Universitat Oberta de Catalunya

uoc.edu

Gestión de Certificados Digitales en el Cloud

Estudiante: Soraya Tena Morell
Plan de Estudios: Máster de Ciberseguridad y Privacidad
Área del Trabajo Final: Seguridad Empresarial

Director del TFM: Angel Linares Zapater
Profesora responsable de la asignatura: Cristina Romero Tris

Fecha de Entrega: Diciembre 2021

C) Copyright

FICHA DEL TRABAJO FINAL

Título del trabajo:	Gestión de Certificados Digitales en el Cloud
Nombre del autor:	Soraya Tena Morell
Nombre del consultor/a:	Ángel Linares Zapater
Nombre del PRA:	Cristina Romero Tris
Fecha de entrega (mm/aaaa):	12/2021
Titulación:	Máster Universitario en Ciberseguridad y Privacidad
Área del Trabajo Final:	Seguridad Empresarial
Idioma del trabajo:	Castellano
Palabras clave	Certificado, Gestión, Cloud

Resumen del Trabajo:

La finalidad de este Trabajo de Fin de Máster es seleccionar, en base a una metodología propia desarrollada y fundamentada, el mejor servicio de gestión de certificados en el Cloud.

El trabajo se centrará en el estudio de los servicios de gestión de certificados que ofrecen las tres plataformas cloud más relevantes de la actualidad: Amazon Web Services, Google Cloud Platform y Azure. Se procederá a investigar de forma individual diferentes servicios, ofrecidos por estas plataformas cloud, para la gestión de certificados.

Una vez finalizada la fase de investigación se llevará a cabo la fase de análisis y desarrollo de la metodología, donde se extraerán las características más relevantes.

En una fase posterior y con el conocimiento adquirido hasta ese momento sobre la gestión de certificados, se aplicará la metodología desarrollada y se extraerán los resultados y conclusiones derivados de la aplicación de la misma.

Abstract:

The purpose of this Master's thesis is to select the best certificate management service in the Cloud.

The essay will focus on studying the certificate management services offered by the three more relevant cloud platforms currently: Amazon Web Services, Google Cloud Platform and Azure. For this purpose, different certificate management services offered by these platforms will be researched.

Once finished the researching phase, the analysis phase will be carried out. In this phase, main characteristics will be extracted and the methodology will be built.

At a later stage, the knowledge about certificate management acquired will be used to apply the developed method, extracting results and conclusions.

Índice

1. Introducción

1.1 Contexto y justificación del Trabajo

El campo de estudio que se pretende abordar en este Trabajo de Fin de Máster (TFM) es la gestión de certificados en entornos Cloud.

El modelo de Centro de Proceso de Datos (CPD) de las empresas está experimentando una fuerte tendencia hacia el uso de proveedores que ofrecen servicios en infraestructura cloud, en detrimento del uso de infraestructura propia de la empresa. Este cambio en el paradigma se debe, principalmente, a la rapidez, escalabilidad y fiabilidad de los servicios que ofrecen las plataformas cloud. Los tiempos de puesta en producción de soluciones se han visto reducidos de forma considerable, especialmente a la hora de provisionar infraestructura. Las empresas pueden tardar meses en provisionar un nuevo servidor en un centro de datos propio, sin embargo consiguen provisionarlo *en unos pocos clicks*, o incluso de forma automática, a través del uso de los servicios que ofrecen estos proveedores.

La fiabilidad que ofrecen los servicios de proveedores cloud está provocando que aumente su uso, lo que desemboca en que, cada vez, se ejecuten cargas de trabajo más sensibles en dichas plataformas. En consecuencia, las empresas necesitan añadir seguridad a estas cargas de trabajo, por lo que están empezando a utilizar los servicios de seguridad que ofrecen los entornos cloud.

La línea de trabajo que suelen seguir estas organizaciones se basa en llegar a obtener, en estas cargas de trabajo en el cloud, un nivel de seguridad lo más similar al que existe en sus propios centros de procesamiento de datos.

Si se piensa, por ejemplo, en una empresa que cuenta con una Infraestructura de Clave Pública (PKI) en su CPD, es muy probable que al migrar cargas de trabajo a entornos Cloud se empiece a plantear la securización de las mismas mediante una PKI. En ese momento, surgen disyuntivas como la siguiente: ¿utilizar los servicios de cómputo que ofrece el cloud para implementar la PKI o aprovechar los servicios gestionados que ofrece el cloud para facilitar la implementación de la misma?

Si se opta por la opción de beneficiarse de los servicios de gestión de certificados que ofrecen los entornos cloud, aparecerán nuevas preguntas:

- ¿Son los servicios de gestión de certificados del cloud tan fiables y seguros como los existentes en el centro de datos de la empresa?
- ¿Tendrá el proveedor cloud acceso a las claves privadas asociadas a mis certificados?
- ¿Puedo importar mis propias claves privadas?
- ¿Se utilizan Autoridades de Certificación (CAs) reconocidas?
- ¿Qué medidas de seguridad se implementan en el end to end de la gestión de certificados?

Estas, y algunas otras cuestiones, se tratarán de abordar en este Trabajo de Fin de Máster.

Se estudiarán diferentes alternativas existentes para la gestión de certificados en las infraestructuras cloud de los proveedores AWS, GCP y Azure, se realizará una comparativa de los diferentes servicios, ventajas y desventajas, y se hará hincapié en los aspectos de seguridad y privacidad ofrecidos por estos servicios.

1.2 Objetivos del Trabajo

Los objetivos generales que se quieren alcanzar en la realización de este TFM se detallan a continuación:

1. Analizar las diferentes opciones de gestión de certificados en AWS y sus características en cuanto seguridad se refiere.
2. Analizar las opciones de gestión de certificados que ofrece GCP y sus características en cuanto seguridad se refiere.
3. Analizar las alternativas de gestión de certificados que ofrece Azure y sus características en cuanto seguridad se refiere.
4. Realizar una comparativa de los servicios de gestión de certificados ofrecidos por AWS, GCP y Azure.

1.3 Enfoque y método seguido

La metodología que se seguirá durante la realización de este trabajo académico será la combinación de metodología cuantitativa y cualitativa.

Será cualitativa porque se investigará acerca de las características de diferentes servicios de gestión de certificados en el cloud. Así mismo, será cuantitativa porque se realizará una comparación de las características detectadas en los servicios de gestión de certificados estudiados. Para obtener dicha valoración cuantitativa se definirá un marco que permita identificar las características que se consideren más relevantes y, en base a esto y a determinadas premisas, se identificará, si es posible[1], el servicio de gestión de certificados más completo. Dicho marco, se realizará una vez analizados los diferentes servicios de gestión de certificados propuestos en el apartado *Planificación del Trabajo* de este documento.

En la siguiente tabla se detalla el método a seguir:

Procedimiento	
1. Fase de Investigación	a. Comprensión del funcionamiento del servicio de gestión de certificados en el cloud. b. Extracción de características relevantes en términos de seguridad.
2. Fase de Comparación	a. Elaboración del marco que permita identificar las características más relevantes, basándose en la investigación previamente realizada. b. Se detectará qué características de las definidas en el marco (punto a) cumple cada servicio y cuáles no. c. Se realizará una valoración final en base al resultado ofrecido al aplicar el marco en el punto b.

Para desarrollar la investigación propuesta a través de la metodología se apoyará tanto en la documentación existente en las plataformas de AWS[2], GCP [3] y Azure[4], como en bibliografía relacionada con dichos proveedores cloud. Algunos ejemplos de la bibliografía que se utilizará son los siguientes:

- **Tracy Pierce, Aravind Kodandaramaiah, Rafael Koike, Alex Rosa (2021).** “AWS Certified Security Specialty All-in-One Exam Guide”.

[1] Llegado el momento, existe la posibilidad de que los servicios a comparar posean características tan similares, que sea más adecuado efectuar una valoración cualitativa que destaque las bondades de cada uno de ellos.
[2] https://docs.aws.amazon.com/
[3] https://cloud.google.com/docs
[4] https://docs.microsoft.com/azure/

- **Karl Ots (2021).** “Azure Security Handbook: A Comprehensive Guide for Defending Your Enterprise Environment”.
- **Mustafa Toroman, Tom Janetscheck (2020).** “Mastering Azure Security”.
- **Dan Sullivan (2019).** “Official Google Cloud Certified Associate Cloud Engineer Study Guide”.

1.4 Planificación del Trabajo

Tareas a realizar para alcanzar los objetivos:

1. Análisis de las características de seguridad del Servicio AWS Certificate Manager.
2. Investigación de otros servicios de AWS que ofrezcan la posibilidad de gestionar certificados.
3. Análisis de las características de seguridad del Servicio GCP Certificate Authority Service.
4. Investigación de otros servicios de GCP que ofrezcan la posibilidad de gestionar certificados.
5. Análisis de las características de seguridad del Servicio Azure Key Vault.
6. Investigación de otros servicios de Azure que ofrezcan la posibilidad de gestionar certificados.
7. Desarrollo de una metodología que permita efectuar la comparativa de las soluciones de gestión de certificados analizadas.
8. Extraer resultados y conclusiones de la aplicación de la metodología.

Planificación temporal de las tareas:

La planificación de tareas y dependencias se adecuará en tiempo y forma a las diferentes PECs que se irán abordando a lo largo de la asignatura. Dado que existen 3 PECs con fecha de inicio y fin ya acordada, a continuación se detallarán los contenidos de cada una de ellas

PEC 2

Fecha de inicio	29/09/2021
Fecha de fin	26/10/2021
Contenido	Tarea 1: revisión del estado del arte.
	Tarea 2: se analizará el servicio AWS Certificate Manager.
	Tarea 3: se investigarán otras posibilidades que pueda ofrecer la nube de AWS para la gestión de Certificados.

PEC 3

Fecha de inicio	27/10/2021
Fecha de fin	23/11/2021
Contenido	Tarea 1: se analizará el servicio GCP Certificate Authority.
	Tarea 2: se investigarán otras posibilidades que pueda ofrecer la nube de GCP para la gestión de certificados.

PEC 4

Fecha de inicio	24/11/2021
Fecha de fin	28/12/2021
Contenido	Tarea 1: se analizará el servicio Azure Key Vault.
	Tarea 2: se investigarán otras posibilidades que pueda ofrecer la nube de Azure para la gestión de certificados.
	Tarea 3:

	- Se elaborará el marco de comparación mencionado en el apartado de este documento en el que se describe la metodología a utilizar y, en base al mismo, se realizará una comparativa de los principales servicios de gestión de certificados de AWS, GCP y Azure que se hayan investigado con anterioridad. - Se extraerán las conclusiones derivadas del trabajo de investigación realizado. En base a un caso de uso, se elegirá el servicio Cloud que se considere más adecuado, apoyándose en la metodología desarrollada.

En la siguiente página se muestra la planificación de las tareas mediante un diagrama de Gantt.

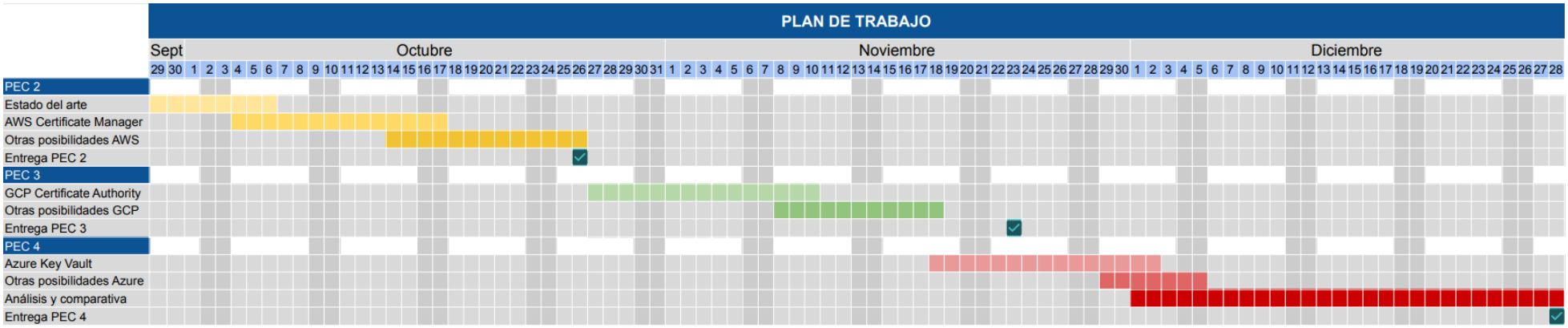

Figura 0: Diagrama de Gantt

Al abordar estas 3 PECs, se deberán haber alcanzado los objetivos fijados en el apartado *Objetivos del trabajo*, dando lugar así, a la finalización del estudio propuesto en este Trabajo de Fin de Máster.

1.5 Breve descripción de los otros capítulos de la memoria

La memoria contará con 3 capítulos: Investigación, Desarrollo Metodología y Conclusiones.

Capítulos	Contenido por apartados
Capítulo 2: Investigación	2.1 Servicios de gestión de Certificados en AWS 2.2 Análisis del servicio AWS Certificate Manager 2.3 Servicios de gestión de Certificados en GCP 2.4 Análisis del servicio GCP Certificate Authority 2.5 Servicios de gestión de Certificados en Azure 2.6 Análisis del servicio Azure Key Vault
Capítulo 3: Metodología y valoración de los servicios analizados	3.1 Se desarrollará la metodología a utilizar 3.2 Aplicación de la metodología a los servicios analizados 3.3 Valoración de los servicios analizados
Capítulo 4: Conclusiones	Conclusiones obtenidas como resultado del trabajo

1.6 Estado del arte

Un certificado permite establecer una comunicación segura entre un cliente o navegador web y un servidor. Esto es posible debido a que existe un tercero de confianza, llamado Autoridad de Certificación (Certification Authority, CA), encargado de asegurar que el cliente y el servidor son quien dicen ser.

