del contenido refleje los requisitos comerciales, legales, de cumplimiento y normativos.

Los múltiples servicios de AWS proporcionan una integración total con el KMS de AWS para permitir el cifrado de los datos. Amazon S3 permite cifrar el contenido seleccionando una clave KMS en la carga de objetos. Amazon S3 también ofrece la posibilidad de cargar un objeto ya cifrado. Además proporciona la capacidad de cargar un objeto junto con una clave de cifrado que se utiliza en memoria para cifrar el objeto. Para recuperar el objeto, se debe proporcionar la misma clave. Esta función se conoce como cifrado del lado del cliente (Client-Side Encryption).

La otra opción es cifrar los datos del lado del servidor (Server-Side Encryption). S3 proporciona la función de cifrado del lado del servidor para cifrar los datos del usuario. Este proceso de cifrado es transparente para el usuario final (cliente) ya que se realiza en el lado del servidor. AWS gestiona la clave maestra usada para este cifrado y asegura que esta llave se rota regularmente. AWS genera un cifrado único para cada objeto y luego cifra el objeto usando AES-256. La clave de cifrado del objeto se cifra así misma usando AES-256,

con una llave maestra (Master Key), que también puede ser generada por AWS o por el cliente (CMK).

Amazon Elastic Block Store (Amazon EBS) permite elegir una clave KMS para cifrar un volumen de almacenamiento en bloque u operación de copia de la imagen de la máquina de Amazon (AMI). Amazon RDS permite elegir una clave de cifrado para cifrar el almacenamiento de la instancia de la base de datos en reposo (incluidas las instantáneas de copia de seguridad - *snapshots* -).

Recomendaciones particulares por servicio de almacenamiento de AWS:

Amazon S3

AWS S3 da la opción de añadir permisos a de nivel de *bucket* y a nivel de objeto, además se puede complementar con las políticas de IAM para un mejor control de acceso tanto a los objetos como a los *buckets* que los contienen.

- Restringir el acceso público: Los datos contenidos en los *bucket* S3 nunca deben estar expuestos a través de Internet, salvo en el caso de datos públicos y su distribución a través de redes de distribución de contenidos (CDN) como CloudFront o directamente S3.

- Versionado de objetos: Se deberá habilitar el versionado del *bucket* en todos los *bucket* S3 que contengan datos críticos para el correcto funcionamiento de la aplicación o del servicio cloud con el fin de garantizar la integridad y protegerlos contra borrados accidentales o malintencionados. Se puede restaurar un objeto a su versión anterior si la actual se considera que está comprometida.

  En el caso de datos muy críticos que sean almacenados en S3, se recomienda configurar el *bucket* con Cross-Region Replication (CRR).

- Borrado de objetos en S3 con MFA: En aquellos *buckets* que contengan información crítica se deberá implementar un control de borrado de objetos con MFA.

- Bloquear objetos mediante S3 Bloqueo de objetos (S3 Object Lock): Con S3 Bloqueo de objetos, se pueden almacenar objetos con un modelo de escritura única y lectura múltiple (Write Once Read Many). Se puede usar para evitar que se elimine o se sobrescriba un objeto durante un periodo de tiempo determinado o de manera indefinida, ayudando a cumplir con los requisitos normativos que precisen de almacenamiento durante, al menos, un número de años determinado fijando el periodo legal de retención. [150]

Amazon Glacier

AWS utiliza AES-256 para cifrar cada objeto de Glacier, ya que es una clase de almacenamiento de S3. Se generan claves de cifrado únicas y separadas para cada uno de los objetos. Por defecto, todos los datos almacenados en Glacier están protegidos por el cifrado del lado del servidor. La clave de cifrado se cifra a sí misma usando AES-256 con una clave maestra. Esta llave maestra se rota

regularmente. También se pueden cifrar los datos antes de cargarlos en Glacier.

Amazon EBS

Cada uno de los volúmenes de EBS se replican automáticamente dentro de su zona de disponibilidad, lo que protege contra el fallo de los componentes de un volumen de EBS, pero no protege ante fallos en la zona de disponibilidad.

- Realización de *backups*: Se deben crear instantáneas para los volúmenes de EBS de cara a obtener copias puntuales de los datos almacenados en el volumen de EBS. Estas instantáneas se almacenan en AWS S3 y se cifran tal como se ha dicho anteriormente. Dado que son objetos de S3, es posible y se deben aplicar las políticas adecuadas. Si se considera que un volumen ha sufrido una manipulación que pudiera haber comprometido la integridad de los datos, se podrían utilizar las copias de seguridad para restaurar una copia genuina.

- Cifrado de EBS: Se deben cifrar los volúmenes de EBS dado que el rendimiento de entradas y salidas por segundo (IOPS) de un volumen cifrado es similar a un volumen no cifrado, con un efecto insignificante en la latencia. Por lo tanto, en general, no hay razón para no cifrar estos volúmenes. También se integra con AWS KMS.

Amazon RDS

RDS permite cifrar los datos para volúmenes EBS, instantáneas, réplicas de lectura y copias de seguridad automatizadas de las instancias de RDS. Uno de los beneficios de trabajar con RDS es que el proceso de descifrado se maneja por el RDS de manera transparente para el usuario.

Amazon DynamoDB

DynamoDB permite implementar una capa de cifrado de datos sobre el servicio estándar de DynamoDB.

5.4.4 Protección de los datos en tránsito (in transit)

Los datos en tránsito son todos los datos que se transmiten de un sistema a otro. Esto incluye la comunicación entre los recursos dentro del entorno, así como la comunicación entre otros servicios y los usuarios finales. Al proporcionar el nivel adecuado de protección de los datos en tránsito, se protege la confidencialidad e integridad de los datos. Para proteger los datos en tránsito, los habitual es utilizar la Seguridad de la Capa de Transporte (TLS - Transport Layer Security).

Los servicios AWS proporcionan puntos finales HTTPS utilizando TLS para la comunicación, proporcionando así cifrado en tránsito al comunicarse con las API de AWS. El cliente tiene control total sobre sus recursos para implementar el cifrado en tránsito a través de los servicios. Además, el servicio AWS

Certificate Manager (ACM) ofrece la posibilidad de gestionar y desplegar certificados públicos y privados.

Además, se puede aprovechar la conectividad VPN - VPC o a través de las VPC para facilitar el cifrado del tráfico. En el apartado anterior (5.3) se presentó el diagrama de arquitectura para la implementación de múltiples VPN. En concreto, se representa en la imagen 64.

Algunos de los servicios de almacenamiento de datos que soportan SSL/TLS son Amazon S3, Amazon RDS, Amazon RDS, etc.

La parte relacionada con las copias de seguridad (backups), réplica de los datos y recuperación de datos se ha incluído en el desarrollo de los apartados anteriores.

Para finalizar la sección 5.4 - Protección de los datos, se proponen algunos de los servicios de AWS que pueden ayudar al cliente a conseguir los objetivos en materia de protección de datos:

AWS IAM: Para la gestión de las credenciales de los usuarios, la configuración de los permisos y la autorización del acceso a los datos.

AWS Web Application Firewall (WAF) y AWS Shield: Para proteger las aplicaciones web de los vectores de ataque más comunes (por ejemplo, SQL Injection, Cross-Site Scripting - XSS - y DDoS).

Amazon Macie: Puede ayudar a los clientes a inventariar y clasificar los datos sensibles y críticos para el negocio almacenados en AWS, Macie utiliza el aprendizaje automático para automatizar el proceso de descubrir, clasificar, etiquetar y aplicar las normas de protección a los datos. Esto ayuda a los clientes a comprender mejor dónde se almacena la información sensible, claves de cifrado incluidas, y cómo se accede a ella, incluyendo las autenticaciones de los usuarios y los patrones de acceso.

Se pueden configurar notificaciones cuando los datos protegidos salen de la zona segura y puede detectar eventos cuando se comparte una cantidad inusual de datos sensibles, ya sea interna o externamente.

AWS Organizations: Ayuda a gobernar el entorno de AWS de forma centralizada con la creación de cuentas automatizada, la agrupación de cuentas para reflejar las necesidades de la empresa y las políticas para hacer cumplir el gobierno. Las políticas pueden incluir acciones necesarias como el etiquetado de recursos.

AWS Glue: Para almacenar datos y descubrir metadatos asociados, así como la definición de tablas y esquemas, en el catálogo de datos de AWS Glue.

Amazon Neptune: Base de datos de gráficos totalmente gestionada que puede dar a los clientes una visión de las relaciones entre los diferentes conjuntos de datos. Esto puede incluir la identificación y la trazabilidad de los datos sensibles a través del análisis de metadatos.

AWS KMS: Para la gestión de claves de cifrado con claves generadas por AWS o aportando el cliente una clave propia (BYOK). AWS KMS cuenta con la validación FIPS 140-2 (Nivel 2).

AWS CloudHSM: Módulo de seguridad de hardware para la gestión de claves de cifrado con claves generadas por AWS o aportando el cliente una clave propia (BYOK), AWS CloudHSM cuenta con la validación FIPS 140-2 (Nivel 3). El módulo hardware es exclusivamente para el cliente y las claves nunca salen del módulo hardware.