La Autoridad de Certificación es la entidad a cargo de la emisión de certificados y, para ello, se apoya en diferentes componentes, formando lo que se conoce como Infraestructura de Clave Pública o PKI por sus siglas en inglés (Public Key Infraestructure). Los diferentes componentes que conforman una PKI se encargan de gestionar, controlar y administrar el proceso de emisión, revocación y validación de certificados digitales. A continuación se detallan cada uno de los elementos que forman parte de la arquitectura de una PKI y una breve descripción de los mismos.

Tal y como ya se ha comentado, la CA es el componente de la PKI que se encarga de emitir el certificado. También se encarga de determinar su validez. Para ello, necesita apoyarse en la Autoridad de Validación (Validation Authority, VA) y la Autoridad de Registro (Registration Authority, RA).

La RA actúa como intermediaria entre el usuario final, que solicita el certificado, y la CA, que lo emite. La función principal de la RA es comprobar la veracidad de la información que el usuario final quiere incluir en el certificado.

Por ejemplo, cuando el usuario final quiere obtener un certificado de servidor para un dominio, la RA se encarga de verificar que el usuario está en posesión del dominio para el que solicita el certificado. Para ello, envía al usuario final un reto (*challenge*) que le permite comprobar que el usuario posee el dominio. Un ejemplo de *challenge* puede ser solicitar al usuario final que modifique un registro DNS, asociado al dominio en cuestión, con la información que la RA le indique.

La solicitud que el usuario final envía a la RA para iniciar el proceso de emisión del certificado se conoce como petición de firma del certificado (Certificate Signing Request, CSR). En esta solicitud el usuario final envía, además de la información que debe contener el certificado, la clave pública que quiere asociar al mismo.

Una vez que la RA ha verificado la información para la que se solicita expedir el certificado, registra la petición y solicita a la CA que expida el certificado. La CA expide un certificado que contiene la clave pública y la información proporcionada por el usuario final, así como la firma del certificado utilizando la

clave privada de la CA. Como resultado, la CA devuelve el certificado firmado al usuario final.

El papel que juega la VA en la arquitectura PKI es el de almacenar un listado de certificados revocados que se conoce como lista de revocación de certificados (Certificates Revocation List, CRL). Para comprobar si un certificado está revocado o para revocarlo, se consultan/modifican las CRLs o se hace uso del protocolo OCSP (Online Certificate Status Protocol).

Llegado a este punto, el usuario final estará en posesión del certificado digital solicitado.

Cuando se trata de un certificado de servidor y se instala en el mismo, este certificado permitirá que la conexión entre el cliente y el servidor se realice mediante el protocolo seguro de la capa de transporte (Transport Layer Security, TLS). Esto se debe a que el navegador del cliente, en el momento de conectarse al servidor en el que se instala el certificado, es capaz de verificar la validez del certificado del servidor. Esto se produce porque todos los navegadores web tienen configuradas un conjunto de CAs en las que confían, por lo tanto, en el momento de establecer el canal TLS son capaces de validar la firma del certificado, siempre que dicha firma fuese realizada por alguna de las CAs cargadas en el navegador.

Una vez validado el certificado del servidor el cliente estará en posesión de la clave pública asociada al certificado del servidor, que podrá utilizar para establecer un canal de comunicación seguro, cifrando con dicha clave todas las peticiones que se realicen al servidor. De manera que, apoyándose en un esquema de cifrado asimétrico, sólo el servidor, que posee la clave privada asociada al certificado del servidor, podrá descifrar las peticiones. No obstante, en la mayoría de los casos se utiliza la clave pública del servidor para cifrar una clave simétrica que genera el cliente y que envía al servidor, con el objetivo de tener una clave simétrica compartida que sólo conocen cliente y servidor, y que se utiliza para cifrar todos los mensajes intercambiados entre los mismos.

No obstante, ¿qué ocurre si la CA que emite el certificado no es una CA de confianza o la seguridad de la PKI no es suficientemente buena? Que la seguridad del certificado emitido no está garantizada y, entre otros, la

comunicación entre el cliente y servidor quedará expuesta a la red, permitiendo que se vulneren aspectos como la integridad y confidencialidad de la misma.

Si la CA no es de confianza o la PKI tiene fallos de seguridad podría ocurrir que no se verifique fehacientemente la información del certificado, y que el cliente no tenga la garantía de conectarse al sitio web que está bajo el dominio indicado. Otra de las vulnerabilidades más comunes podría ser también la exposición de la clave privada que utiliza la CA para firmar los certificados, de manera que un usuario malintencionado podría generar un certificado para un sitio web con fines maliciosos.

Actualmente existen varias autoridades de certificación consideradas de confianza, como pueden ser Digicert o Comodo, que son empresas que se dedican, entre otros, a la emisión de certificados digitales. Adquirir uno de estos certificados tiene un coste asociado. Por otro lado, existe también Let’s Encrypt que, a diferencia de los anteriores, es una Autoridad de Certificación que expide certificados de forma gratuita.

2. Investigación

2.1 Servicios de gestión de Certificados en AWS

AWS pone a disposición de los usuarios 2 servicios que permiten la gestión de certificados a diferentes niveles.

El servicio AWS Certificate Manager (ACM) [4] proporciona la capacidad de gestionar certificados dirigidos a la protección de sitios web o aplicaciones creadas en AWS. Dicho de otro modo, ACM gestiona certificados de servidor.

El servicio AWS Certificate Manager Private Certificate Authority (ACM PCA) [5] proporciona al usuario la capacidad de implementar su propia PKI, proporcionándole una CA privada gestionada por AWS. De esta manera, puede disponer tanto de certificados de tipo servidor como de tipo cliente.

En los siguientes apartados se procederá al análisis de ambos servicios.

2.2 Análisis del servicio AWS Certificate Manager

Amazon Certificate Manager es el servicio de AWS que facilita la creación, almacenamiento y renovación de certificados SSL/TLS X.509 utilizados para proteger sitios web o aplicaciones creadas en AWS. También facilita la gestión de las claves asociadas a dichos certificados.

2.2.1 Características y funcionalidades

ACM proporciona a los usuarios las siguientes capacidades:

- ACM gestiona tanto certificados propios, emitidos por ACM, como certificados importados.
- Los certificados de ACM están validados por dominio (Domain Validated, DV), por lo que el campo *subject* del certificado identifica a un nombre de dominio que está validado. En el momento en el que se solicita el certificado a ACM, se podrá demostrar la posesión del nombre de dominio mediante email o DNS (ver detalles en 2.2.3).
- El periodo de validez de los certificados expedidos por ACM es de 13 meses (395 días).

- ACM gestiona el proceso de renovación de los certificados que expide y los provisiona tras su renovación. Dicho proceso de renovación se puede delegar totalmente en ACM, de manera que se encarga de renovar el certificado de forma automática cuando éste está próximo a su fecha de caducidad, o se puede configurar para que el servicio de ACM notifique por email cuando el certificado esté próximo a expirar (ver detalles en 2.2.4).
- La mayoría de los navegadores confía en los certificados de ACM (Google Chrome, Microsoft Internet Explorer, Microsoft Edge, Mozilla Firefox y Apple Safari). Java también confía en estos certificados.
- Los certificados expedidos por ACM deben incluir al menos un nombre de dominio completo (Fully Qualified Domain Name, FQDN). Además, se pueden incluir nombres de dominio adicionales y utilizar comodines (*), de manera que queden también protegidos los subdominios de primer nivel que estén bajo el dominio al que se asigna el certificado.
- Los algoritmos y tamaño de la clave que pueden ser utilizados por ACM para emitir un certificado a través de las CAs de Amazon son los siguientes:
    - RSA con tamaño de clave de 2048 bit.
    - RSA con tamaño de clave de 4096 bit.
    - Curva elíptica con tamaño de clave de 256 bit.
    - Curva elíptica con tamaño de clave de 384 bit.
- Los certificados expedidos por ACM son gratuitos y de carácter regional, por lo que si se quiere utilizar un certificado para el mismo nombre de dominio en más de una región de AWS, se deberá solicitar o importar un certificado para cada región.
- Los algoritmos y tamaños de clave asociados a certificados importados en ACM son los siguientes:
    - RSA con tamaño de clave de 1024 bit.
    - RSA con tamaño de clave de 2048 bit.
    - RSA con tamaño de clave de 3072 bit.
    - RSA con tamaño de clave de 4096 bit.
    - Curva elíptica con tamaño de clave de 256 bit.

    - Curva elíptica con tamaño de clave de 384 bit.
    - Curva elíptica con tamaño de clave de 512 bit.
- AWS define una serie de cuotas, por defecto, que definen entre otras cosas, el número máximo de certificados emitidos por ACM para una región y cuenta concreta o el número máximo de certificados ACM por año. Estos números se pueden ampliar si el usuario se pone en contacto con el Centro de Soporte de AWS.
- Los usuarios no pueden añadir ni eliminar dominios de un certificado existente, por lo que cada vez que se quiera añadir o eliminar un dominio de un certificado concreto, se deberá solicitar un nuevo certificado y revocar el anterior. Los certificados revocados también cuentan como certificados emitidos, por lo que a la hora de solicitar un nuevo certificado conviene haber realizado un estudio previo para cometer el menor número de fallos posibles y tratar de no superar las cuotas establecidas. Por ejemplo, para los diferentes entornos de pruebas de una aplicación, conviene generar un certificado para el dominio de pruebas y utilizar comodines, de modo que queden también protegidos los subdominios de primer nivel que estén bajo el dominio de pruebas. De esta forma, se evita agotar un gran número de certificados para realizar pruebas en diferentes entornos de test.

2.2.2 Gestión de la seguridad del servicio

2.2.2.1 Protección de claves privadas asociadas a los certificados

ACM utiliza el servicio de Gestión de Claves de AWS (AWS Key Management Service, KMS) para gestionar la clave maestra que se utiliza para cifrar las claves privadas asociadas a los certificados, tanto si se trata de un certificado expedido por ACM, como si se trata de un certificado importado. En este sentido, la única diferencia es que cuando el certificado lo expide ACM, por motivos de seguridad, no permite la descarga del certificado ni de la clave privada asociada al mismo.

A continuación se detalla el proceso que se sigue para cifrar las claves privadas:

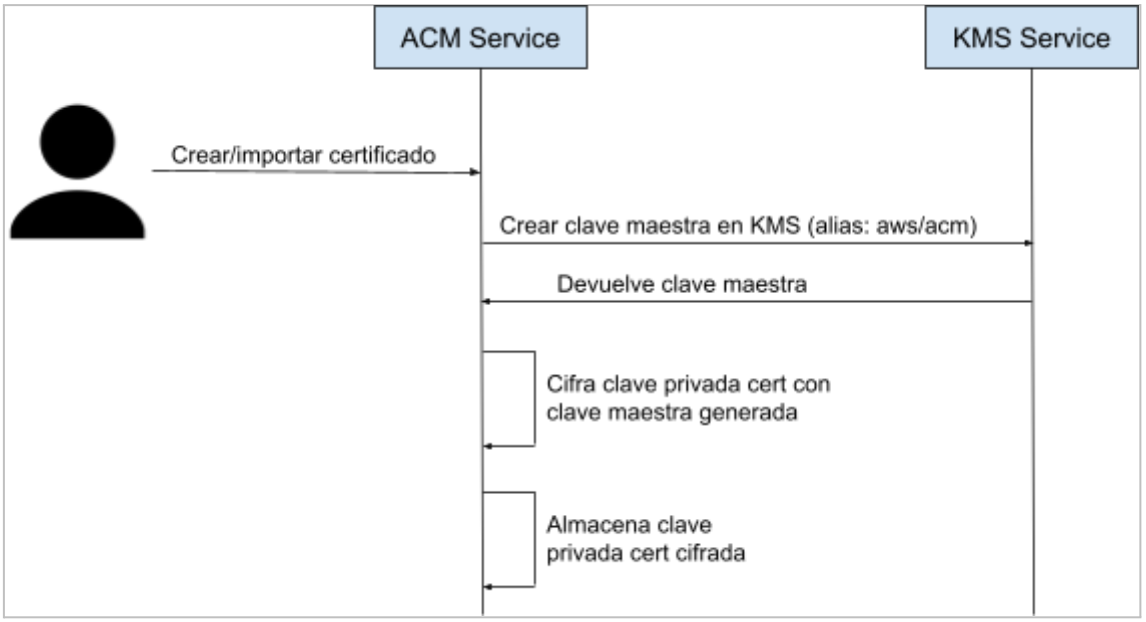

Figura 1. Proceso de creación/importación de certificado

La primera vez que un usuario crea o importa un certificado en una región de AWS del servicio ACM, éste genera, mediante el servicio KMS de AWS, una clave maestra que utilizará para cifrar todas las claves privadas asociadas a los certificados creados o importados en la región concreta del servicio ACM.

De esta manera, ACM almacena siempre cifradas las claves privadas asociadas a los certificados, utilizando una clave maestra para cada región de AWS en la que el usuario utilice el servicio ACM.

Merece la pena indicar que, cada vez que un servicio de AWS se integra con ACM con el objetivo de utilizar alguno de los certificados almacenados, se genera en KMS un tipo de permiso (*grant*) que permite que el servicio integrado con ACM pueda acceder al KMS y utilizar la clave maestra para descifrar la clave privada asociada al certificado. De este modo, la clave privada se transmite cifrada al servicio, lo que aporta protección a la misma cuando viaja por el canal.

Del mismo modo, cuando el certificado gestionado por ACM se desvincula del servicio integrado, se elimina el permiso generado en KMS para que dicho servicio pueda acceder a la clave maestra.

2.2.2.2 Gestión de la Identidad y el Acceso

La gestión de la identidad y el acceso a AWS Certificate Manager se realiza mediante el servicio de gestión de acceso e identidades de Amazon (Amazon Identity and Access Management, IAM). A grandes rasgos, este servicio permite identificar a un usuario a través de los siguientes tipos de identidades:

- Usuario raíz de la cuenta de aws: es el usuario que se genera en el momento de la creación de la cuenta, tiene acceso completo a todos los recursos de la cuenta de AWS y a todos los servicios de AWS. No se recomienda su uso.
- Usuario de IAM: es una identidad a la que se le asignan permisos mediante el uso de políticas, que determinan las acciones que la identidad puede realizar o no. El uso habitual de este tipo de identidades es poder utilizar un usuario de IAM y una contraseña para acceder a las páginas web en las que se encuentran la Consola de Gestión de AWS, los Foros de Debate de AWS o el Centro de Apoyo de AWS. Además, también es posible generar un máximo de dos claves de acceso (*access keys*) asociadas a un usuario de IAM. Cada clave de acceso está formada por un identificador de la clave (*access key ID*) y un secreto (*secret access key*), y se pueden utilizar para acceder a los servicios de AWS de forma programática.
- Rol de IAM: es una identidad a la que se le asignan permisos mediante el uso de políticas, que determinan las acciones que la identidad puede realizar o no. A diferencia de un usuario de IAM, un Rol de IAM no se asigna únicamente a una persona, sino que dicho Rol puede ser asumido por una o varias personas (incluso servicios) de forma temporal, siempre y cuando las mismas tengan permiso para asumirlo. El principal beneficio de asociar permisos a roles en lugar de a usuarios, es que un rol no tiene asociadas credenciales estáticas, sino que obtiene unas credenciales temporales cada vez que el rol va a ser asumido por un usuario. Por lo tanto, evita la gestión y almacenamiento de secretos (credenciales) y facilita la gestión operativa de los usuarios, ya que en lugar de otorgar permisos uno a uno, permite establecer un paradigma con ciertos roles definidos que se asocian al usuario. De esta manera, si se necesita añadir o eliminar algún permiso a los usuarios, basta con que dicho permiso se elimine del rol.

AWS Certificate Manager permite asociar políticas de permisos, sobre los recursos que gestiona (certificados), a usuarios de IAM, grupos y roles, estas políticas se conocen como políticas basadas en la identidad (*identity-based policies*). Dichas políticas definen quién puede acceder al recurso y qué acciones puede ejecutar sobre él, y pueden ser: políticas gestionadas por AWS, políticas gestionadas por el usuario de la cuenta de AWS o políticas en línea.

Políticas gestionadas por AWS

Las políticas gestionadas por AWS son una serie de políticas predefinidas por AWS, de manera que es AWS el encargado de añadir o eliminar permisos a las mismas.

Concretamente, para el servicio ACM, AWS proporciona las siguientes políticas gestionadas:

- Permisos de lectura, *AWSCertificateManagerReadOnly*. Esta política proporciona acceso de sólo lectura sobre cualquier recurso de ACM, por lo que permite a las identidades a las que se le asocia efectuar operaciones que permitan describir, listar y recuperar certificados del servicio ACM. A continuación se muestran los detalles de la política:

```
{
   "Version":"2012-10-17",
   "Statement":{
      "Effect":"Allow",
      "Action":[
         "acm:DescribeCertificate",
         "acm:ListCertificates",
         "acm:GetCertificate",
         "acm:ListTagsForCertificate",
         "acm:GetAccountConfiguration"
      ],
      "Resource":"*"
   }
}
```

Figura 2. Política que habilita el acceso de sólo lectura a ACM

- Acceso completo, *AWSCertificateManagerFullAccess*. Esta política permite realizar cualquier acción sobre cualquier recurso de ACM. A continuación se muestran los detalles de la política:

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "acm:*"
         ],
         "Resource":"*"
      },
      {
         "Effect":"Allow",
         "Action":"iam:CreateServiceLinkedRole",

"Resource":"arn:aws:iam::*:role/aws-service-role/acm.amazon
aws.com/AWSServiceRoleForCertificateManager*",
         "Condition":{
            "StringEquals":{
               "iam:AWSServiceName":"acm.amazonaws.com"
            }
         }
      },
      {
         "Effect":"Allow",
         "Action":[
            "iam:DeleteServiceLinkedRole",
            "iam:GetServiceLinkedRoleDeletionStatus",
            "iam:GetRole"
         ],