AWS S3, EBS, Glacier y demás servicios de almacenamiento: Servicios de almacenamiento que se integran con AWS KMS para el cifrado de los objetos, bloques, ficheros, etc.

Replicación Cruzada de S3 (*Cross-Region Replication*): Característica a nivel de *bucket* de S3 que permite la copia automática y asíncrona de objetos a través de *buckets* en diferentes Regiones de AWS.

Instantánea (*snapshot*) de EBS: Copias de seguridad de los volúmenes adjuntos a las instancias EC2.

AWS CloudTrail: Registro extenso para rastrear quién, qué y cuándo crearon, accedieron, copiaron/movieron, modificaron y eliminaron los datos.

AWS Systems Manager: Útil para ver y gestionar las operaciones de servicio, como la aplicación de parches, junto con AWS Inspector para realizar escaneos de vulnerabilidades.

AWS Certificate Manager: Permite aprovisionar, administrar e implementar con facilidad certificados (SSL/TLS) públicos y privados para su uso con servicios de AWS y recursos internos conectados.

Balanceadores de carga (ELB): Soportan HTTPS y se integra con AWS Certificate Manager.

Amazon CloudFront (CDN): Soporta *endpoints* cifrados para la distribución de contenido.

AWS GuardDuty: Detección inteligente de amenazas apoyando los requerimientos de monitorización continua.

AWS Config: Gestión de los cambios de configuración e implementar reglas de gobierno.

5.5 Respuesta a incidentes

Incluso implantando correctamente todos los controles preventivos indicados en esta sección, cualquier organización debe poner en marcha procesos para responder y mitigar el impacto potencial de los incidentes de seguridad. Se deben poner en marcha las herramientas y procedimientos antes de un incidente de seguridad, y luego practicar periódicamente la respuesta a los posibles incidentes de cara a realizar simulacros lo más parecidos a situación que pueden llegar. [151]

En cada incidente, se debe conocer el impacto de la situación, es uno de los principios más importantes. Utilizando etiquetas para describir adecuadamente los recursos de AWS, los responsables de responder ante un incidente de seguridad, pueden determinar rápidamente el impacto potencial de un incidente.

Por ejemplo, una buena práctica es etiquetar las instancias y otros recursos con un propietario o una cola de trabajo que permita que el equipo pueda captar más rápidamente a las personas adecuadas. Al etiquetar los sistemas con una clasificación de datos o un atributo de criticidad, el impacto de un incidente puede estimarse con mayor precisión y celeridad.

Durante el incidente, las personas adecuadas pueden requerir acceso para aislar y contener el incidente, y después realizar una investigación forense para identificar rápidamente la causa que lo ha provocado. En algunos casos, el equipo de respuesta a incidentes también participa activamente en la reparación y en la recuperación. Determinar de antemano cómo van a obtener el acceso las personas adecuadas durante un incidente ayuda a agilizar la respuesta y volver al punto objetivo de recuperación (RTO - Recovery Time Objective) lo antes posible.

Por lo tanto, debe estar perfectamente documentado quiénes son los responsables ante un incidente de seguridad y todo aquello que necesiten para contener el incidente y volver al punto de situación con las menores pérdidas posibles.

En AWS prácticamente todo es automatizable y debería tenerse especial consideración en este apartado. Tener todo el procedimiento de gestión de incidentes automatizado puede hacer que de manera muy sencilla se contenga el incidente y se vuelva a la situación previa de manera casi transparente.

Por ejemplo, deben haber medidas automatizadas para la recolección de logs y salvaguardado de estos cifrados, scripts para el aislamiento de las instancias, copias de seguridad de los volúmenes y volcado de la memoria de la instancias. Scripts para deshabilitar usuarios y credenciales que probablemente hayan sido comprometidas.

Para realizar un análisis forense uno de los puntos que deben estar automatizados es el realizar una *snapshot* (instantánea) de las instancias afectadas y volcarlo en un *bucket* de S3.

De nuevo, se vuelve a recomiendar el uso de CloudFormation para crear rápidamente un nuevo entorno de confianza en el que llevar a cabo una investigación más profunda. La plantilla de CloudFormation puede preconfigurar instancias en un entorno aislado que contenga todas las herramientas necesarias que los equipos forenses necesitan para determinar la causa del incidente. Esto reduce el tiempo necesario para reunir las herramientas necesarias y aislar los sistemas a examinar.

Además de lo anterior, es recomendable realizar:

- Alertas de seguridad que avisen de un posible incidente atendiendo a umbrales.
- Realizar pruebas de procedimientos de recuperación: Se deberá estresar a la arquitectura diseñada de manera que se pongan a prueba todos los procedimientos de recuperación.
- Por supuesto se deben realizar obligatoriamente copias de seguridad de aquellos sistemas que almacenen datos esenciales para el negocio e incluso se ubicarán en distintas zonas de disponibilidad o regiones para estar cubiertos en el caso de caída de una zona de disponibilidad o región del proveedor de servicios cloud.

Todos los usuarios de AWS dentro de una organización deben tener una comprensión básica de los procesos de respuesta a los incidentes de seguridad, y el personal de seguridad debe comprender profundamente cómo reaccionar ante los problemas de seguridad. La base de un programa de respuesta a incidentes exitoso consiste en la educación, la preparación, la simulación y en las iteraciones realizadas.

Los servicios de AWS que ayudarán a cumplir con las recomendaciones anteriores son:

IAM: Debe utilizarse para conceder la autorización adecuada a los equipos de respuesta a incidentes.

AWS CloudFormation: Automatizar la creación de entornos de confianza para llevar a cabo investigaciones más profundas.

AWS CloudTrail: Proporciona el historial de llamadas a la API de AWS que pueden ayudar en la respuesta, en la detección automatizada y activación de los sistemas de respuesta.

Amazon CloudWatch Events: Para desencadenar diferentes acciones automatizadas a partir de cambios en los recursos de AWS incluyendo CloudTrail.

AWS Step Functions: Permite coordinar las tareas individuales en un flujo lógico para que se pueda crear y actualizar aplicaciones rápidamente. Los

flujos de trabajo que se crean con Step Functions se denominan máquinas de estado, y a cada paso de su flujo de trabajo se le denomina un estado. Un ejemplo de flujo puede ser un proceso de respuesta a incidentes. Las acciones que se pueden llevar a cabo en los estados pueden ser manuales o automática, pero se desaconsejan las acciones manuales en la medida de lo posible, ya que son más lentas y puede conducir a errores operativos.

5.6. Ejemplos de arquitecturas en AWS

Por último, se van a presentar tres ejemplos de arquitecturas, la primera enfocada a proporcionar la información suficiente para poder planificar el cumplimiento del PCI DSS [152], la segunda, es una implementación de arquitectura adecuada para una solución de *Open Banking* - API abiertas. [153] La tercera, enfocada a implantar una solución de teletrabajo, en particular la implantada en BBVA con ayuda de AWS en las últimas semanas. [156]

Se recomienda consultar la parte de AWS Quick Starts [93] y los repositorios de GitHub[11] introduciendo como búsqueda "AWS Samples" para obtener arquitecturas ya revisadas y contrastadas en la industria para que, al menos, sirvan de soporte y ayuda en el diseño de una arquitectura propia enfocada al caso de uso de cada organización. Por último, se recomienda consultar el sitio web de recursos de arquitectura de AWS [154].

5.6.1 Arquitectura PCI-DSS

Como ya se detalló en el apartado 3.2, el propósito del PCI DSS es proteger los datos del titular de la tarjeta (CardHolder Data) y los datos sensibles de autenticación contra el acceso no autorizado y la pérdida. Los datos del titular de la tarjeta consisten en el número de cuenta principal (PAN), el nombre del titular, la fecha de caducidad y el código de servicio.

Las aplicaciones que almacenan, procesan o transmiten datos de los titulares de tarjetas deben estar protegidas y requieren una planificación detallada tanto para implementar como para demostrar el cumplimiento de todos los controles del PCI DSS.

Es importante señalar que el PCI DSS no es sólo un estándar de tecnología, sino que también abarca a las personas y a los procesos involucrados. La seguridad y el cumplimiento de PCI DSS son responsabilidades compartidas entre AWS y el cliente.

El listado de los servicios de AWS marcados como compatibles con el PCI DSS significa que tienen la capacidad de ser configurados por los clientes para cumplir con los requisitos del PCI DSS, pero no significa que cualquier uso de ese servicio sea automáticamente compatible. Los clientes son responsables de la implementación de los controles adicionales que puedan ser necesarios o aplicables.

Es fundamental comprender el flujo completo de datos de los titulares de las tarjetas dentro de las aplicaciones y el entorno, incluidas las interacciones con los procedimientos y el código de la aplicación. El flujo de datos determina la aplicabilidad del PCI DSS, define los límites y los componentes del entorno de datos de los titulares de tarjetas (CDE) y el alcance de una evaluación del PCI DSS.