"Resource":"arn:aws:iam::*:role/aws-service-role/acm.amazon
aws.com/AWSServiceRoleForCertificateManager*"
```

Figura 3. Política que habilita el acceso completo a ACM

Dado que ACM sólo ofrece 2 políticas, una para acceso de lectura y otra para acceso completo, cualquier usuario que utilice el servicio deberá crear sus propias políticas para conseguir que la gestión del servicio cumpla con los

estándares de segregación de funciones establecidos habitualmente en la gestión de certificados.

Políticas gestionadas por el usuario

Las políticas gestionadas por el usuario de la cuenta de AWS son políticas que él mismo define, pudiendo añadir o eliminar permisos de la misma en cualquier momento.

Políticas en línea

Las políticas en línea también son políticas gestionadas por el usuario, con la diferencia de que éstas se integran directamente en un sólo usuario grupo o rol.

2.2.2.3 Operaciones que se pueden ejecutar sobre el API de ACM

Todas las acciones sobre recursos de ACM que cualquier identidad puede ejecutar sobre el API de ACM se traducen en un permiso. Estas acciones permiten solicitar un certificado, eliminarlo o recuperar los metadatos del mismo. También permite listar los certificados pertenecientes a una cuenta de AWS y obtener el certificado emitido por ACM y su cadena de confianza, así como añadir etiquetas, eliminarlas o listar las etiquetas asociadas a un certificado. A través del API, también es posible importar un certificado de un tercero y solicitar el reenvío del email de validación del dominio.

2.2.3 Emisión y gestión de certificados

El servicio ACM emite certificados de servidor que permiten cifrar las comunicaciones entre el servidor y los clientes que se conectan al mismo. Para solicitar un certificado se deberá haber registrado el dominio previamente.

En el momento en el que se solicita la emisión del certificado, se deberá indicar el/los dominios a proteger. En caso de querer proteger, además del dominio principal, cualquier subdominio de primer nivel del mismo, se deberá añadir un nuevo nombre de dominio al certificado utilizando un comodín. Por ejemplo: **.example.com* protegería los subdominios de primer nivel del dominio *example.com*.

ACM proporciona a los usuarios dos formas de validar el dominio: validación de DNS o validación por correo electrónico.

Si se elige la validación por correo electrónico, AWS Certificate Manager enviará:

- un email de validación a tres direcciones de email registradas en la base de datos WHOIS,
- y otro a cinco direcciones de administración del sistema

para cada nombre de dominio. Por lo tanto, se podrán recibir hasta 8 emails de validación de dominio por cada dominio que se quiera asociar al certificado. Se dispondrá de un periodo de 72 horas para contestar a uno de los hasta 8 mails de validación que se envían para cada dominio.

Sin embargo, para que ACM pueda llevar a cabo esta acción, el usuario, durante el proceso de registro del dominio, deberá configurar su información de contacto para que sea visible, de lo contrario, ACM enviará los correos a las direcciones de email ofuscadas que aparezcan en la información de contacto pública en WHOIS, el usuario nunca recibirá el email y, en consecuencia, será inviable que ACM emita los certificados.

Dado que este método de validación del dominio implica exponer públicamente la información de contacto del dueño del dominio, AWS Certificate Manager proporciona otro método de validación del dominio que podrá llevarse a cabo si el usuario tiene capacidad de editar la configuración de su DNS. Para realizar la validación del dominio mediante DNS, ACM solicitará al usuario que modifique el DNS del dominio para el que quiere solicitar el certificado. Concretamente, le solicitará que añada al dominio un registro CNAME. Este registro CNAME contiene un par *clave-valor* único que sirve como prueba de que el usuario controla el dominio, el valor es un alias que apunta a un dominio de AWS que utilizará ACM para validar la posesión del dominio, y para renovar automáticamente el certificado si así se configura. Se solicitarán tantas modificaciones de registros CNAME como dominios se quieran asociar al certificado. Una vez añadidos los registros al DNS, ACM dispondrá de 72 horas para comprobar que se han modificado los registros CNAME con los valores solicitados, y en el caso de que así sea, dará por probada la posesión del dominio.

Si los certificados son importados por el usuario, el servicio ACM no valida el dominio asociado al mismo, ya que dicha validación habrá sido realizada por la entidad que expidió el certificado que se quiere importar en ACM.

ACM no permite eliminar aquellos certificados que estén siendo utilizados por servicios de AWS, para poder eliminarlos, previamente se debe haber desvinculado el certificado del servicio que lo está utilizando.

2.2.4 Renovación automática de certificados ACM

ACM proporciona a los usuarios la capacidad de renovar automáticamente los certificados que emite, o avisar al usuario de que el certificado está próximo a expirar. Esto dependerá del método de validación de dominio utilizado en el momento de emitir el certificado.

Si en el momento de emitir el certificado se optó por la validación DNS, ACM configura directamente la automatización de la renovación del certificado. Para ello, 60 días antes de que expire el certificado comprueba que está siendo utilizado por un servicio de AWS, que existe un registro DNS válido para el nombre de dominio completo, que el token CNAME configurado en la validación DNS está presente y accesible en el registro DNS y que cada dominio y subdominio presente en el certificado existe en el registro DNS. Si todas las validaciones son correctas, ACM renueva el certificado automáticamente, si no lo son, notifica al dueño del dominio para que realice las acciones manuales necesarias para llevar a cabo la renovación del certificado. Los avisos al dueño del dominio se realizarán 45, 30, 7 y 1 día antes de que expire el certificado.

Si en el momento de emitir el certificado se optó por la validación por correo, ACM no podrá renovar el certificado automáticamente, por lo que enviará un aviso por email avisando de que el certificado está próximo a caducar, y las instrucciones para renovarlo si se desea. El aviso se enviará a las mismas direcciones de correo utilizadas para validar el dominio mediante email. Para evitar acciones manuales para la renovación del certificado, el usuario podrá implementar un proceso que detecte los emails enviados por ACM cuando un

certificado está próximo a expirar, y que realice las acciones que se indican en dicho correo electrónico.

2.2.5 Importar certificados de terceros en ACM

Cuando un usuario quiere importar un certificado en ACM, deberá importar, en formato *.pem*, el certificado, la clave privada -en claro- asociada al mismo y, en caso de que se trate de un certificado no autofirmado, la cadena de confianza del mismo. Además, el certificado importado deberá cumplir los siguientes requisitos:

- Los algoritmos criptográficos y el tamaño de la clave del certificado importado deberá coincidir con uno de los siguientes:
    - RSA con tamaño de clave de 1024 bit.
    - RSA con tamaño de clave de 2048 bit.
    - RSA con tamaño de clave de 3072 bit.
    - RSA con tamaño de clave de 4096 bit.
    - Curva elíptica con tamaño de clave de 256 bit.
    - Curva elíptica con tamaño de clave de 384 bit.
    - Curva elíptica con tamaño de clave de 521 bit.

  Además, se deberá tener en cuenta los algoritmos y tamaños de clave admitidos por los servicios de AWS en los que el certificado va a ser utilizado, dado que no siempre admiten todos los algoritmos y tamaños de clave admitidos por ACM para la importación de certificados.
- Debe ser un certificado de tipo SSL/TLS X.509 versión 3.
- El certificado deberá contener la clave pública asociada al mismo, el nombre de dominio completo (FQDN) o la dirección IP del sitio web, así como información del emisor del certificado.
- El certificado debe ser válido en el momento en el que se importa.
- La clave privada del certificado no debe exceder los 5 KB.

Adicionalmente, los usuarios podrán reimportar un certificado antes de que expire siempre y cuando se mantenga la asociación de los servicios de AWS existentes para el certificado original.

2.2.6 Renovación automática de certificados importados

Los certificados importados no pueden ser renovados de forma automática por AWS Certificate Manager, sin embargo, es posible configurar el servicio de AWS CloudWatch para que avise al usuario cuando el certificado esté próximo a caducar.

2.3 Análisis del servicio AWS Certificate Manager Private Certificate Authority

AWS Certificate Manager Private Certificate Authority (ACM PCA) es un servicio de AWS que permite, a los usuarios de esta plataforma cloud, tener su propia CA privada y gestionada por AWS. Esto significa que los certificados emitidos por dicha CA privada y sus CAs subordinadas podrán utilizarse para cifrar canales de comunicación utilizando TLS, autenticar usuarios, servidores y otros componentes.

Puesto que se trata de una CA Privada, los certificados emitidos por la misma no tendrán validez en ningún entorno de Internet público, ya que no se trata de una CA reconocida. Por este motivo, los certificados emitidos por la CA Privada sólo tendrán validez para autenticar recursos que se encuentren bajo la misma organización de AWS.

2.3.1 Características y funcionalidades

ACM PCA proporciona a los usuarios las siguientes capacidades:

- Al igual que los recursos de ACM, los recursos de ACM PCA son de carácter regional, por lo que si se quiere utilizar CAs privadas en más de una región, será necesario crear las CAs privadas en todas las regiones en las que se necesite.
- Si se utiliza el servicio ACM para solicitar un certificado de PKI privado firmado por la CA privada generada mediante el servicio ACM PCA, dicho certificado se puede asociar a cualquiera de los servicios de AWS con los que se integra el servicio ACM.

- ACM PCA permite integrar CAs privadas en el servicio de Kubernetes gestionado por AWS (AWS EKS), de manera que las carga de trabajo que se ejecutan sobre los nodos del cluster podrían autenticarse utilizando los certificados emitidos por la CA privada.
- Admite los mismos algoritmos de cifrado para la generación de claves privadas que el servicio de ACM.
- Proporciona los siguientes algoritmos para firmar los certificados expedidos:
    - SHA256 con ECDSA.
    - SHA384 con ECDSA.
    - SHA512 con ECDSA.
    - SHA256 con RSA.
    - SHA384 con RSA.
    - SHA512 con RSA.
- El número de certificados y Autoridades de Certificación que te permite utilizar el servicio son limitadas, pudiendo tener un máximo de 200 CAs por región, expidiendo cada una de ellas un máximo de 200 certificados. No obstante, se podría llegar a ampliar si se solicita. Los ratios de peticiones sobre el API de ACM PCA también son limitados.
- El servicio se factura mensualmente en función del número de CAs activas y certificados emitidos.
- ACM PCA permite crear informes de auditoría con la información de los certificados emitidos o revocados por las CAs privadas. Además, permite almacenar dichos informes cifrados en un bucket de S3. Admite tanto el cifrado con claves gestionadas por AWS (AES-256), como el cifrado con claves gestionadas por el usuario utilizando el KMS de AWS.
- La CA raíz podrá contener tantas ramas como desee el usuario, no obstante la jerarquía de PKI no podrá exceder de 5 niveles.
- ACM PCA controla que los certificados emitidos por las CAs privadas no tengan una validez superior en el tiempo a la validez del certificado de la CA. Si se intenta emitir un certificado con validez superior al de la CA que lo expide, el proceso falla.

- ACM PCA proporciona 2 métodos para renovar el certificado de una CA: reemplazar la CA y subordinarla (*chain*) a la misma CA principal o importar un nuevo certificado para la CA. En ningún caso la renovación de estos certificados se realiza de forma automática.
- ACM PCA permite configurar la revocación de los certificados mediante OCSP o CRL.
- ACM PCA permite delegar la renovación automática de los certificados expedidos por sus CA privadas al servicio ACM.

2.3.2 Gestión de la seguridad del servicio

2.3.2.1 Almacenamiento de claves privadas asociadas a los certificados

Las claves privadas asociadas a los certificados emitidos por las CAs privadas se almacenan en HSMs, gestionados por AWS y que cumplen con el estándar FIPS PUB 140-2 (nivel 3 o superior para todas las regiones, excepto para Osaka que es nivel 2 o superior).

2.3.2.2 Gestión de la Identidad y el Acceso

La gestión de la identidad y el acceso, al igual que para el servicio ACM, se realiza en base a identidades (usuarios y roles) del IAM de AWS a las que se pueden asociar políticas (*identity-based policies*) que habilitan acciones sobre los recursos (CAs) de ACM PCA.

Las políticas también pueden ser: políticas gestionadas por AWS, políticas gestionadas por el usuario y políticas en línea. A diferencia del servicio ACM, el servicio ACM PCA sí admite políticas basadas en recursos (*resource-based policies*), de esta manera se posibilita el acceso a las CAs o Certificados desde cuentas diferentes a la cuenta de AWS en la que residen las CAs. Esto se debe a que las políticas basadas en recursos permiten configurar recursos concretos (CAs o certificados) para que puedan ser accedidos por determinados roles o usuarios que no tienen porqué estar asociados a la cuenta de AWS en la que residen las CAs.

Políticas gestionadas por AWS

A continuación se detallan las diferentes políticas gestionadas por AWS:

- Acceso completo, *FullAccess*. Permite el control total del servicio, posibilita ejecutar cualquier acción sobre el API.

- Acceso de lectura, *ReadOnly*. Esta política proporciona acceso de sólo lectura sobre cualquier recurso de ACM PCA.
- Usuario privilegiado, *PrivilegedUser*. Permite emitir y revocar certificados asociados a las CA.
- Usuario, *User*. Permite emitir y revocar certificados emitidos por las CA.