En la imagen 68 se muestra un ejemplo a través del diagrama de flujo de datos:

[11] https://github.com/aws-samples/

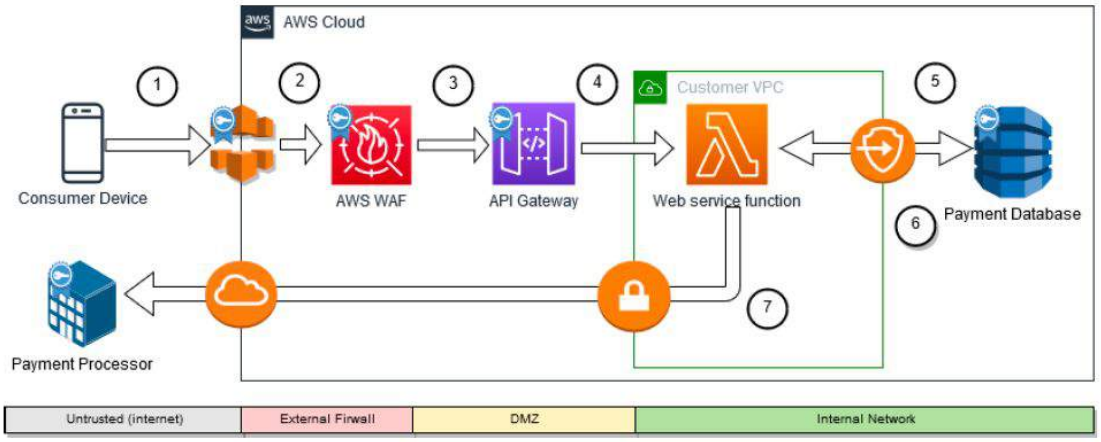

Imagen 68. Diagrama flujo de datos transacción sujeta a PCI DSS.

Y en la imagen 69, se muestra cada uno de los pasos detallados:

Step	Source	Transport	Protection	Access Control	CHD	Destination	Term TLS?
1	Consumer device	Internet	TLS	• Anti-spoofing • Permit only HTTPS on port 443	PAN, Name, Expiration, CVV2 – if new payment method only	Amazon CloudFront	No
2	Amazon CloudFront	Amazon network	TLS	• WAF listening ports (only 443 in this case) • Stateful inspection • Application attack rules	PAN, Name, Expiration, CVV2	AWS WAF	Yes
3	AWS WAF instance	Amazon network	TLS	• URL parameter rules • Authentication • Authorization	PAN, Name, Expiration, CVV2	Amazon API Gateway	Yes
4	Amazon API Gateway	Amazon network	Private network	• Function parameter validation	PAN, Name, Expiration, CVV2	Lambda web service request handler function (AWS Lambda)	NA
5	Web service request handler function	Private VPC	TLS	• Security Group • VPC endpoint for Amazon DynamoDB on private VPC • AWS API credentials • IAM roles • Resource policies	PAN, Name, Expiration – Save payment method	Future purchase Database (Amazon DynamoDB)	Yes
6	Future purchase Database	Private VPC	TLS	N/A - response traffic	PAN, Name, Expiration – Retrieve payment method	Web service request handler function	N/A
7	Web service request handler function	Internet	IPSec VPN	3rd party service provider defined	PAN, Name, Expiration, CVV2 (only for initial authorization)	3rd party payment processor	3rd party service provider defined

Imagen 69. Pasos flujo de datos transacción sujeta a PCI DSS.

El PCI DSS requiere que los clientes mantengan los diagramas de red actualizados, ya que son diagramas críticos. Deben mostrar claramente los límites de las redes y el entorno, todos los puntos de entrada y salida, y los controles de acceso a la red en los puntos de comunicación entre el entorno de datos del titular de la tarjeta y las redes tanto de confianza como de no confianza.

Una arquitectura [155] estándar para PCI DSS en AWS se muestra en la imagen 70.

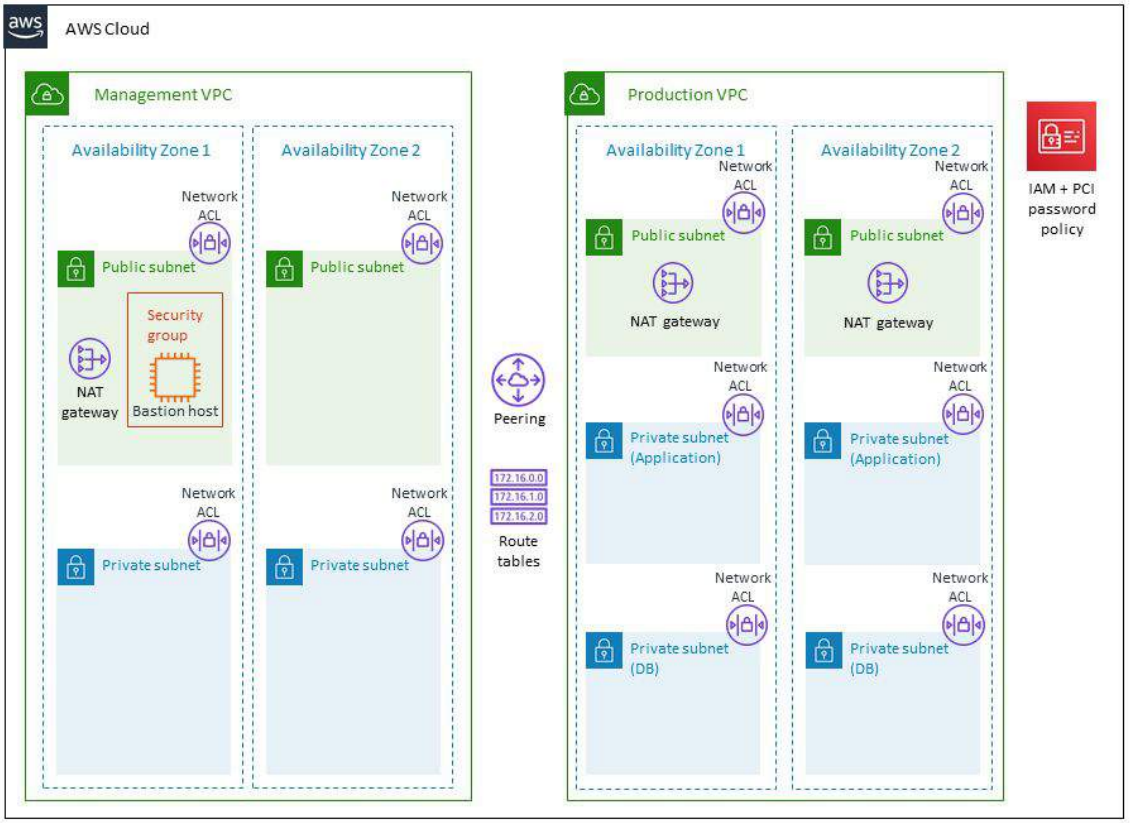

Imagen 70. Arquitectura de red estándar para PCI DSS en AWS

La arquitectura incluye los siguientes componentes y características:

- Configuración básica de AWS IAM con políticas personalizadas de IAM con grupos, roles y perfiles de instancia asociados.
- Política de contraseña que cumple los requisitos de la PCI.
- Una arquitectura Multi-AZ de VPC externa estándar con subredes independientes para diferentes capas de la aplicación y subredes privadas (*backend*) para la aplicación y la base de datos.
- Las gateways NAT (Traducción de direcciones de red) administrados para permitir el acceso de salida a Internet a los recursos de las subredes privadas.

- Un host bastión de inicio de sesión protegido para facilitar el acceso de SSH mediante la línea de comandos a las instancias EC2 para la resolución de problemas y actividades de administración de sistemas
- Reglas de lista de control de acceso a red (NACL) para filtrar tráfico.
- Grupos de seguridad estándar para instancias EC2.

Profundizando en el detalle de arquitectura de la base de datos, un ejemplo de referencia podría ser el mostrado en la imagen 71.

Imagen 71. Arquitectura de base de datos.

La arquitectura incluye los siguientes componentes y características:

- Clúster de base de datos cifrada MySQL de Amazon Aurora en varias zonas de disponibilidad
- Grupo de seguridad para la base de datos. El grupo de seguridad permite el acceso sólo a través del puerto 3306 y sólo desde la VPC especificada.

- La clave maestra de cliente (CMK) AWS Key Management Service (AWS KMS) con alias de clave definida por el usuario y con rotación automática activada.
- Grupos de IAM con permisos de uso para administradores de claves y usuarios.
- Secrets Manager establecido para rotar la contraseña de la base de datos de manera periódica.

5.6.2 Arquitectura banca abierta (Open banking)

Como se ha indicado en la introducción de la sección, se va a incluir una referencia a la arquitectura propuesta por AWS de cara a la implementación de una arquitectura adecuada para las APIs abiertas. Esto ayudará a las entidades financieras a desplegar una arquitectura apropiada para el cumplimiento de PSD2 (visto en el apartado 3.3).

La arquitectura se muestra en la imagen 72.