- Auditor, *Auditor*. Tiene acceso de sólo lectura a las operaciones de las APIs y permiso para generar un reporte de auditoría de la CA.

2.3.2.3 Integración con CloudWatch

ACM PCA admite diferentes métricas por defecto de CloudWatch que permiten al usuario lo siguiente:

- Generar una CRL de los certificados emitidos por la CA privada.
- Generar avisos con respecto a la política del bucket en la que se almacena la CRL, cuando dicha política no esté correctamente configurada.
- El tiempo que se tarda en emitir un certificado.
- Métricas que señalan los procesos de emisión de certificados que terminaron de forma exitosa o con fallos.

2.3.2.4 Acceso al API de ACM PCA

El acceso al API de ACM PCA se realiza siempre de forma autenticada y autorizada utilizando alguno de los diferentes mecanismos mencionados en el apartado 2.3.2.2.

A nivel de red, el acceso podrá llevarse a cabo por Internet o utilizando la red privada de AWS mediante la tecnología AWS PrivateLink. El acceso utilizando la red privada de AWS permite al usuario realizar la llamadas desde su cuenta de AWS al VPC endpoint del API de ACM PCA, este acceso conlleva un coste asociado por cada PrivateLink que se habilita en la cuenta de AWS.

2.3.2.5 Almacenamiento de las credenciales de la CA raíz

ACM PCA permite a los usuarios almacenar las credenciales asociadas a la CA raíz tanto en AWS como en las instalaciones del usuario. En caso de que el usuario decida almacenar las credenciales de la CA raíz en sus instalaciones,

en primer lugar, deberá generar una infraestructura PKI en sus instalaciones. En segundo lugar, deberá empezar a configurar ACM PCA y crear, en ACM PCA, una CA que sea subordinada de la CA raíz que se ejecuta en sus instalaciones. De esta manera, la infraestructura PKI generada por ACM PCA formará parte del árbol de la PKI que se ejecuta en las instalaciones del usuario y consecuentemente, el usuario será el custodio de las credenciales asociadas a la CA raíz.

2.4 Servicios de gestión de Certificados en GCP

Google Cloud Platform ofrece a los usuarios un servicio de gestión de certificados de servidor y otro servicio que permite implementar una PKI privada, gestionando tanto certificados cliente como de servidor.

El servicio que ofrece la posibilidad de gestión de certificados de servidor, se ofrece a través de una funcionalidad del servicio Cloud Load Balancing [7], que permite a los usuarios instalar un certificado de servidor en el balanceador. Dicho balanceador actúa como punto de entrada a la infraestructura o software que el usuario tiene alojado en su proyecto de GCP. Instalar un certificado de servidor en dicho balanceador posibilita que las llamadas de cualquier cliente que se conecte a los servicios situados tras el balanceador lo haga mediante un canal cifrado con TLS.

El servicio que ofrece la posibilidad de gestionar tanto certificados cliente como de servidor se trata del servicio Certificate Authority [8] de GCP, que posibilita a los usuarios la creación de una Infraestructura de Clave Pública (PKI) privada.

En los siguientes apartados se detallan las características y funcionalidades de la gestión de certificados de servidor a través del servicio Cloud Load Balancing, y la gestión de certificados cliente y servidor mediante el servicio Certificate Authority.

2.5 Certificados de Servidor en GCP

El servicio de balanceo de carga de GCP (Cloud Load Balancing, CLB) proporciona a sus usuarios la posibilidad de implementar uno o varios certificados SSL en el balanceador, con el objetivo de proporcionar el cifrado de las comunicaciones desde un cliente hacia dicho balanceador. El servicio CLB no soporta autenticación basada en certificado cliente (mTLS).

Los certificados SSL ofrecidos para instalar en el balanceador pueden ser certificados administrados por el usuario o certificados administrados por Google.

2.5.1 Certificados administrados por el usuario

Los certificados administrados por el usuario los obtiene, aprovisiona y renueva el propio usuario. En este caso, GCP admite los siguientes tipos de certificados:

- Certificados de Validación de Dominio (Domain Validation, DV).
- Certificados de Validación de Organización (Organization Validation, OV).
- Certificados de Validación Extendida (Extended Validation, EV).

Queda a elección del usuario la elección de la CA con la que se expide el certificado, pudiendo ser una CA reconocida oficialmente, una CA gestionada por el propio usuario o, incluso, la utilización de certificados autofirmados.

2.5.1.1 Gestión de la Identidad y el Acceso

La gestión de la identidad y el acceso de los usuarios que administran el ciclo de vida de los certificados se controla mediante Roles del IAM de GCP. Este servicio permite identificar a los usuarios mediante los siguientes tipos de identidades (*principals*):

- Cuenta de Google: identidad que representa a una persona que interactúa con los servicios de GCP. Este tipo de usuario se identifica mediante su email asociado.
- Cuenta de servicio: identidad que representa a una aplicación o carga de trabajo.
- Grupo de Google: representa un conjunto de Cuentas de Servicio y/o Cuentas de Google. No es una identidad en sí misma, dado que no tiene credenciales asociadas.
- Cuenta de Google Workspace: representa un grupo virtual de todas las Cuentas de Google que contiene. No es una identidad en sí misma, dado que no tiene credenciales asociadas.

- Dominio de Identidad Cloud: representa un grupo virtual de todas las Cuentas de Google de una organización. No es una identidad en sí misma, dado que no tiene credenciales asociadas.
- Todos los usuarios autenticados: es un identificador que representa todas las Cuentas de Servicio y Usuarios de Internet que se han autenticado con una Cuenta de Google. No es una identidad en sí misma, dado que no tiene credenciales asociadas.
- Todos los usuarios: identifica a cualquiera que esté en Internet. No es una identidad en sí misma, dado que no tiene credenciales asociadas.

Para que el usuario pueda gestionar sus propios certificados (recursos) debe tener asignados ciertos roles o bien pertenecer a un grupo que los tenga. De este modo, GCP facilita el control de acceso a los certificados mediante su IAM, que se basa, a grandes rasgos, en definir políticas de IAM que vinculan una identidad o conjunto de identidades (*principals*) a un rol o roles. Posteriormente, se adjunta la política al recurso sobre el que se quiere controlar el acceso. En este caso, los roles que permiten la creación o modificación de los certificados SSL en un proyecto de GCP son:

- Project Owner.
- Project Editor.
- Compute Security Admin role.
- Compute Network Admin role.
- Un rol personalizado que incluya los permisos *compute.sslCertificates.**, o uno de los siguientes: *compute.targetHttpsProxies.** o *compute.targetSslProxies.**.

2.5.1.2 Importar certificados

Los certificados y la clave privada asociada al mismo, se deberán importar en formato *.pem*. Además, la clave privada se importará en claro y se almacenará cifrada en GCP, siguiendo un formato de cifrado propio de esta nube. El algoritmo criptográfico y el tamaño de la clave privada deberá ser uno de los siguientes:

- RSA con tamaño de clave de 2048 bit.

- ECDSA con tamaño de clave de 256 bit.

GCP garantiza que la clave privada asociada al certificado se almacena de forma segura y no se muestra a los usuarios con permisos mediante la Consola de GCP, la utilidad de *gcloud* ni vía API.

2.5.1.3 Renovar, rotar o reemplazar certificados

Los certificados importados por el usuario no pueden renovarse, rotarse o reemplazarse de forma automática.

2.5.2 Certificados administrados por Google

Los certificados administrados por Google son certificados de Validación de Dominio que obtiene, administra y renueva de forma automática GCP. Por lo tanto, no se pueden utilizar para demostrar la identidad del individuo u organización asociado al certificado. Estos certificados soportan comodines en el campo Common Name del certificado, de modo que protejan los subdominios de primer nivel que estén bajo el dominio al que se asocia el certificado.

Estos certificados admiten hasta 100 dominios asociados al mismo y no es posible aumentar esta cuota.

La validez de estos certificados es de 90 días.

2.5.2.1 Gestión de la Identidad y el Acceso

La gestión de la identidad y el acceso a certificados administrados por Google es idéntica a la gestión de la identidad y el acceso cuando los certificados son administrados por el usuario, se utilizan los mismos roles y permisos.

2.6 Análisis del servicio GCP Certificate Authority

El servicio Certificate Authority de GCP permite a los usuarios crear su propia infraestructura de clave pública (PKI), ya que ofrece capacidades de creación y gestión de CAs privadas.

Puesto que se trata de una CA privada, los certificados emitidos por la misma no tendrán validez en ningún entorno de Internet público, ya que no se trata de una CA reconocida.

2.6.1 Características y funcionalidades

Certificate Authority proporciona a los usuarios las siguientes capacidades:

- Tiene 2 modelos de operación: DevOps y Enterprise. El modelo DevOps está orientado a la emisión de un alto volumen de certificados por segundo con un tiempo de vida corto; el modelo Enterprise ofrece un volumen de emisión de certificados menor y un tiempo de vida más largo. Las principales diferencias entre ambos es que el modelo DevOps no admite que las claves de la CA sean gestionadas por el usuario mediante el KMS de GCP ni tiene soporte para listar, describir y revocar los certificados emitidos, y el modelo Enterprise sí admite ambas opciones. En cualquiera de los dos modelos de operación el número máximo de certificados emitidos por segundo es de 100, siendo 7 certificados por segundo para cada CA del modelo Enterprise y 25 certificados por segundo para cada CA del modelo DevOps.
- La gestión de las claves que se utilizan para firmar los certificados y las listas de revocación (CRLs) puede ser realizada por el usuario o por Google. En cualquiera de los casos, se utilizará el servicio KMS de GCP.
- En caso de que la gestión de claves sea realizada por Google, el usuario podría elegir el algoritmo y el tamaño de la clave asociadas a la CA en el momento de su creación.
- La gestión del almacenamiento del certificado de la CA y las CRLs publicadas por la CA puede ser realizada por el usuario o por Google.
- Las CA encargadas de la emisión de certificados se pueden configurar asignándole políticas de emisión de los mismos, con el objetivo de establecer un control sobre el contenido de algunos campos de los certificados emitidos. Por ejemplo, el tiempo de vida del certificado o el algoritmo y longitud de la clave que debe tener la clave pública que se quiere asociar al certificado (sólo podrá ser una clave RSA o Curva Elíptica).

- Las CAs generadas bajo el ámbito del servicio Certificate Authority pueden tener como CA raíz una CA externa al servicio Certificate Authority.

2.6.2 Grupo de CA

Un grupo de CA es una colección de múltiples CAs que tienen en común:

- Una política de IAM.
- Una política de emisión de certificados.
- Están ubicadas en la misma región.
- Comparten modelo de operación (DevOps o Enterprise).

2.6.3 Emisión de certificados por un Grupo de CA

El servicio Certificate Authority proporciona 2 métodos para emitir un certificado:

- El usuario genera su par de claves público/privada, genera el CSR y lo presenta a la CA.
- El usuario solicita a la CA que expida un certificado asociado a un par de claves público/privada. En este caso la CA se encarga además de generar las claves asociadas al certificado.

Sin embargo, Certificate Authority sólo valida que el usuario está en posesión de la clave privada si la solicitud se realiza mediante un CSR en formato PKCS#10, de acuerdo al RFC 2986.

2.6.4 Revocar Certificados emitidos por un Grupo de CA

El servicio Certificate Authority permite revocar certificados mediante la publicación de su número de serie y motivo de revocación en las listas de revocación (CRLs). Esta opción sólamente está disponible en el modelo de operación Enterprise, habiendo un límite de 500.000 certificados revocados no vencidos por CRL.

Para que la revocación de certificados funcione se debe habilitar de forma explícita en un grupo de CA para que ésta publique las CRLs. Se debe tener en cuenta que, cualquier certificado emitido previo a la activación de la funcionalidad de revocación en el grupo de CA, no tendrá la extensión necesaria para realizar comprobaciones de revocación. Dicha extensión es una URL a la CRL que se incluye en el certificado en el momento de su emisión y se conoce como punto de distribución CRL (CRL Distribution Point, CDP).

2.6.5 Gestión de la Identidad y el Acceso

La gestión de la identidad y el acceso al servicio Certificate Authority se controla mediante el IAM de GCP, tal como se explicó en el apartado 2.5.2.1.

En particular, Certificate Authority posee una serie de Roles predefinidos con el objetivo de dotar a los usuarios de una segregación de permisos óptima. A continuación se lista cada uno de los roles y sus permisos asociados.

- Auditor, *privateca.auditor*. Este rol dota de permisos de lectura sobre todos los recursos del servicio y permite recuperar y listar las propiedades asociadas a un grupo de CA, CA, certificados, listas de revocación, políticas de IAM y proyectos. A continuación se muestras los permisos asociados al rol:

Figura 4. Permisos asociados al rol de Auditor

- Solicitante de certificado, *certificateRequester*. Este rol permite a la identidad a la que se asocia solicitar certificados a un grupo de CA. Sólo tiene asociado el permiso *privateca.certificates.create*.
- Solicitante de certificado de carga de trabajo, *privateca.workloadCertificateRequester*. Permite solicitar certificados con la identidad del llamante. Sólo tiene asociado el permiso *privateca.certificates.createForSelf*.
- Administrador de certificados, *privateca.certificateManager*. Posee los permisos asociados al rol de solicitante de certificado y auditor.
- Usuario de plantilla. Puede leer, listar y utilizar las plantillas de certificado existentes. Posee los siguientes permisos asociados:

```
privateca.
certificateTemplates.get
privateca.
certificateTemplates.list
privateca.
certificateTemplates.use
```

Figura 5. Permisos asociados al rol Usuario de plantilla

- Administrador de operaciones, *privateca.caManager*. Puede crear, actualizar y eliminar CAs y grupos de CA, revocar certificados y crear *buckets* de Cloud Storage. También posee todos los permisos asignados al rol de Auditor. A continuación se listan los permisos asociados a este rol:

```
All permissions from roles/
privateca.auditor, plus:
privateca.certificates.update
privateca.caPools.create
privateca.caPools.delete
privateca.caPools.update
privateca.
certificateAuthorities.create
privateca.
certificateAuthorities.delete
privateca.
certificateAuthorities.update
privateca.
certificateRevocationLists.
update
privateca.
certificateTemplates.create
privateca.
certificateTemplates.delete
privateca.
certificateTemplates.update
privateca.certificates.update
privateca.operations.cancel
privateca.operations.delete
resourcemanager.projects.get
resourcemanager.projects.list
storage.buckets.create
```

Figura 6. Permisos asociados al rol Administrador de operaciones

- Administrador, *privateca.admin*. Este rol hereda todos los permisos del rol de Administrador de certificados y Administrador de operaciones.

Adicionalmente, puede realizar todas las acciones posibles sobre el servicio Certificate Authority como por ejemplo configurar políticas de IAM para un grupo de CA o plantillas de certificados. A continuación se listan los permisos asociados al rol de Administrador:

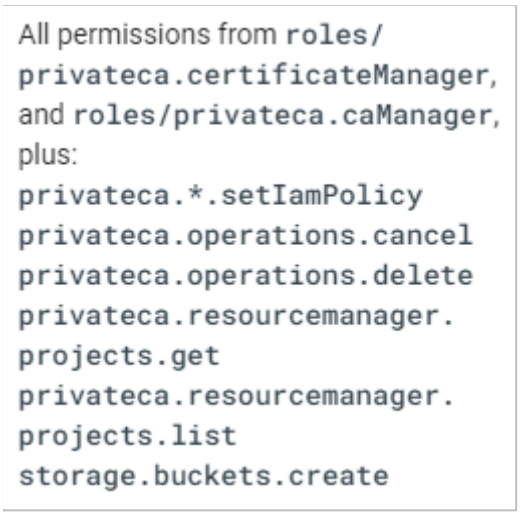

Figura 7. Permisos asociados al rol Administrador

2.7 Servicios de gestión de Certificados en Azure

Azure no posee un servicio exclusivo para la gestión de certificados ni para la implementación de una PKI privada. Sin embargo, el servicio de almacenamiento seguro de Azure Key Vault puede utilizarse para gestionar certificados.

Merece la pena mencionar que Azure, de forma similar a la nube de GCP, también ofrece funcionalidades de gestión de certificados de servidor en servicio como: Application Gateway [9], App Service [10], SQL Server [11] y otros. No obstante, dado que la funcionalidad también se ofrece de forma centralizada a través del servicio Key Vault, y para limitar el alcance del análisis, el estudio se centrará en el análisis de Key Vault como servicio para la gestión de certificados.

2.8 Análisis del servicio Azure Key Vault

El servicio Azure Key Vault ofrece al usuario la capacidad de gestionar secretos claves y/o certificados. Dado que el alcance de este Trabajo es la gestión de certificados, nos centraremos en el análisis de Key Vault (KV) como un servicio

de gestión de certificados, apoyándonos en las capacidades de almacenamiento para claves y secretos que nos sean de utilidad a la hora de gestionar los certificados.

Azure ofrece 2 capas diferentes para este servicio que difieren principalmente en lo siguiente:

- Capa estándar: ofrece protección para claves, secretos y certificados utilizando capacidades de cifrado mediante software, a través de vaults.
- Capa premium: ofrece protección de claves utilizando capacidades de cifrado mediante hardware, a través del uso de un HSM.

En un escenario en el que se utilice este servicio para la gestión de certificados podría tener sentido utilizar Key Vault combinando las 2 capas de la siguiente manera: utilizar la capa estándar para el almacenamiento de los certificados, y utilizar la capa premium para almacenar la clave privada asociada a los certificados.

2.8.1 Características y funcionalidades

Key Vault proporciona a los usuarios las siguientes capacidades:

- KV tiene la capacidad de versionar la información almacenada, de manera que a cada objeto almacenado le asigna una URL y un identificador únicos. Así, cuando se crea un nuevo objeto con el nombre de uno ya existente, Azure le asigna al objeto una nueva versión con un identificador y URL únicos.
- Admite certificados autofirmados y certificados emitidos por CAs reconocidas.
- KV se integra con DigiCert y GlobalSign para emitir certificados SSL de validación de dominio (DV) o de validación extendida (EV).
- Permite al usuario generar certificados mediante Key Vault, utilizando las CAs integradas de DigiCert o GlobalSign o generando certificados autofirmados. También permite importar en KV certificados emitidos por terceros.
- Todos los certificados que se almacenan en Key Vault tienen una política asociada en la que se indica la información necesaria para que KV

pueda gestionar el ciclo de vida del certificado. A continuación se detalla parte de la información que contiene la política:

    - Propiedades utilizadas para solicitar el certificado X509, como por ejemplo el *subject name* o el *subject alternate names*.
    - Propiedades de la clave: tipo de clave, longitud, si se puede exportar o no, o si se puede reutilizar la clave cuando se renueve el certificado.
    - Acciones: permite configurar acciones relativas al ciclo de vida del certificado, como por ejemplo avisar al propietario o renovar el certificado automáticamente cuando este está a punto de caducar.
    - Emisor: información acerca del emisor del certificado.
    - Atributos asociados a la política.

- Los algoritmos y tamaño de la clave soportados por Key Vault se listan a continuación:
    - RSA con tamaños de clave de 2048, 3072 y 4096 bits.
    - Curva Elíptica con tamaños de clave de 256, 384 y 521 bits.

2.8.2 Almacenamiento de secretos, claves y certificados

Es necesario conocer si se opta por el almacenamiento hardware o software, ya que en función de esto, el servicio proporciona diferentes niveles de seguridad. No obstante, en cualquiera de estos dos casos, el servicio está diseñado para que Azure no pueda ver ni extraer la información almacenada.

A continuación se detallan las características ofrecidas por cada tipo de almacenamiento.

2.8.2.1 Almacenamiento mediante software (vaults)

El almacenamiento mediante software está protegido por Azure, que utiliza algoritmos y longitudes de clave estándar de la industria para proteger la información almacenada cifrada.

2.8.2.2 Almacenamiento mediante hardware (HSM)

El almacenamiento mediante hardware permite al usuario importar o generar las claves en HSMs de nCipher[5], gestionados por Azure, de tipo FIPS 140-2 nivel 3. Cada HSM está aislado del resto de HSM utilizados por otras cuentas de Azure. Además, permite utilizar herramientas de nCipher en caso de que se necesiten migrar las claves desde HSMs propios del usuario al servicio de Azure Key Vault.

2.8.3 Gestión de la identidad y el acceso, autenticación y autorización

2.8.3.1 Identidad y acceso

Azure Key Vault proporciona autenticación en el acceso a los secretos mediante Azure Active Directory (AD), que es el servicio de Azure que gestiona las identidades para los recursos y usuarios de Azure. Este servicio abstrae al usuario de la gestión de identidades. A continuación se listan el tipo de identidades (*security principals*) existentes en Azure AD:

- Usuario: es un objeto que identifica a un individuo que tiene un perfil en AD.
- Grupo: es un objeto que identifica a un conjunto de individuos existentes en AD. Cuando se otorga un permiso o un rol sobre un grupo, todas las personas pertenecientes al mismo obtienen dicho permiso o rol.
- Service principal: es un objeto que identifica a una aplicación o servicio.

Con respecto la obtención de una identidad para una aplicación o servicio, es decir, cuando se quiere obtener un *service principal*, Azure AD proporciona 2 formas de adquirirlo:

- Utilizando una identidad asignada a un sistema. Este tipo de *service principal* posee las siguientes características:

[5] Solución de mercado adquirida por la empresa Entrust en 2019: https://www.entrust.com/digital-security/hsm/products/nshield-hsms?nc_sfid=7013a000002pZaK&gclid=Cj0KCQiA_JWOBhDRARIsANymNOZyls30vFlJ3pPrXwsoLWQiI4Ex9Kaye9GJKgrzVUcPKeDD_nz8fCwaAu8GEALw_wcB

    - Está ligado al sistema/aplicación desde el momento en el que se crea, por lo que cuando el sistema/aplicación se elimina, la identidad también.
    - No tiene credenciales asociadas, en su lugar, se utiliza la identidad para obtener un token de AD en el momento en el que necesitan autenticarse ante un recurso de Azure.
- Utilizando una identidad asociada a un usuario. Este tipo de *service principal* implica dar de alta a la aplicación/sistema en AD, por lo que, en la práctica sería una identidad de tipo “Usuario”. Por este motivo, las identidades de tipo *usuario* pueden asignarse tanto a individuos como a sistemas/aplicaciones. Las principales características de las identidades asociadas a un usuario son:
    - Son independientes al ciclo de vida del sistema/aplicación, por lo que si el sistema que tiene asociada esta identidad se elimina, la identidad seguirá existiendo.
    - Sí tienen credenciales asociadas, por lo que se deberá asegurar un correcto almacenamiento y gestión de las mismas.

No todos los servicios/aplicaciones admiten identidades asignadas a sistemas, no obstante se optará por este método de identificación siempre que sea posible, ya que facilita la gestión del ciclo de vida de la identidad y abstrae al usuario de la gestión y almacenamiento de la credencial.

Además de la identificación utilizando el servicio de AD, Key Vault también admite autenticación mediante una entidad de servicio y un certificado o secreto asociado, pero este tipo de autenticación no se recomienda, por lo que no se profundizará en la misma.

2.8.3.2 Autenticación

Cualquier identidad, individuo o sistema/aplicación, autenticada en AD obtendrá como resultado un token OAuth2 (*access token*) con el que podrá identificarse en los servicios de Azure, y mediante el cual podrá llevarse a cabo el proceso de autorización.

2.8.3.3 Autorización

Hasta este momento, tanto si se utiliza el almacenamiento en vault como si se utiliza el almacenamiento en HSM, los mecanismos de identificación y autenticación que se proporcionan son los que se acaban de comentar. Sin embargo, cuando se trata de autorización conviene diferenciar el almacenamiento en vault del almacenamiento en HSM, puesto que no comparten el mismo funcionamiento.

Mecanismos de autorización en vault

Se proporcionan 2 métodos para el control del acceso a los secretos almacenados:

- Control de acceso basado en roles (RBAC): existen roles predefinidos por Azure y el usuario puede crear los suyos propios.
- Control de acceso basado en políticas: el usuario puede crear políticas de acceso para asociarlas a identidades de Azure. En el caso de Key Vault, dichas políticas de acceso están formadas por la identidad a la que se le otorga y el conjunto de acciones que puede ejecutar sobre Key Vault.

El primero de ellos, RBAC, se puede utilizar para gestionar el plano de operación del Vault (por ejemplo, crear, eliminar o modificar vaults) y para controlar el acceso a la información almacenada (plano de datos); mientras que el segundo, basado en políticas, sólo se puede utilizar para controlar el acceso a la información almacenada.

A continuación se describen los roles predefinidos en Azure y sus acciones asociadas:

- Key vault administrator: puede ejecutar cualquier operación sobre el plano de datos de un vault.

Actions	Description
Microsoft.Authorization/*/read	Read roles and role assignments
Microsoft.Insights/alertRules/*	Create and manage a classic metric alert
Microsoft.Resources/deployments/*	Create and manage a deployment
Microsoft.Resources/subscriptions/resourceGroups/read	Gets or lists resource groups.
Microsoft.Support/*	Create and update a support ticket
Microsoft.KeyVault/checkNameAvailability/read	Checks that a key vault name is valid and is not in use
Microsoft.KeyVault/deletedVaults/read	View the properties of soft deleted key vaults
Microsoft.KeyVault/locations/*/read	
Microsoft.KeyVault/vaults/*/read	
Microsoft.KeyVault/operations/read	Lists operations available on Microsoft.KeyVault resource provider
NotActions	
none	
DataActions	
Microsoft.KeyVault/vaults/*	
NotDataActions	
none	

Figura 8: acciones asociadas al rol *Key vault administrator*

- Key vault certificates officer: puede efectuar cualquier acción sobre los certificados de un vault, excepto gestionar permisos.

Actions	Description
Microsoft.Authorization/*/read	Read roles and role assignments
Microsoft.Insights/alertRules/*	Create and manage a classic metric alert
Microsoft.Resources/deployments/*	Create and manage a deployment
Microsoft.Resources/subscriptions/resourceGroups/read	Gets or lists resource groups.
Microsoft.Support/*	Create and update a support ticket
Microsoft.KeyVault/checkNameAvailability/read	Checks that a key vault name is valid and is not in use
Microsoft.KeyVault/deletedVaults/read	View the properties of soft deleted key vaults
Microsoft.KeyVault/locations/*/read	
Microsoft.KeyVault/vaults/*/read	
Microsoft.KeyVault/operations/read	Lists operations available on Microsoft.KeyVault resource provider
NotActions	
none	
DataActions	
Microsoft.KeyVault/vaults/certificatecas/*	
Microsoft.KeyVault/vaults/certificates/*	
NotDataActions	
none	

Figura 9: acciones asociadas al rol *Key vault certificates officer*

- Key vault crypto officer: permite efectuar cualquier acción sobres las claves excepto gestionar los permisos.

Actions	Description
Microsoft.Authorization/*/read	Read roles and role assignments
Microsoft.Insights/alertRules/*	Create and manage a classic metric alert
Microsoft.Resources/deployments/*	Create and manage a deployment
Microsoft.Resources/subscriptions/resourceGroups/read	Gets or lists resource groups.
Microsoft.Support/*	Create and update a support ticket
Microsoft.KeyVault/checkNameAvailability/read	Checks that a key vault name is valid and is not in use
Microsoft.KeyVault/deletedVaults/read	View the properties of soft deleted key vaults
Microsoft.KeyVault/locations/*/read	
Microsoft.KeyVault/vaults/*/read	
Microsoft.KeyVault/operations/read	Lists operations available on Microsoft.KeyVault resource provider
NotActions	
none	
DataActions	
Microsoft.KeyVault/vaults/keys/*	
NotDataActions	
none	

Figura 10: acciones asociadas al rol *Key vault crypto officer*

- Key vault crypto service encryption user: permite leer los metadatos de una clave y realizar operaciones de encapsulado/desencapsulado de claves.

Actions	Description
Microsoft.EventGrid/eventSubscriptions/write	Create or update an eventSubscription
Microsoft.EventGrid/eventSubscriptions/read	Read an eventSubscription
Microsoft.EventGrid/eventSubscriptions/delete	Delete an eventSubscription
NotActions	
none	
DataActions	
Microsoft.KeyVault/vaults/keys/read	List keys in the specified vault, or read properties and public material of a key. For asymmetric keys, this operation exposes public key and includes ability to perform public key algorithms such as encrypt and verify signature. Private keys and symmetric keys are never exposed.
Microsoft.KeyVault/vaults/keys/wrap/action	Wraps a symmetric key with a Key Vault key. Note that if the Key Vault key is asymmetric, this operation can be performed by principals with read access.
Microsoft.KeyVault/vaults/keys/unwrap/action	Unwraps a symmetric key with a Key Vault key.
NotDataActions	
none	

Figura 11: acciones asociadas al rol *Key vault crypto service encryption user*

- Key vault crypto user: permite realizar operaciones criptográficas utilizando las claves.

Actions	Description
none	
NotActions	
none	
DataActions	
Microsoft.KeyVault/vaults/keys/read	List keys in the specified vault, or read properties and public material of a key. For asymmetric keys, this operation exposes public key and includes ability to perform public key algorithms such as encrypt and verify signature. Private keys and symmetric keys are never exposed.
Microsoft.KeyVault/vaults/keys/update/action	Updates the specified attributes associated with the given key.
Microsoft.KeyVault/vaults/keys/backup/action	Creates the backup file of a key. The file can used to restore the key in a Key Vault of same subscription. Restrictions may apply.
Microsoft.KeyVault/vaults/keys/encrypt/action	Encrypts plaintext with a key. Note that if the key is asymmetric, this operation can be performed by principals with read access.
Microsoft.KeyVault/vaults/keys/decrypt/action	Decrypts ciphertext with a key.
Microsoft.KeyVault/vaults/keys/wrap/action	Wraps a symmetric key with a Key Vault key. Note that if the Key Vault key is asymmetric, this operation can be performed by principals with read access.
Microsoft.KeyVault/vaults/keys/unwrap/action	Unwraps a symmetric key with a Key Vault key.
Microsoft.KeyVault/vaults/keys/sign/action	Signs a message digest (hash) with a key.
Microsoft.KeyVault/vaults/keys/verify/action	Verifies the signature of a message digest (hash) with a key. Note that if the key is asymmetric, this operation can be performed by principals with read access.
NotDataActions	
none	

Figura 12: acciones asociadas al rol *Key vault crypto user*