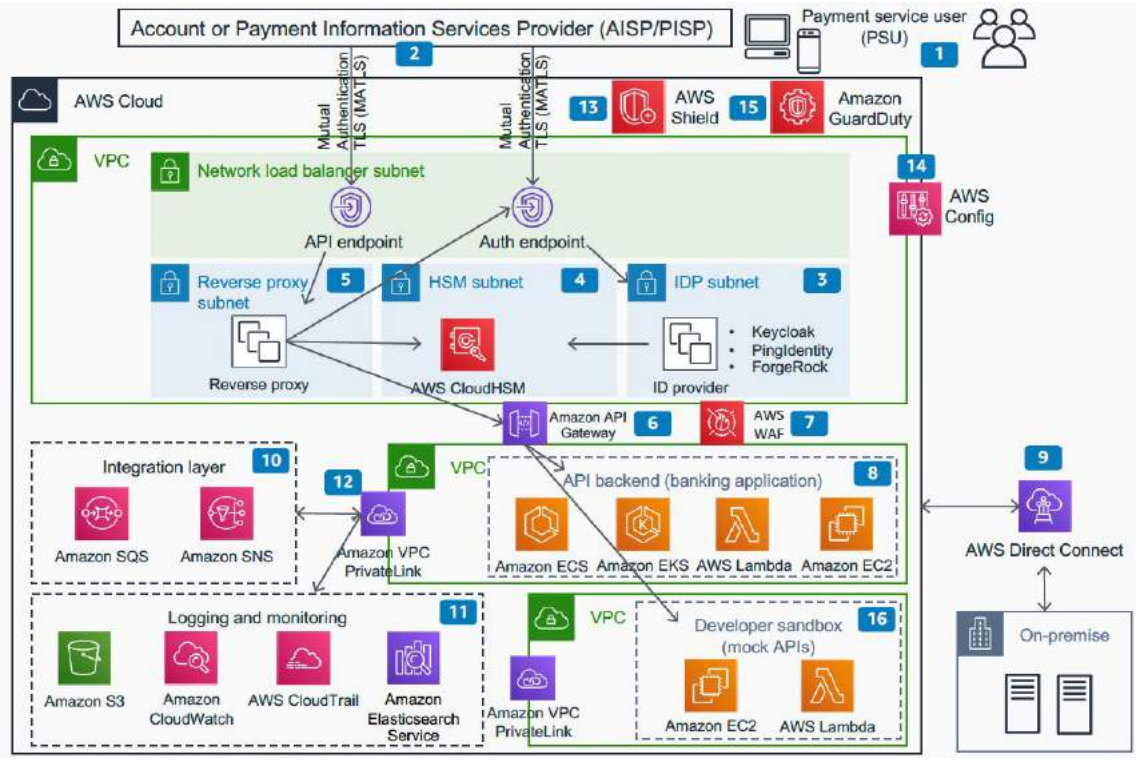

Imagen 72. Arquitectura de referencia Open banking - PSD2.

Los números de la imagen 72 representan lo siguiente:

1. El usuario del servicio de pago accede a la aplicación de terceros; puede utilizar cualquier servicio dentro de dicha aplicación.
2. Los terceros - proveedores de servicios de información de cuentas o pagos (AISP/PISP) - construyen aplicaciones en torno a los pagos, la transferencia de dinero, etc. La agregación de datos entre los bancos

proporciona más información al cliente como, por ejemplo, el análisis de gastos, el balance entre bancos.

3. La aplicación de terceros obtiene un token de acceso del proveedor de servicios de pago de cuentas (ASPSP) para atender las solicitudes de los usuarios. El ASPSP valida el certificado de AISP/PISP utilizando la autenticación mutua TLS (mTLS) y proporciona un token de acceso.
4. El CloudHSM se encarga de gestionar los certificados SSL para los puntos finales de API y Auth.
5. Se utiliza un proxy inverso como, por ejemplo, Nginx para cumplir con el requisito de mTLS del estándar de Open Banking.
6. Amazon API Gateway se encarga de la gestión completa de las API bancarias.
7. El AWS WAF se integra con el API Gateway para protegerse contra los exploits web comunes.
8. La lógica bancaria se implementa usando AWS Lambda, contenedores, o ejecutando instancias de Amazon EC2.
9. Desde lo implementado en el punto 8, se accede al centro de datos *on premises* de la entidad financiera usando AWS Direct Connect (conexión punto a punto dedicada que no atraviesa Internet).
10. El SQS (servicio de colas) y el SNS (servicio de notificaciones) de Amazon proporcionan capacidades de integración y notificación entre diferentes servicios para implementar arquitecturas desacopladas.
11. Los logs de los servicios recogidos por CloudWatch y CloudTrail se almacenan en un *bucket* de S3 y se analizan usando el Amazon Elasticsearch.
12. AWS PrivateLink conecta la VPC a los servicios de AWS soportados.
13. En la capa perimetral, AWS Shield protege contra los ataques de DDoS.
14. Con AWS Config se proporciona un cumplimiento continuo de la cuenta de AWS.
15. Amazon GuardDuty monitoriza continuamente la actividad maliciosa y el comportamiento no autorizado; protegiendo la cuenta de AWS.
16. Por último, los terceros utilizan una *sandbox* de desarrollo separada para construir sus aplicaciones en un entorno controlado.

5.6.3 Arquitectura trabajo remoto con Amazon AppStream 2.0 - BBVA

Este último ejemplo pone de manifiesto varias ventajas de las soluciones en la nube como son la velocidad en el despliegue y la elasticidad. Estas dos ventajas que proporciona la nube son características clave cuando las organizaciones se enfrentan a escenarios inesperados como, por ejemplo, la pandemia actual.

En BBVA prácticamente la totalidad de los empleados sigue haciendo su trabajo fuera de las oficinas. BBVA ha implementado un plan de trabajo en remoto global que protege a los clientes y empleados por igual. También ha garantizado que se pudieran seguir realizando operaciones de manera continua e ininterrumpidas tanto para consumidores como para clientes comerciales al fortalecer el acceso digital a su conjunto completo de servicios.

BBVA, como entidad financiera que opera en Europa, está sujeta a un conjunto de requisitos altamente regulados, tal y como se ha visto en el apartado tres de este trabajo. Por lo tanto, debían buscar una solución rápida de implementar, adaptable para escalar gradualmente en los diversos países en los que opera, y capaz de cumplir con los requisitos operativos, de seguridad y reglamentarios. Todo ello para dar soporte a los más de 86000 empleados que actualmente trabajan de forma remota.

Para ello, BBVA seleccionó Amazon AppStream 2.0 [157], para los casos de uso de aplicaciones que, debido a su sensibilidad, no están expuestas a Internet como, por ejemplo, aplicaciones financieras, internas de empleados y de seguridad.

AppStream 2.0 es un servicio de transmisión de aplicaciones totalmente administrado por AWS que proporciona a los usuarios acceso instantáneo a sus aplicaciones de escritorio desde cualquier lugar, independientemente del dispositivo que estén utilizando.

AppStream 2.0 funciona con entornos de TI, se puede administrar a través del SDK o la consola de AWS, se escala automáticamente a nivel mundial bajo demanda y se administra completamente en AWS. Esto significa que no hay hardware o software que implementar, parchear o actualizar por parte del cliente.

Una arquitectura típica puede ser la mostrada en la imagen 73:

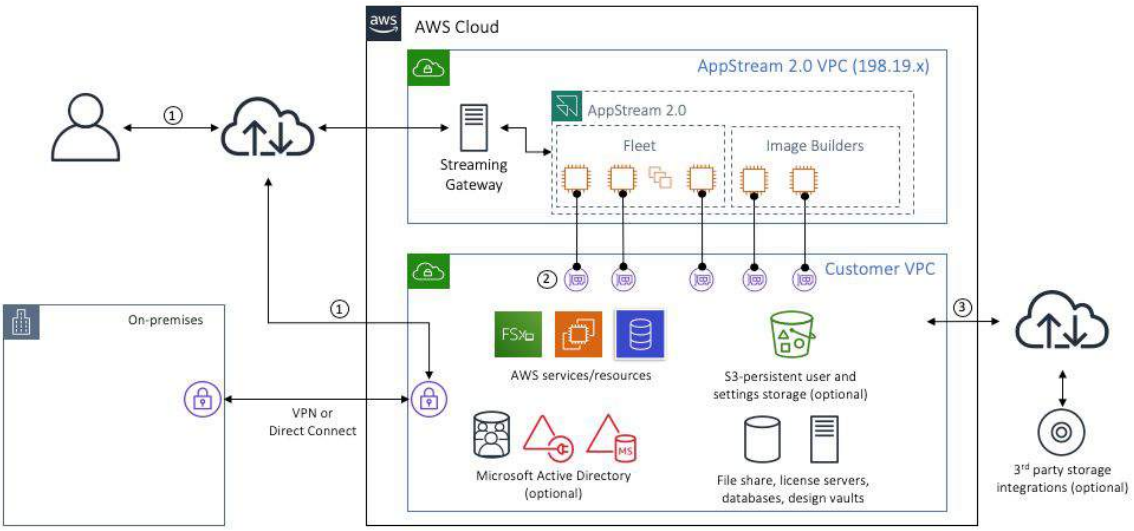

Imagen 73. Arquitectura AppStream 2.0

Destacar que la transmisión y las entradas del usuario se envían a través de HTTPS y se cifran con SSL entre las instancias de AppStream 2.0 que ejecutan las aplicaciones y los usuarios finales (1). Los grupos de seguridad (Security Groups) se utilizan para controlar el acceso de red a la VPC del cliente (2) y el acceso a la instancia de transmisión de AppStream 2.0 a Internet se realiza a través de la VPC del cliente (3).

Las flotas de instancias de AppStream 2.0 se crean por caso de uso para aplicar restricciones de seguridad según la sensibilidad de los datos. Al configurar el portapapeles, la transferencia de archivos o las preferencias de impresión en las opciones de dispositivos locales, las flotas de instancias controlan el movimiento de datos hacia y desde las sesiones de transmisión AppStream 2.0 de los empleados.

La arquitectura desplegada por BBVA es la mostrada en la imagen 74.

Para simplificar la arquitectura de red, BBVA usa AWS Transit Gateway para construir una topología de red de concentrador con control total sobre el enrutamiento y la seguridad de la red.

Hay situaciones en las que la aplicación transmitida en AppStream 2.0 necesita conectarse:

1. A las instalaciones, mediante AWS Direct Connect más VPN lo que proporciona una conexión privada con cifrado IPsec.

2. A Internet a través de un proxy VPC saliente con listas blancas de dominio y filtrado de contenido para controlar la información y las amenazas en la navegación del empleado.

La actividad de AppStream 2.0 se registra en un repositorio centralizado, en particular en un *bucket* de Amazon S3, que sirve para detectar patrones de comportamiento inusuales además de por requisitos regulatorios.

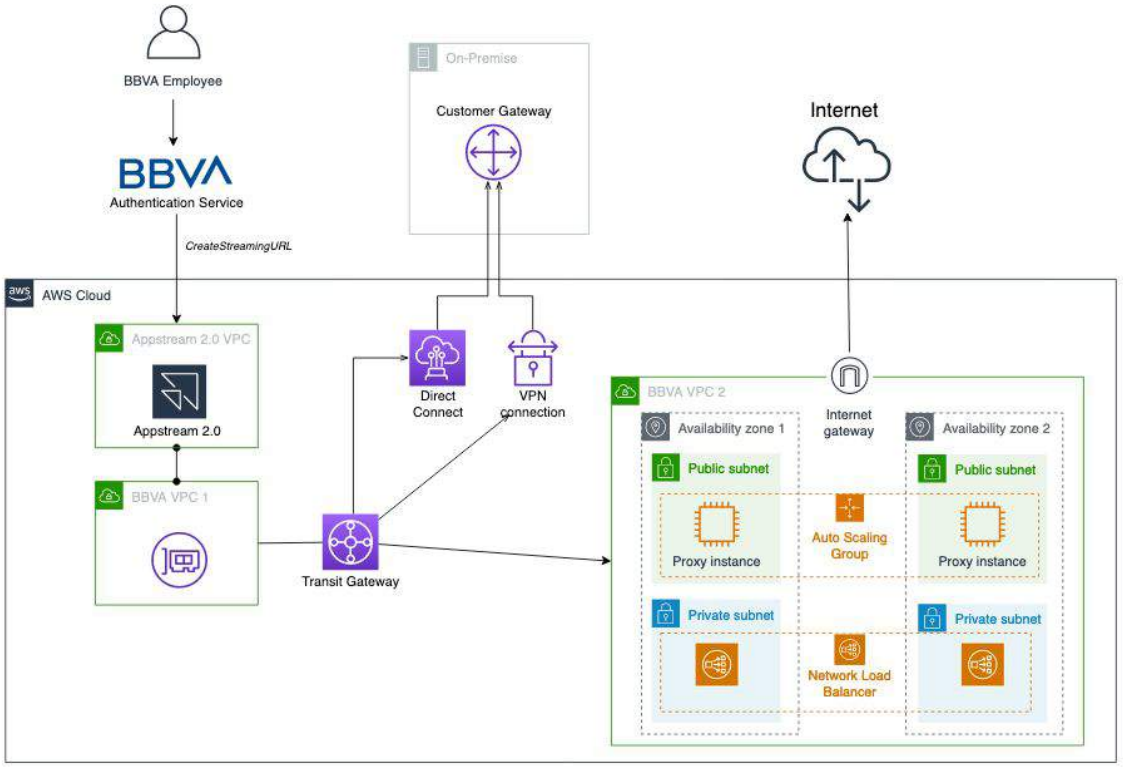

Imagen 74. Arquitectura AppStream 2.0 desplegada por BBVA en AWS

Por último, destacar que BBVA tiene flotas de instancias desplegadas tanto en Europa como en América para proveer una solución altamente disponible, tolerante a fallos y que ofrece unas latencias menores en función de la ubicación de los empleados. Además, la autenticación de los empleados se delega en el proveedor de identidad de la propia organización.

En muy poco tiempo, BBVA ha creado una solución global que reduce el tiempo de implementación en un 90% en comparación con los proyectos locales y cumple con los requisitos operativos, de seguridad, así como los impuestos por los regulares.

6. Conclusiones

Este trabajo surge de la necesidad de conocer qué acciones pueden llevar a cabo las empresas del sector financiero dado que cada vez surgen más casos de bancos digitales que están ganándoles parte del negocio que estos tenían no hace muchos años. Además, se pretendía conocer qué opciones tenían para llevar a cabo la migración, en qué condiciones y bajo qué regulaciones debido a que es obligatorio cumplir con las mismas.

Que las entidades financieras lleven unos años realizando el proceso de transformación digital se debe a que estos nuevos competidores son empresas pensadas para nacer con una filosofía 100% digital reduciendo las dificultades de las entidades financieras con centros de procesamiento de datos tradicionales. Algunas de estas desventajas son aprovisionamiento de máquinas, instalación y configuración, etc. que deriva en un largo *time to market.*

Además, el sector financiero se ha visto forzado a realizar una profunda transformación digital porque han surgido directivas como la PSD2 que abre el negocio bancario a terceras empresas que no son entidades financieras (no tienen licencia bancaria), pero pueden hacer uso de los datos bancarios de los clientes siempre que estos lo hayan autorizado explícitamente para proveer valor al cliente en base a sus datos.

Por lo tanto, con este trabajo se pretendía revisar qué ofrecen estos proveedores cloud, que normativas, regulaciones, etc. aplican a las entidades financieras y estudiar posibles arquitectura en su migración a sistemas cloud, ya que es básico migrar gran parte de la infraestructura tradicional debido a las bondades de estos sistemas si no quieren quedarse atrás.

El estudio se ha realizado teniendo el foco en la parte de seguridad, ya que más allá de los datos internos que cualquier empresa puede tener, en las entidades financieras existen datos muy sensibles de los clientes. Por ejemplo, datos identificativos, datos económicos, datos de salud, si ofrecen seguros de salud, y multitud de otros datos muy sensibles. Por lo tanto, es esencial mantenerlos lo más seguros posibles en sistemas cloud tal y como se pretende en sistemas *on premises.*

Al inicio de este trabajo se ofrecían datos de cómo las empresas almacenan sus datos en proveedores cloud y se evidenciaba que había muchas oportunidades de mejora en este ámbito. Este trabajo puede ser una puerta de entrada para muchas de estas empresas en materia de protección de datos en sistemas cloud, ya que introduce a múltiples opciones para tratar de mantener los datos más seguros que como se encuentran actualmente.

Por lo tanto, se han cumplido todos los objetivos que se propusieron en el apartado 1.2, ya que se han estudiando qué ofrecen los proveedores de servicios cloud para la migración y el almacenamiento de los datos. Se han revisado soluciones para realizar la migración de los datos desde los sistemas *on premises* a los sistemas cloud, se han introducido qué opciones de almacenamiento existen para tratar de dar cabida a cualquier tipo de almacenamiento utilizado en sistemas tradicionales y se han revisado las

opciones de cifrado que se ofrecen. También se han estudiado el conjunto de servicios de seguridad para montar un ecosistema lo más seguro posible.

Enfocado al sector financiero, se han revisado regulaciones y directivas de obligado cumplimiento para las entidades financieras europeas como el RGPD, PCI-DSS y PDS2. No obstante, destacar que el RGPD afecta a cualquier organización que opere en la Unión Europea, sea del sector que sea y es de obligado cumplimiento desde el 25 de mayo de 2018.

Por último, se han introducido sistemas de seguridad en la nube, pero ajenos a los principales de proveedores de servicios cloud. En particular se han introducido los agentes de seguridad de acceso a la nube, conocidos como CASB.

Para concluir, se han presentado diferentes arquitecturas de más complejidad que las mostradas a lo largo del trabajo y que cubren casos básicos y actuales para una entidad financiera como el cumplimiento de PCI DSS, API de PSD2 y disponibilizar aplicaciones internas en tiempos de teletrabajo global.

Respecto a lo aprendido, aunque contaba con algunas nociones básicas en la mayoría de apartados del trabajo, estas se han visto fuertemente reforzadas con el estudio realizado en estos meses y, en muchos casos, han sido realmente importantes por el descubrimiento de nuevos conceptos y necesidades a la hora de realizar diseños de arquitecturas en sistemas en la nube.

Destacar que no ha sido necesario introducir cambios a nivel temporal respecto a la planificación mostrada en el apartado 1.4. Sí se ha introducido algún cambio en el contenido, pero siempre para proporcionar una visión más completa, ya que antes de realizar el estudio detallado de la sección no se tenía el conocimiento suficiente sobre el alcance del mismo.