- Key vault reader: permite leer los metadatos del vault y los certificados claves y secretos contenidos en el mismo. No permite leer información sensible tal como el contenido de los secretos o las claves.

Actions	Description
Microsoft.Authorization/*/read	Read roles and role assignments
Microsoft.Insights/alertRules/*	Create and manage a classic metric alert
Microsoft.Resources/deployments/*	Create and manage a deployment
Microsoft.Resources/subscriptions/resourceGroups/read	Gets or lists resource groups.
Microsoft.Support/*	Create and update a support ticket
Microsoft.KeyVault/checkNameAvailability/read	Checks that a key vault name is valid and is not in use
Microsoft.KeyVault/deletedVaults/read	View the properties of soft deleted key vaults
Microsoft.KeyVault/locations/*/read	
Microsoft.KeyVault/vaults/*/read	
Microsoft.KeyVault/operations/read	Lists operations available on Microsoft.KeyVault resource provider
NotActions	
none	
DataActions	
Microsoft.KeyVault/vaults/*/read	
Microsoft.KeyVault/vaults/secrets/readMetadata/action	List or view the properties of a secret, but not its value.
NotDataActions	
none	

Figura 13: acciones asociadas al rol *Key vault reader*

- Key vault secrets officer: permite realizar cualquier acción sobre los secretos excepto gestionar los permisos.

Actions	Description
Microsoft.Authorization/*/read	Read roles and role assignments
Microsoft.Insights/alertRules/*	Create and manage a classic metric alert
Microsoft.Resources/deployments/*	Create and manage a deployment
Microsoft.Resources/subscriptions/resourceGroups/read	Gets or lists resource groups.
Microsoft.Support/*	Create and update a support ticket
Microsoft.KeyVault/checkNameAvailability/read	Checks that a key vault name is valid and is not in use
Microsoft.KeyVault/deletedVaults/read	View the properties of soft deleted key vaults
Microsoft.KeyVault/locations/*/read	
Microsoft.KeyVault/vaults/*/read	
Microsoft.KeyVault/operations/read	Lists operations available on Microsoft.KeyVault resource provider
NotActions	
none	
DataActions	
Microsoft.KeyVault/vaults/secrets/*	
NotDataActions	
none	

Figura 14: acciones asociadas al rol *Key vault secrets officer*

- Key vault secrets user: permite leer el contenido de los secretos.

Actions	Description
none	
NotActions	
none	
DataActions	
Microsoft.KeyVault/vaults/secrets/getSecret/action	Gets the value of a secret.
Microsoft.KeyVault/vaults/secrets/readMetadata/action	List or view the properties of a secret, but not its value.
NotDataActions	
none	

Figura 15: acciones asociadas al rol *Key vault secrets user*

Mecanismos de autorización en HSM

Cuando se utiliza un HSM gestionado por Azure, la autorización se realiza siempre atendiendo a roles mediante RBAC. No obstante, dichos roles son

gestionados por Azure o por el propio HSM dependiendo de si se trata de un acceso a la información almacenada o de un acceso de operación del HSM.

- El acceso para operar el HSM se controla mediante Roles (RBAC) gestionados por Azure. Existen varios roles predefinidos por Azure y también se otorga al usuario la capacidad de crear sus propios roles.
- El acceso a la información almacenada en el HSM se controla mediante Roles (RBAC) gestionados por el HSM.

De esta forma, en el momento de la creación del HSM se proporciona un listado de administradores de la información almacenada en el HSM, y sólo dichos administradores tienen capacidad de otorgar permiso de acceso a la información a otros usuarios. Este acceso se otorga mediante roles gestionados por el HSM, por lo que Azure no tiene ninguna capacidad de actuar sobre ellos y el plano de operación queda totalmente segregado del plano de acceso a la información.

A continuación se describen los roles predefinidos a nivel HSM:

- Managed HSM administrator: puede realizar cualquiera de las acciones relacionadas con el dominio de seguridad[6], la gestión de roles, copias de seguridad y restauraciones. Este rol no puede efectuar ninguna acción sobre las claves.
- Managed HSM crypto officer: puede ejecutar cualquier acción de gestión de permisos, recuperar, exportar o eliminar permanentemente claves.
- Managed HSM crypto user: permite ejecutar cualquier acción relativa a la gestión de claves excepto recuperarlas, exportarlas o eliminarlas de forma permanente.
- Managed HSM policy administrator: permite crear y eliminar asignaciones a roles.
- Managed HSM crypto auditor: otorgar permiso para leer los atributos de las claves, pero no para utilizarlos.
- Managed HSM crypto service encryption user: otorga permiso a un servicio de cifrado para utilizar una clave.
- Managed HSM backup: otorga permiso para realizar una copia de

[6] Conjunto de credenciales core del HSM necesarias para recuperar el HSM gestionado en caso de desastre

seguridad de una clave o de todo el HSM.

Con respecto a los roles predefinidos a nivel de Azure para el plano de operación, únicamente se tiene el rol *Key vault contributor*, puesto que es el único rol predefinido que actúa sobre el plano de operación. A continuación se proporciona la descripción del rol y sus acciones asociadas.

- Key vault contributor: puede gestionar los vaults pero no permite asignar roles en el sistema de RBAC de Azure, tampoco permite acceder a secretos, claves o certificados.

Actions	Description
Microsoft.Authorization/*/read	Read roles and role assignments
Microsoft.Insights/alertRules/*	Create and manage a classic metric alert
Microsoft.KeyVault/*	
Microsoft.Resources/deployments/*	Create and manage a deployment
Microsoft.Resources/subscriptions/resourceGroups/read	Gets or lists resource groups.
Microsoft.Support/*	Create and update a support ticket
NotActions	
Microsoft.KeyVault/locations/deletedVaults/purge/action	Purge a soft deleted key vault
Microsoft.KeyVault/hsmPools/*	
Microsoft.KeyVault/managedHsms/*	
DataActions	
none	
NotDataActions	
none	

Figura 16: acciones asociadas al rol *Key vault contributor*

2.8.4 Acceso al API de Key Vault

El acceso al API de Key Vault se realiza siempre de forma autenticada y autorizada mediante alguno de los mecanismos expuestos en el apartado 2.8.2.

A nivel de red, el acceso se encuentra habilitado por defecto para que se lleve a cabo por Internet, no obstante, se puede configurar para que sólamente pueda ser accedido desde ciertos rangos de IPs, redes privadas o para que el

acceso se limite a peticiones provenientes de la red interna de Azure mediante endpoints privados.

2.8.5 Monitorización

Azure Key Vault proporciona la capacidad de monitorizar el acceso a las claves, certificados y secretos almacenados habilitando los logs del vault con el objetivo de: guardarlos, enviarlos a un sistema de procesamiento de eventos o al servicio de logs de Azure (Azure Monitor). Si se elige la opción de almacenarlos se crea de forma automática un contenedor para estos logs, *insights-logs-auditevent*, en una cuenta de almacenamiento de Azure.

Si se opta por la opción de almacenar las claves criptográficas en un HSM gestionado por Azure, también es posible monitorizar los accesos al HSM y almacenar dichos logs en una cuenta de almacenamiento de Azure, del mismo modo en el que se hace para Key Vault. Esto posibilita que los logs del HSM también puedan visualizarse mediante el servicio Azure Monitor, con el objetivo de ejecutar consultas sobre los logs para poder efectuar análisis sobre los mismos y obtener información en caso de que sea necesario. El servicio de Azure Monitor también permite, entre otras cosas, configurar alertas en base a los logs recopilados.

2.8.6 Emitir e importar certificados

Azure Key Vault tiene capacidad de emitir certificados autofirmados y certificados firmados por autoridades de confianza, a través de la integración con DigiCert y GlobalSign. El proceso de emisión de certificados expedidos por CAs reconocidas (DigiCert y GlobalSign) queda totalmente delegado en dichos proveedores, por lo que KV no proporciona ningún mecanismo para garantizar la validez de la información que se quiere asociar al certificado solicitado.

En el caso de que se quiera utilizar otro proveedor de certificados se deberá importar el certificado en Key Vault, una vez emitido por la autoridad de certificación que hayamos elegido. Los certificados importados pueden estar en formato PEM o PFX. Si el certificado importado está protegido por contraseña, se deberá proporcionar la contraseña en el momento de importarlo. Una vez importado, KV elimina dicha protección del archivo mediante contraseña.

Cuando KV genera un CRS, un certificado autofirmado o un certificado emitido por DigiCert o GlobalSign, en el momento de la creación se puede indicar, mediante la política, si la clave asociada al certificado es o no exportable. En caso de que se configure la clave como no exportable, ésta se genera dentro del vault y nunca queda expuesta al usuario, es decir, ni siquiera el dueño del certificado tiene acceso a la misma en claro.

2.8.7 Renovación de certificados

La renovación automática de los certificados emitidos por KV es configurable, tanto si se trata de certificados autofirmados, como si se trata de certificados emitidos por KV a través de la integración con DigiCert o GlobalSign. En el momento de la creación de los mismos podremos configurar lo siguiente:

- Que KV renueve automáticamente el certificado cuando éste esté próximo a su fecha de vencimiento.
- Que KV envíe un aviso al usuario mediante correo electrónico cuando el certificado esté próximo a caducar.

Sin embargo, cuando se trata de certificados importados no es posible efectuar la rotación automática del mismo. No obstante, KV permite configurar el envío de un email de aviso al usuario cuando el certificado esté próximo a su vencimiento. Además, KV también puede generar un par de claves y el CSR, con el objetivo de que el usuario lo descargue y lo envíe a la CA de su elección para que firme el certificado y lo vuelva a importar. Al importar de nuevo el certificado, KV es capaz de reconocer que se trata de un certificado ya existente y por tanto lo almacena como una nueva versión del mismo.

3. Metodología y aplicación

En este apartado se llevará a cabo el desarrollo de la metodología que se aplicará a los diferentes servicios analizados y extraerán los resultados y conclusiones de este Trabajo.

Antes de comenzar con el desarrollo de la metodología conviene diferenciar los servicios que realizan gestión de certificados de aquellos que, además de realizar gestión de certificados, permiten al usuario implementar una PKI privada. Esta diferenciación es fundamental, ya que de lo contrario se estaría exigiendo características propias de una PKI a servicios cuya finalidad no es la implementación de una PKI.

Por el motivo que se acaba de exponer se desarrollarán dos metodologías: una se aplicará sobre servicios que realicen gestión de certificados y otra sobre servicios que permitan al usuario la implementación de una PKI privada. Así, por un lado tendremos una metodología que se aplicará sobre los servicios AWS Certificate Manager, Cloud Load Balancing de GCP[7] y Azure Key Vault; y por otro, una metodología que se aplicará sobre los servicios AWS Certificate Manager Private Certificate Authority y GCP Certificate Authority.

3.1 Desarrollo de la metodología

En primer lugar, antes de empezar con el desarrollo de la metodología, se define un escenario de aplicación con el objetivo de reducir el alcance. Por este motivo, las dos metodologías a desarrollar se construirán poniendo foco en dos objetivos:

- Maximizar la seguridad.
- Facilitar la operación.

Por lo tanto, los criterios utilizados para construir dichas metodologías tendrán como objetivo aumentar la seguridad del servicio o facilitar la operación del mismo.

[7] Limitado a la funcionalidad que permite la gestión de certificados en el mismo

3.1.1 Metodología para servicios de gestión de certificados

Para construir esta metodología, en primer lugar se elegirá un conjunto de criterios enfocados en maximizar la seguridad del servicio y facilitar la operación.

3.1.1.1 Criterios de seguridad

Los criterios que se tendrán en cuenta, con el objetivo de garantizar una seguridad adecuada en un servicio de gestión de certificados, irán orientados principalmente a la securización de las claves privadas asociadas a los certificados.

Para ello se tendrán en cuenta las medidas de protección que ofrece el proveedor cloud para proteger dichas claves. Entre otros, se valorará si existen mecanismos para establecer controles de acceso y auditorías de las mismas o cómo se protegen en reposo y en tránsito. Dichas medidas, junto con otras, se detallan en la tabla que se muestra a continuación, que será la que se utilice en el momento de aplicar la metodología.

Criterios de Seguridad	AWS	GCP	Azure
Protección en reposo de claves privadas asociadas a los certificados			
Admite el uso de un servicio de gestión de claves propio del cloud para proteger las claves privadas de los certificados propios			
Admite el uso de un servicio de gestión de claves propio del cloud para almacenar la clave maestra que se utilizar para proteger las claves privadas de los certificados importados			
Las claves privadas asociadas a certificados se almacenan siempre cifradas			
Las claves privadas de los certificados emitidos por el servicio no se pueden exportar			
El servicio admite la configuración de un HSM para almacenar las claves privadas de los certificados			
El proveedor cloud no puede ver ni extraer la información almacenada en el servicio			

Protección en tránsito de claves privadas asociadas a los certificados			
La clave privada del certificado se transmite cifrada a nivel de dato y canal (TLS)			
Control de acceso a las claves privadas			
Existen mecanismos para identificar y autenticar a los usuarios y/o sistemas/aplicaciones que acceden a las claves			
Existen mecanismos para segregar el acceso a la claves, permitiendo otorgar a cada usuario/sistema/aplicación los permisos mínimos necesarios			
Al implementar el almacenado en HSM los roles de operador del HSM y los roles que permite el acceso a la claves están gestionados por sistemas de autorización distintos			
Capacidades de monitorización			
Se integra con servicios propios del proveedor cloud para facilitar la monitorización de cualquier acción relacionada con la gestión de certificados			
Características de los certificados emitidos			
Emite certificados utilizando su propia CA reconocida			
Los certificados emitidos por el servicio cuentan con validación de dominio (DV)			
Los certificados emitidos por el servicio cuentan con validación extendida (EV)			
La validación del dominio se realiza mediante modificaciones en el registro DNS del dominio			
La validación del dominio se realiza por email			
Los certificados emitidos por el servicio admiten comodines			
Puede emitir certificados basándose en el algoritmo RSA con tamaño de clave de 4096 bits			
Puede emitir certificados basándose en el algoritmo			

de curva elíptica con tamaño de clave de 384 bits			
Se pueden importar certificados basados en algoritmo RSA con tamaño de clave de 4096 bits			
Se pueden importar certificados basados en algoritmo de curva elíptica con tamaño de clave de 512 bits			

3.1.1.2 Criterios que facilitan la operación

Los criterios que se tendrán en cuenta irán orientados a valorar si el servicio ofrece funcionalidades que faciliten la operación, por ejemplo: que el servicio proporcione la renovación automática de los certificados.

A continuación se muestra una tabla que contiene funcionalidades que se consideran útiles desde el punto de vista de la operación del servicio. Al igual que en el caso anterior, esta misma tabla será la que se utilice para aplicar la metodología más adelante.

Criterios de Operación	AWS	GCP	Azure
Se puede modificar el certificado añadiendo nombres de dominio o eliminándolos			
El servicio ofrece una consola centralizada en la que se pueden administrar todos los certificados utilizados bajo una misma cuenta			
Renueva los certificados emitidos de forma automática			
Notifica al usuario (vía email) cuando un certificado emitido por el servicio está próximo a su vencimiento			
Notifica al usuario (vía email) cuando un certificado importado está próximo a su vencimiento			
El servicio no permite eliminar certificados que estén siendo utilizados por otro servicio del mismo proveedor cloud			
La generación de los certificados que emite el servicio no delega acciones intermedias en el usuario (p. ej: descarga de CSR, subida del certificado al cloud)			

3.1.2 Metodología para servicios que facilitan la implementación de una PKI privada

Para construir esta metodología se seguirán los mismos pasos, estableciendo criterios orientados a maximizar la seguridad del servicio y facilitar la operación. En este caso, nos enfocaremos en establecer criterios que proporcionen buenas medidas de seguridad a una PKI privada y que faciliten la operación de la misma. Algunos criterios serán idénticos a los establecidos para la metodología de gestión de certificados, ya que algunas características como el almacenamiento de las claves o los procesos de emisión y renovación de certificados, siguen siendo especialmente relevantes cuando se trata de analizar una PKI privada.