A raíz de la realización de este trabajo surgen varias posibilidades de trabajos futuros, algunos de ellos son los siguientes:

1. Propuesta de arquitectura basada en un caso de uso real para pequeñas y medianas empresas. Este trabajo está enfocado en empresas del sector financiero por la sensibilidad de sus datos y por la multitud de regulaciones a las que están expuestas. Debido a que prácticamente todo el contenido el extrapolable a pymes, se considera que un posible trabajo futuro es acotarlo a un ejemplo real, tratar de dar un marco de arquitectura para empresas que estén interesadas en la migración a sistemas en la nube para reducir costes, reducir los tiempos de aprovisionamiento y despliegue, sin tener por ello que reducir los aspectos de seguridad e incluso en la mayoría de casos aprovechar para realizar una correcta implementación de seguridad para tratar de mitigar los riesgos asociados. Para ello, sería útil reutilizar las pequeñas arquitecturas mostradas en las imágenes a lo largo de este trabajo.
2. Como se ha visto en el apartado 5.4.1, es vital realizar una clasificación de los datos que tiene la empresa antes de abordar cualquier diseño de arquitectura y, en particular, el almacenamiento y tratamiento de los datos, ya sea cifrado, tokenizado, etc. Por lo tanto, otro trabajo muy interesante podría ser tratar de profundizar en este tema y realizar una

propuesta de clasificación de datos para empresas de gran tamaño como puede ser una entidad financiera, pero manteniendo el foco en la reutilización por parte de otras empresas que su conjunto de datos sea menor o sea un subconjunto de los analizados.

3. Una vez que se migra la infraestructura a sistemas de proveedores en la nube hay que estar preparados para los posibles incidentes de seguridad que pueden llegar. Por ello se abren dos posibles vías de trabajo que en función del tamaño de la organización pueden unificarse en una.
    a. Realizar el sistema de gestión de seguridad de la información (SGSI) en sistemas en la nube.
    b. Realizar pruebas de estrés para la arquitectura desplegada de cara a ver cómo funciona el plan de recuperación de desastres (Disaster Recovery Plan). Lo ideal sería simular fallos en las máquinas para revisar cómo la propia arquitectura desplegada es capaz de recuperarse escalando o incluso, levantando una nueva arquitectura apoyándose, por ejemplo, en las soluciones de IaC - Infraestructura como Código (Infrastructure as Code).

7. Glosario

A continuación se muestra el listado de los términos y acrónimos más relevantes utilizados dentro del trabajo.

2FA - Segundo factor de autenticación.

ACL - Access Control List. Lista de control de acceso.

AD - Active Directory. Directorio activo.

AISP - Account Information Services. Servicios de Información de Cuentas. Servicios accesibles mediante API para los TPP.

AMI - Amazon Machine Image.

AoC - Attestation of Compliance. Declaración de cumplimiento de PCI.

API - Interfaz de programación de aplicaciones.

ASPSP - Account Servicing Payment Service Provider. Proveedor de servicios de pago de servicios de cuenta. Entidad financiera en la que un usuario de servicios de pago tiene cuentas a cuya información un tercero puede acceder en su nombre o en la puede iniciar una transferencia.

AWS - Amazon Web Services.

AZ - Availability Zones. Zonas de disponibilidad en una región de AWS.

Backup - Copia de seguridad.

BBDD - Base de datos.

BYOK - Bring Your Own Key. El cliente lleva, proporciona su propia clave de cifrado.

CASB - Cloud Access Security Broker. Agentes de seguridad de acceso a la nube.

CCM - Cloud Controls Matrix. Matriz de controles para el análisis de proveedores cloud de la CSA.

CMK - Customer Master Key. Clave maestra del cliente.

CPD - Centro de procesamiento de datos.

CSA - Cloud Security Alliance.

CVE - Common Vulnerabilities and Exposures. Vulnerabilidades y exposiciones comunes. Lista de información registrada sobre vulnerabilidades de seguridad conocidas, en la que cada referencia tiene un número de identificación CVE-ID.

DBaaS - Database as a Service. Bases de datos como servicio.

DDoS - Distributed Denial of Service. Denegación de servicio distribuido.

DMS - Database Migration Service. Servicio de migración de bases de datos.

DNS - Domain Name Service. Servicio de nombres de dominio.

EBA - European Banking Authority. Autoridad Bancaria Europea.

EBS (AWS) - AWS Elastic Block Service.

EC2 (AWS) - AWS Elastic compute cloud.

EFS (AWS) - AWS Elastic File System.

EKM - Encryption Keys Management. Gestión de claves de cifrado.

ELB (AWS) - Elastic Load Balancer. Balanceador de carga.

ET - Encargado del tratamiento en el ámbito del RGPD.

Firewall - Sistema de seguridad para bloquear accesos no autorizados y permitir los accesos autorizados.

Gbps - Gigabits por segundo.

GDPR - General Data Protection Regulation.

HSM - Hardware Security Module. Módulo de seguridad hardware.

HYOK - Hold Your Own Key. El cliente mantiene sus propias claves de cifrado.

IaaS - Infraestructura como servicio.

IaC - Infraestructura como código.

IT - Tecnologías de la información.

KMS (AWS) - AWS Key Management Service. Servicio de gestión de claves.

KMS CSE - Customer Side Encryption. Cifrado en el lado del cliente.

KMS SSE - Server Side Encryption. Cifrado en el lado del servidor.

LOPD - Ley Orgánica de Protección de Datos.

MFA - Multi-Factor Authentication. Autenticación multifactor.

mTLS - mutual TLS. Autenticación mutua bidireccional, las dos partes de la comunicación se autentican entre sí al mismo tiempo.

NACL - Network Access Control List. Lista de control de acceso de red.

NAT - Network Address Translation. Traducción de direcciones de red

NIST - National Institute of Standards and Technology (USA).

OAuth 2.0 - Open Authorization versión 2.

Open Banking - La banca abierta es un término de servicios financieros como parte de la tecnología financiera que se refiere, entre otras cosas, al uso de API abiertas que permiten a los desarrolladores externos crear aplicaciones y servicios alrededor de las instituciones financieras.

PaaS - Platform as a Services. Plataforma como servicio.

PCI - Payment Card Industry. Industria pago con tarjeta.

PCI-DSS - Payment Card Industry Data Security Standard. Estándar de seguridad de los datos en los pagos con tarjetas.

PISP - Payment Initiation Service Provider. Proveedor de servicios de iniciación de pagos. TPP de servicios de transferencia bancaria gestionados en nombre de un usuario de servicios de pago a través de una API ofrecida por su entidad bancaria (ASPSP) previo consentimiento explícito del usuario al ASPSP.

PSD2 - Payment Services Directive. Directiva de servicios de pago versión 2.

RDS (AWS) - Relational Database Service. Servicio de bases de datos relacionales de AWS.

RGPD - Reglamento general de protección de datos.

RPO - Recovery Point Objective. Objetivo de posible pérdida máxima de datos introducidos desde la última copia de seguridad, hasta la caída del sistema ante un incidente.

RT - Responsable del tratamiento en el ámbito del RGPD.

RTO - Recovery Time Objective. Tiempo definido dentro del nivel de servicio en el que un proceso de negocio debe ser recuperado después de un desastre.

SaaS - Software as a Service. Software como servicio.

SAML 2.0 - Security Assertion Markup Language 2.0. Lenguaje de marcado para confirmaciones de seguridad utilizado para intercambiar identidades de autenticación y autorización entre dominios de seguridad.

SFTP - SSH File Transfer Protocol. Protocolo de transferencia de archivos seguro.

SGSI - Sistema de Gestión de la Seguridad de la Información.

SQL - Structured Query Language. Lenguaje de consulta estructurada.

SSH - Secure SHell.

SSL - Secure Sockets Layer. Capa de sockets seguros.

SSO - Single Sign-On. Inicio de sesión único.

TB - Terabytes

TIC - Tecnologías de la información y la comunicación

TLS - Transport Layer Security. Seguridad de la capa de transporte.

Tokenización - Proceso de sustitución de un elemento de datos sensible por un equivalente no sensible.

TPP - Third Party Provider. Prestador Financiero, AISP o PISP. Actúa en nombre de un usuario de servicios de pago accediendo a su información bancaria en otra entidad o iniciando una transferencia.

VPC (AWS) - Amazon Virtual Private Cloud. Nube privada virtual, permite aprovisionar una sección de la nube de AWS aislada de forma lógica

VPN - Virtual Private Network. Red privada virtual.

WAF - Web application firewall. Firewall de aplicaciones web.

8. Bibliografía

Todas las referencias de la [1] a la [77] se han visitado en marzo de 2020.

Todas las referencias de la [78] a la [119] se han visitado en abril de 2020.

Todas las referencias de la [120] a la [155] se han visitado en mayo de 2020.

[1] Estudio de Thales sobre el uso del cifrado en la cloud pública.
https://www.thalesesecurity.com/resources/infographics/2019-cloud-security-study

Tanto la referencia [2] como la [3] se han utilizado durante todo el estudio y desarrollo del apartado 2.5.

[2] Curso en Linux Academy - Plataforma para aprender sobre Cloud visitado en marzo de 2020: AWS Certified Solutions Architect – Associate Level

[3] Curso en Linux Academy - Plataforma para aprender sobre Cloud visitado en marzo de 2020: AWS Certified Security – Specialty Certification

[4] Modelo de responsabilidad compartida de AWS
https://aws.amazon.com/es/compliance/shared-responsibility-model/

[5] Modelo de responsabilidad compartida de Azure
https://docs.microsoft.com/es-es/azure/security/fundamentals/shared-responsibility

[6] Modelos de cloud públicas
https://aws.amazon.com/es/types-of-cloud-computing/

[7] Introducción a AWS
https://aws.amazon.com/es/what-is-aws/

[8] Infraestructura de AWS
https://www.infrastructure.aws/

[9] AWS Organizations
https://aws.amazon.com/es/organizations/

[10] Guía de usuario AWS Organizations
https://docs.aws.amazon.com/es_es/organizations/latest/userguide/organizations-userguide.pdf

[11] AWS EC2
https://aws.amazon.com/es/ec2/

[12] Guía de usuario - AWS EC2
https://docs.aws.amazon.com/es_es/AWSEC2/latest/UserGuide/concepts.html

[13] AWS VPC
https://aws.amazon.com/es/vpc/

[14] Categorías y servicios de AWS
https://aws.amazon.com/es/products/

[15] Página principal documentación de AWS
https://docs.aws.amazon.com/index.html

[16] Servicios de AWS desplegados por regiones
https://aws.amazon.com/es/about-aws/global-infrastructure/regional-product-services/

[17] Familia de productos Snow*
https://aws.amazon.com/es/snow/

[18] AWS Route 53 FAQs
https://aws.amazon.com/es/route53/faqs/

[19] AWS VPN FAQs
https://aws.amazon.com/es/vpn/faqs/

[20] AWS S3
https://aws.amazon.com/es/s3/

[21] AWS S3 FAQs
https://aws.amazon.com/es/s3/faqs/

[22] AWS S3 - Tipos de almacenamiento
https://aws.amazon.com/es/s3/storage-classes/

[23] Comparativa rendimiento distintas clases almacenamiento AWS S3
https://aws.amazon.com/es/s3/storage-classes/

[24] AWS EFS FAQs
https://aws.amazon.com/es/efs/faq/

[25] EBS
https://aws.amazon.com/es/ebs/

[26] EBS FAQs
https://aws.amazon.com/es/ebs/faqs/

[27] Bases de datos en AWS
https://aws.amazon.com/es/products/databases/

[28] Amazon RDS
https://aws.amazon.com/es/rds/features/

[29] Amazon RDS FAQs
https://aws.amazon.com/es/rds/faqs/

[30] Amazon Aurora
https://aws.amazon.com/es/rds/aurora/

[31] Amazon Redshift
https://aws.amazon.com/es/redshift/

[32] Amazon DynamoDB
https://aws.amazon.com/es/dynamodb/

[33] Amazon DynamoDB FAQs
https://aws.amazon.com/es/dynamodb/faqs/

[34] Características Amazon DynamoDB
https://aws.amazon.com/es/dynamodb/features/

[35] ElastiCache
https://aws.amazon.com/es/elasticache/

[36] Redis
https://aws.amazon.com/es/redis/

[37] Memcached
https://aws.amazon.com/es/memcached/

[38] Comparativa Redis - Memcached
https://aws.amazon.com/es/elasticache/redis-vs-memcached/

[39] Matriz controles cloud CSA
https://cloudsecurityalliance.org/research/cloud-controls-matrix/

[40] CSA - Security Guidance for Critical Areas of Focus in Cloud Computing
https://downloads.cloudsecurityalliance.org/assets/research/security-guidance/security-guidance-v4-FINAL.pdf

[41] AWS CloudHSM
https://aws.amazon.com/es/cloudhsm/

[42] AWS CloudHSM FAQs
https://aws.amazon.com/es/cloudhsm/faqs/

[43] AWS KMS
https://aws.amazon.com/es/kms/

[44] AWS KMS FAQs
https://aws.amazon.com/es/kms/faqs/

[45] NIST - FIPS 140-2
https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf

[46] AWS Certificate Manager
https://aws.amazon.com/es/certificate-manager/

[47] AWS Certificate Manager - FAQs
https://aws.amazon.com/es/certificate-manager/faqs/

[48] Private Certificate Authority
https://aws.amazon.com/es/certificate-manager/private-certificate-authority/

[49] Amazon Cognito
https://aws.amazon.com/es/cognito/

[50] AWS IAM
https://aws.amazon.com/es/iam/

[51] AWS IAM FAQs
https://aws.amazon.com/es/iam/faqs/

[52] Documentación AWS IAM
https://docs.aws.amazon.com/iam/index.html

[53] Protocolo aplicación políticas AWS IAM
https://docs.aws.amazon.com/es_es/IAM/latest/UserGuide/reference_policies_evaluation-logic.html

[54] AWS Secret Manager
https://aws.amazon.com/es/secrets-manager/

[55] AWS Secret Manager FAQs
https://aws.amazon.com/es/secrets-manager/faqs/

[56] AWS SSO
https://aws.amazon.com/es/single-sign-on/

[57] AWS SSO FAQs
https://aws.amazon.com/es/single-sign-on/faqs/

[58] Amazon GuardDuty FAQs
https://aws.amazon.com/es/guardduty/faqs/

[59] Documentación Amazon Inspector
https://docs.aws.amazon.com/inspector/latest/userguide/inspector_introduction.html

[60] Amazon Inspector FAQs
https://aws.amazon.com/es/inspector/faqs/

[61] Amazon Macie FAQs
https://aws.amazon.com/es/macie/faq/

[62] Documentación Amazon Macie
https://docs.aws.amazon.com/macie/latest/userguide/what-is-macie.html

[63] Clasificación datos de identificación personal
https://docs.aws.amazon.com/es_es/macie/latest/userguide/macie-classify-objects-pii.html

[64] Clasificación Amazon Macie expresiones regulares
https://docs.aws.amazon.com/es_es/macie/latest/userguide/macie-classify-objects-regex.html

[65] Amazon Detective FAQs
https://aws.amazon.com/es/detective/faqs/

[66] AWS Shield FAQs
https://aws.amazon.com/es/shield/faqs/

[67] AWS WAF FAQs
https://aws.amazon.com/es/waf/faqs/

[68] AWS Firewall Manager FAQs
https://aws.amazon.com/es/firewall-manager/faqs/

[69] AWS Artifact
https://docs.aws.amazon.com/es_es/artifact/latest/ug/what-is-aws-artifact.html

[70] AWS CloudWatch
https://aws.amazon.com/es/cloudwatch/

[71] Características AWS CloudWatch
https://aws.amazon.com/es/cloudwatch/features/

[72] AWS CloudWatch FAQs
https://aws.amazon.com/es/cloudwatch/faqs/

[73] CloudWatch Logs
https://docs.aws.amazon.com/es_es/AmazonCloudWatch/latest/logs/WhatIsCloudWatchLogs.html

[74] CloudWatch Events
https://docs.aws.amazon.com/AmazonCloudWatch/latest/events/WhatIsCloudWatchEvents.html

[75] AWS CloudTrail
https://aws.amazon.com/es/cloudtrail/

[76] AWS CloudTrail FAQs
https://aws.amazon.com/es/cloudtrail/faqs/

[77] Guía de usuario AWS CloudTrail
https://docs.aws.amazon.com/es_es/awscloudtrail/latest/userguide/cloudtrail-user-guide.html

[78] Banco de España
https://www.bde.es/bde/es/secciones/sobreelbanco/

[79] Autoridad Bancaria Europea
https://eba.europa.eu/about-us

[80] Ley 10/2014, de 26 de junio, de ordenación, supervisión y solvencia de entidades de crédito
https://www.boe.es/boe/dias/2014/06/27/pdfs/BOE-A-2014-6726.pdf

[81] EBA/GL/2017/05 - Directrices sobre la evaluación del riesgo de TIC en el marco del proceso de revisión y evaluación supervisora (PRES)
https://www.bde.es/f/webbde/INF/MenuHorizontal/Normativa/guias/EBA-GL_2017-05-ES.pdf

[82] EBA/GL/2019/02 - Directrices sobre externalización
https://www.bde.es/f/webbde/INF/MenuHorizontal/Normativa/guias/EBA-GL-2019_02_ES.pdf

[83] PCI Security Standards Council
https://www.pcisecuritystandards.org/about_us/

[84] PCI DSS 3.2.1
https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf

[85] SAQ - Cuestionario de autoevaluación
https://www.pcisecuritystandards.org/pci_security/completing_self_assessment

[86] Registro global de proveedores de servicios de Visa
https://www.visa.com/splisting/viewSPDetail.do?coName=Amazon%20Web%20Services%2C%20LLC&HeadCountryList=U.S.A.&pageInfo=1%3B30%3BASC%3BcoName

[87] lista de proveedores de servicios en conformidad con MasterCard
https://www.mastercard.com/us/company/en/docs/SP_Post_List.pdf

[88] Servicios de AWS que cumplen PCI DSS
https://aws.amazon.com/es/compliance/services-in-scope/

[89] TECHNICAL WORKBOOK PCI Compliance in AWS
https://d1.awsstatic.com/whitepapers/compliance/AWS_Anitian_Workbook_PCI_Cloud_Compliance.pdf

[90] PCI DSS Virtualization Guidelines
https://www.pcisecuritystandards.org/documents/Virtualization_InfoSupp_v2.pdf

[91] PCI SSC Cloud Computing
Guidelines
https://www.pcisecuritystandards.org/pdfs/PCI_SSC_Cloud_Guidelines_v3.pdf

[92] AWS Quick Start PCI DSS
https://aws.amazon.com/es/quickstart/architecture/compliance-pci/

[93] Guías de inicio rápido de AWS
https://aws.amazon.com/es/quickstart/

[94] PCI PIN Security Requirements and Testing Procedures
https://www.pcisecuritystandards.org/documents/PCI_PIN_Security_Requirements_Testing_v3_Aug2018.pdf

[95] PSD - Directiva de Servicios de Pago
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32007L0064

[96] PSD2 - Directiva de Servicios de Pago revisada
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L2366

[97] REGLAMENTO DELEGADO (UE) 2018/389
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R0389

[98] Fintonic
https://www.fintonic.com/es-ES/inicio/

[99] Web Scraping
https://es.wikipedia.org/wiki/Web_scraping

[100] Arquitectura referencia PSD2
https://developer.ibm.com/apiconnect/2018/08/21/psd2_architecture/

[101] Open Banking en AWS - Webinars noviembre 2019
https://aws.amazon.com/es/webinars-2019/

[102] Amazon API Gateway
https://aws.amazon.com/es/api-gateway/

[103] Amazon API Gateway FAQ
https://aws.amazon.com/es/api-gateway/faqs/

[104] Reglamento General de Protección de Datos - REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

[105] DIRECTIVA 95/46/CE DEL PARLAMENTO EUROPEO Y DEL CONSEJO
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046

[106] Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
https://www.boe.es/buscar/pdf/1999/BOE-A-1999-23750-consolidado.pdf

[107] Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
https://www.boe.es/boe/dias/2018/12/06/pdfs/BOE-A-2018-16673.pdf

[108] Derechos ARCO
https://ayudaleyprotecciondatos.es/2016/06/18/los-derechos-arco-acceso-rectificacion-cancelacion-y-oposicion/

[109] Noticias archivadas sobre el GT Art. 29
https://ec.europa.eu/newsroom/article29/news-overview.cfm

[110] Guidelines WG Art. 29
https://ec.europa.eu/newsroom/article29/news.cfm?item_type=1360

[111] AEPD - Guía para clientes que contraten servicios de Cloud Computing
https://www.aepd.es/sites/default/files/2019-09/guia-cloud-clientes.pdf

[112] AEPD - Orientaciones para prestadores de servicios de Cloud Computing
https://www.aepd.es/sites/default/files/2019-09/guia-cloud-prestadores.pdf

[113] AEPD - Guía Práctica de análisis de riesgos en los tratamientos de datos personales sujetos al RGPD
https://www.aepd.es/sites/default/files/2019-12/guia-rgpd-para-responsables-de-tratamiento.pdf

[114] Guía práctica para las Evaluaciones de Impacto en la Protección de los datos sujetas al RGPD
https://www.aepd.es/sites/default/files/2019-09/guia-evaluaciones-de-impacto-rgpd.pdf

[115] AWS - RGPD
https://aws.amazon.com/es/compliance/gdpr-center/

[116] Cumplimiento del RGPD en AWS
https://d1.awsstatic.com/whitepapers/compliance/GDPR_Compliance_on_AWS.pdf

[117] Comparativa servicios proveedores cloud CCSI
https://www.ccsinet.com/cloud-comparison-chart/

[118] Comparativa servicios proveedores cloud (I)
https://www.datamation.com/cloud-computing/aws-vs-azure-vs-google-cloud-comparison.html

[119] Comparativa servicios proveedores cloud (II)
https://www.paradigmadigital.com/dev/comparativa-servicios-cloud-aws-azure-gcp/

[120] Estudio Gartner CASB
https://www.gartner.com/doc/reprints?id=1-1XOFCANJ&ct=191024&st=sb

[121] Microsoft Cloud App Security
https://docs.microsoft.com/es-es/cloud-app-security/

[122] Procedimientos recomendados de Microsoft Cloud App Security
https://docs.microsoft.com/es-es/cloud-app-security/best-practices#apply-cloud-governance-policies

[123] Azure Active Directory
https://azure.microsoft.com/es-es/services/active-directory/

[124] Microsoft Cloud App Security - Configuración de seguridad para AWS
https://docs.microsoft.com/es-es/cloud-app-security/security-config-aws

[125] Netskope
https://www.netskope.com/products/casb

[126] Netskope Data Sheet
https://resources.netskope.com/netskope-data-sheets/netskope-cloud-security-platform

[127] Netskope Marketplace AWS
https://aws.amazon.com/marketplace/pp/Netskope-Netskope-Public-Cloud-Security/B082878BMG

[128] Netskope MarketPlace AWS
https://aws.amazon.com/marketplace/pp/Netskope-Netskope-Public-Cloud-Security/B082878BMG

[129] MVision Cloud
https://www.mcafee.com/enterprise/en-us/products/mvision-cloud.html

[130] MVision Cloud - Ficha técnica
https://www.mcafee.com/enterprise/en-us/assets/skyhigh/data-sheets/ds-skyhigh-cloud-security-platform.pdf

[131] Cloud Access Security Brokers Market
https://www.gartner.com/reviews/market/cloud-access-security-brokers

[132] Definitive Guide to Azure Security
https://www.mcafee.com/enterprise/en-us/assets/guides/gd-azure-security-guide.pdf

[133] McAfee MVISION Cloud for AWS
https://aws.amazon.com/marketplace/pp/B07SKBHJXR

[134] Skyhigh Networks CASB for Custom Application
https://aws.amazon.com/marketplace/pp/Skyhigh-Networks-Skyhigh-Networks-CASB-for-Custom-/B06XXN17MY

[135] CipherCloud
https://www.ciphercloud.com/

[136] Ficha técnica - CipherCloud CASB
https://ciphercloud.com//wp-content/uploads/2019/05/CipherCloud-CASB-Plus-Data-Sheet-v1.pdf

[137] OWASP
https://owasp.org/

[138] The Top 10 OWASP Cloud Security Risks
https://www.hitachi-systems-security.com/blog/the-top-10-owasp-cloud-security-risks/

[139] ISO 22301
https://www.isotools.org/normas/riesgos-y-seguridad/iso-22301/

[140] Security Pillar AWS Well-Architected Framework
https://d1.awsstatic.com/whitepapers/architecture/AWS-Security-Pillar.pdf

[141] Albert Anthony, AWS: Security Best Practices on AWS, Packt, Birmingham, UK, 2018.
https://www.packtpub.com/virtualization-and-cloud/aws-security-best-practices-aws

[142] Real-time Log streaming with CloudTrail and CloudWatch Logs
https://medium.com/@marcusrosen_98470/real-time-log-streaming-with-cloudtrail-and-cloudwatch-logs-3389c4cc5ef4

[143] Análisis de datos y cumplir los requisitos de seguridad mediante el uso de datos de registro de flujo centralizado
https://aws.amazon.com/es/blogs/security/how-to-facilitate-data-analysis-and-fulfill-security-requirements-by-using-centralized-flow-log-data/

[144] Web Application Hosting in the AWS Cloud
https://d1.awsstatic.com/whitepapers/aws-web-hosting-best-practices.pdf

[145] Rol IAM para instancia EC2
https://docs.aws.amazon.com/es_es/IAM/latest/UserGuide/id_roles_use_switch-role-ec2.html

[146] Data Classification Secure Cloud Adoption
https://d1.awsstatic.com/whitepapers/compliance/AWS_Data_Classification.pdf

[147] AWS Glue
https://aws.amazon.com/es/glue/

[148] AWS SageMaker
https://aws.amazon.com/es/sagemaker/

[149] Etiquetar claves de cifrado en AWS
https://docs.aws.amazon.com/es_es/kms/latest/developerguide/tagging-keys.html

[150] S3 bloqueo de objetos
https://docs.aws.amazon.com/es_es/AmazonS3/latest/dev/object-lock.html

[151] AWS Security Incident Response Guide
https://d1.awsstatic.com/whitepapers/aws_security_incident_response.pdf

[152] Arquitectura PCI DSS en AWS
https://d1.awsstatic.com/whitepapers/compliance/pci-dss-compliance-on-aws.pdf

[153] Arquitectura API abiertas en AWS
https://d1.awsstatic.com/architecture-diagrams/ArchitectureDiagrams/open-banking-on-aws.pdf

[154] Recursos de arquitectura
https://aws.amazon.com/es/architecture/

[155] Arquitectura de PCI DSS en AWS
https://docs.aws.amazon.com/es_es/quickstart/latest/compliance-pci/overview.html

[156] Arquitectura teletrabajo con Amazon AppStream 2.0 BBVA AWS
https://aws.amazon.com/es/blogs/architecture/bbva-helping-global-remote-working-with-amazon-appstream-2-0/

[157] Amazon AppStream 2.0
https://aws.amazon.com/es/appstream2/