3.1.2.1 Criterios de seguridad

Criterios de Seguridad	AWS	GCP
Almacenamiento de las claves privadas		
Las claves privadas de los certificados se almacenan en un HSM gestionado por el proveedor cloud		
Admite el uso de un servicio de gestión de claves propio del cloud para proteger las claves privadas de los certificados emitidos		
Las claves privadas asociadas a certificados se almacenan siempre cifradas		
Control de acceso a las claves privadas		
Existen mecanismos para identificar y autenticar a los usuarios y/o sistemas/aplicaciones que acceden a las claves y certificados		
Existen mecanismos para segregar el acceso a la claves y certificados, permitiendo otorgar a cada usuario/sistema/aplicación los permisos mínimos necesarios		
Capacidades de monitorización		
Se integra con servicios propios del proveedor cloud para facilitar la monitorización de cualquier acción relacionada con la gestión de certificados		

Consulta de estado de vigencia de un certificado		
Admite OCSP para consultar las listas de revocación de certificados		
Admite CRLs para consultar las listas de revocación de certificados		

3.1.2.1 Criterios de operación

Criterios de Operación	AWS	GCP
El servicio permite aprovechar capacidades de integración con otros servicios del cloud para facilitar el despliegue y ciclo de vida de los certificados		
Permite generar informes de auditoría (certs emitidos, revocados…)		
Proporciona mecanismos para renovar el certificado de una CA		
El servicio ofrece una consola centralizada en la que se pueden administrar todos los certificados utilizados bajo una misma PKI privada		
Renueva los certificados de servidor emitidos de forma automática		
Notifica al usuario (vía email) cuando un certificado cliente o servidor emitido por la PKI está próximo a su vencimiento		
Es capaz de emitir un certificado sin que el usuario tenga que importar un CSR		
El servicio permite al usuario crear una CA en AWS que sea subordinada de la CA raíz que se ejecuta en las instalaciones propias del usuario		
El servicio permite crear políticas de emisión de certificados		

3.2 Aplicación de la metodología a los servicios analizados

3.2.1 Aplicación de la metodología para servicios de gestión de certificados

Al aplicar esta metodología se están valorando los siguientes servicios:

- AWS Certificate Manager.
- Cloud Load Balancing de GCP.
- Azure Key Vault.

Antes de aplicar la metodología conviene mencionar lo siguiente: GCP no proporciona a los usuarios un servicio de gestión unificada de certificados de servidor, sino que ofrece dicha funcionalidad a través de su servicio de balanceo de carga.

Esto tiene sus ventajas y sus inconvenientes, dependiendo del caso de uso concreto en el que se esté planteando la utilización de un servicio de gestión de certificados. El hecho de que la solución se proporciona a través de una funcionalidad de un servicio, limita al usuario a emplear el servicio en sí, si quiere disfrutar de esa capacidad.

Puede ocurrir que la arquitectura sobre la que se quiere implementar el servicio de gestión de certificados de servidor exponga los servicios siempre mediante un balanceador de carga, algo que suele ser bastante habitual. Sin embargo, ¿qué ocurre si se quiere proteger con TLS endpoints que no necesitan exponerse mediante un balanceador?

Se podría implementar el balanceador y añadir una pieza más a la arquitectura o se podría optar con configurar el certificado en los endpoints y gestionarlos *ad hoc*. No obstante, en cualquiera de los casos nos encontramos con los siguientes inconvenientes:

- Si se implementa un balanceador delante de cada endpoint se incurre en costes adicionales asociados al balanceador, que a priori no se necesita, y además, se introduce un posible punto de fallo en la arquitectura.
- Si se opta por configurar el certificado en el endpoint, a nivel de operación no se tendrá acceso a una consola de gestión de certificados centralizada. Esto dificultará la gestión de los mismos, pudiendo provocar olvidos de renovación de los certificados configurados *ad hoc*.

Por estos motivos, el hecho de que GCP no tenga un servicio dedicado a la gestión exclusiva de certificados, le deja un poco en desventaja frente a AWS o Azure, que sí los tienen.

Sin embargo, dado que el objetivo que se quiere lograr al aplicar la metodología es:

- facilitar la operación y
- maximizar la seguridad;

teniendo en cuenta que los problemas de operación, en el ejemplo concreto que se acaba de exponer, quedaron solventados incluyendo nuevos balanceadores, se aplicará la metodología también al servicio de Cloud Load Balancing de GCP en lo que refiere a su funcionalidad para la gestión de certificados.

A continuación se aplican los criterios de seguridad y operación definidos en la metodología a las diferentes nubes, para conocer si cumplen o no con los criterios definidos. Todos los criterios están definidos utilizando frases afirmativas o negativas, teniendo en cuenta siempre que estén formulados de forma que favorezcan la seguridad o la operación. De esta manera, el servicio que obtenga más ✅ nos dará un indicador de cuál puede ser el servicio más adecuado, no obstante, esto no será suficiente, ya que habrá que valorar los criterios que se cumplen y razonar el resultado.

Criterios de Seguridad	AWS	GCP	Azure
Protección en reposo de claves privadas asociadas a los certificados			
Admite el uso de un servicio de gestión de claves propio del cloud para almacenar la clave maestra que se utilizar para proteger las claves privadas de los certificados importados	✅	No se especifica	No se especifica
Las claves privadas asociadas a certificados se almacenan siempre cifradas	✅	✅	✅
Las claves privadas de los certificados emitidos por el servicio no se pueden exportar	✅	✅	❌
El servicio admite la configuración de un HSM para almacenar las claves privadas de los certificados	❌	❌	✅
El proveedor cloud no puede ver ni extraer la	No se	No se	✅

información almacenada en el servicio	especifica	especifica	
Protección en tránsito de claves privadas asociadas a los certificados			
La clave privada del certificado se transmite cifrada a nivel de dato y canal (TLS)	✅	No se especifica	No se especifica
Control de acceso a las claves privadas			
Existen mecanismos para identificar y autenticar a los usuarios y/o sistemas/aplicaciones que acceden a las claves	✅	✅	✅
Existen mecanismos para segregar el acceso a la claves, permitiendo otorgar a cada usuario/sistema/aplicación los permisos mínimos necesarios	✅	✅	✅
Al implementar el almacenado en HSM los roles de operador del HSM y los roles que permite el acceso a la claves están gestionados por sistemas de autorización distintos	❌	❌	✅
Capacidades de monitorización			
Se integra con servicios propios del proveedor cloud para facilitar la monitorización de cualquier acción relacionada con la gestión de certificados	✅	No se especifica	✅
Características de los certificados emitidos			
Emite certificados utilizando su propia CA reconocida	✅	✅	❌
Los certificados emitidos por el servicio cuentan con validación de dominio (DV)	✅	✅	Se delega en GlobalSign o DigiCert ✅
Los certificados emitidos por el servicio cuentan con validación extendida (EV)	❌	❌	Se delega en GlobalSign o DigiCert ✅
La validación del dominio se realiza mediante modificaciones en el registro DNS del dominio	✅	No se especifica	Se delega en GlobalSign o DigiCert
La validación del dominio se realiza por email	✅	No se especifica	Se delega en GlobalSign o DigiCert
Los certificados emitidos por el servicio admiten comodines	✅	✅	Se delega en GlobalSign o DigiCert

			✅
Puede emitir certificados basándose en el algoritmo RSA con tamaño de clave de 4096 bits	✅	No se especifica	Se delega en GlobalSign o DigiCert ✅
Puede emitir certificados basándose en el algoritmo de curva elíptica con tamaño de clave de 384 bits	✅	No se especifica	No se especifica
Se pueden importar certificados basados en algoritmo RSA con tamaño de clave de 4096 bits	✅	❌	✅
Se pueden importar certificados basados en algoritmo de curva elíptica con tamaño de clave de 512 bits	✅	❌	✅
Total	16✅ 3❌	7✅ 5❌	13✅ 2❌

Criterios de Operación	AWS	GCP	Azure
Se puede modificar el certificado añadiendo nombres de dominio o eliminándolos	❌	No se especifica	✅
El servicio ofrece una consola centralizada en la que se pueden administrar todos los certificados utilizados bajo una misma cuenta	✅	❌	✅
Renueva los certificados emitidos de forma automática	✅	✅	✅
Notifica al usuario (vía email) cuando un certificado emitido por el servicio está próximo a su vencimiento	✅	No se especifica	✅
Notifica al usuario (vía email) cuando un certificado importado está próximo a su vencimiento	❌	No se especifica	✅
El servicio no permite eliminar certificados que estén siendo utilizados por otro servicio del mismo proveedor cloud	✅	❌	❌
La generación de los certificados que emite el servicio no delega acciones intermedias en el usuario (p. ej: descarga de CSR, subida del certificado al cloud)	✅	✅	❌
Total	5✅ 2❌	2✅ 2❌	5✅ 2❌

Al aplicar la metodología se observa claramente que el servicio de GCP es el que menos información proporciona, seguramente debido a que se trata de una funcionalidad de un servicio más de un servicio en sí mismo. Por este motivo, no sería justo decir que es menos seguro o más difícil de operar. No obstante, dado que no se dispone de información suficiente, y teniendo en cuenta los motivos argumentados antes de aplicar la metodología, se descartará la elección de este servicio y finalmente se realizará una valoración entre ACM y KV para obtener un resultado.

3.2.2 Aplicación de la metodología a PKIs privadas

Esta vez se aplicará la metodología a los servicios Amazon Certificate Manager Private Certificate Authority y GCP Certificate Authority.

Del mismo modo que se realizó para los servicios de gestión de certificados, todos los criterios están definidos utilizando frases afirmativas o negativas, teniendo en cuenta siempre que estén formulados de forma que favorezcan la seguridad o la operación. De esta manera, el servicio que obtenga más ✅ nos dará un indicador de cuál puede ser el servicio más adecuado, no obstante, esto no será suficiente, ya que habrá que valorar los criterios que se cumplen y razonar el resultado.

La valoración del resultado es fundamental, ya que se han proporcionado criterios en la metodología que favorecen la seguridad y la operación, pero no todos la favorecen en la misma medida. Por ejemplo, se valora que un servicio proporcione OCSP para gestionar las consultas de certificados revocados, pero también se valora que proporcione CRLs para realizar esto mismo. En un escenario de implementación de PKI privada, se optará por una solución que admita sólo CRLs frente a otra que admita sólo OCSP, ya que en una solución que admita sólo OCSP se podría llegar a saturar el servidor. Sin embargo, si alguna de las soluciones ofrece CRL y OCSP, será preferible frente a la que admite sólo CRLs, ya que la que admite CRL y OCSP proporciona más margen de actuación en función del caso de uso.

Criterios de Seguridad	AWS	GCP
Almacenamiento de las claves privadas		
Las claves privadas de los certificados se almacenan en un HSM gestionado por el proveedor cloud	✅	❌

Admite el uso de un servicio de gestión de claves propio del cloud para proteger las claves privadas de los certificados emitidos	❌	✅ (KMS)
Las claves privadas asociadas a certificados se almacenan siempre cifradas	✅	✅
Control de acceso a las claves privadas		
Existen mecanismos para identificar y autenticar a los usuarios y/o sistemas/aplicaciones que acceden a las claves y certificados	✅	✅
Existen mecanismos para segregar el acceso a la claves y certificados, permitiendo otorgar a cada usuario/sistema/aplicación los permisos mínimos necesarios	✅	✅
Capacidades de monitorización		
Se integra con servicios propios del proveedor cloud para facilitar la monitorización de cualquier acción relacionada con la gestión de certificados	✅	✅
Consulta de estado de vigencia de un certificado		
Admite OCSP para consultar las listas de revocación de certificados	✅	❌
Admite CRLs para consultar las listas de revocación de certificados	✅	✅
Total	7✅ 1❌	6✅ 2❌

Criterios de Operación	AWS	GCP
El servicio permite aprovechar capacidades de integración con otros servicios del cloud para facilitar el despliegue y ciclo de vida de los certificados	✅	❌
Permite generar informes de auditoría (certs emitidos, revocados…)	✅	✅
Proporciona mecanismos para renovar el certificado de una CA	✅	✅
El servicio ofrece una consola centralizada en la que se pueden administrar todos los certificados utilizados bajo una	✅	✅

misma PKI privada		
Renueva los certificados de servidor emitidos de forma automática	✅	❌
Notifica al usuario (vía email) cuando un certificado cliente o servidor emitido por la PKI está próximo a su vencimiento	✅	❌
Es capaz de emitir un certificado sin que el usuario tenga que importar un CSR	❌	✅
El servicio permite al usuario crear una CA en AWS que sea subordinada de la CA raíz que se ejecuta en las instalaciones propias del usuario	✅	✅
El servicio permite crear políticas de emisión de certificados	✅	✅
Total	8✅ 1❌	6✅ 3❌

4. Resultados

4.1 Servicios de Gestión de Certificados

A continuación se adjunta de nuevo el resultado de la aplicación de la metodología, en este caso, limitado a ACM y KV por los motivos expuestos anteriormente. Además se eliminarán de la tabla los criterios que cumplan ambos servicios para facilitar la valoración.

Criterios de Seguridad	AWS	Azure
Protección en reposo de claves privadas asociadas a los certificados		
Admite el uso de un servicio de gestión de claves propio del cloud para almacenar la clave maestra que se utilizar para proteger las claves privadas de los certificados importados	✅	No se especifica
Las claves privadas de los certificados emitidos por el servicio no se pueden exportar	✅	❌
El servicio admite la configuración de un HSM para almacenar las claves privadas de los certificados	❌	✅
El proveedor cloud no puede ver ni extraer la información almacenada en el servicio	No se especifica	✅
Protección en tránsito de claves privadas asociadas a los certificados		
La clave privada del certificado se transmite cifrada a nivel de dato y canal (TLS)	✅	No se especifica
Control de acceso a las claves privadas		
Al implementar el almacenado en HSM los roles de operador del HSM y los roles que permite el acceso a la claves están gestionados por sistemas de autorización distintos	❌	✅
Características de los certificados emitidos		
Emite certificados utilizando su propia CA reconocida	✅	❌
Los certificados emitidos por el servicio cuentan con validación de dominio (DV)	✅	Se delega en GlobalSign o DigiCert ✅

Los certificados emitidos por el servicio cuentan con validación extendida (EV)	❌	Se delega en GlobalSign o DigiCert ✅
La validación del dominio se realiza mediante modificaciones en el registro DNS del dominio	✅	Se delega en GlobalSign o DigiCert
La validación del dominio se realiza por email	✅	Se delega en GlobalSign o DigiCert
Los certificados emitidos por el servicio admiten comodines	✅	Se delega en GlobalSign o DigiCert ✅
Puede emitir certificados basándose en el algoritmo RSA con tamaño de clave de 4096 bits	✅	Se delega en GlobalSign o DigiCert ✅
Puede emitir certificados basándose en el algoritmo de curva elíptica con tamaño de clave de 384 bits	✅	No se especifica
Total	10✅ 3❌	7✅ 2❌

A nivel de seguridad cobra especial relevancia Azure Key Vault porque permite configurar un HSM para gestionar las claves de los certificados y AWS Certificate Manager no cuenta con esta capacidad.

Por contra, KV servicio no es autónomo a la hora de emitir certificados y AWS Certificate Manager sí es autónomo, es decir, tiene su propia CA.

Otra de las bondades de Azure Key Vault es que permite emitir certificados de validación extendida, a través de su integración con GlobalSign y DigiCert. Sin embargo ACM no tiene capacidad para emitir certificados de validación extendida.

Finalmente, otra de las características en las que se diferencian ambos servicios es en la exportación de claves de los certificados que emiten. ACM no posibilita la exportación de la clave privada asociada a los certificados emitidos, lo que otorga especial seguridad a dichas claves, ya que se asegura que nunca salen del entorno de AWS. Por contra, la exportación de claves privadas en KV es configurable, y llegado el momento se podría configurar que las claves fueran exportables, por lo que Azure, como proveedor cloud, no garantiza que

las claves privadas no salgan del entorno de su cloud, lo deja a elección del usuario.

Criterios de Operación	AWS	Azure
Se puede modificar el certificado añadiendo nombres de dominio o eliminándolos	❌	✅
Notifica al usuario (vía email) cuando un certificado importado está próximo a su vencimiento	❌	✅
El servicio no permite eliminar certificados que estén siendo utilizados por otro servicio del mismo proveedor cloud	✅	❌
La generación de los certificados que emite el servicio no delega acciones intermedias en el usuario (p. ej: descarga de CSR, subida del certificado al cloud)	✅	❌
Total	2✅ 2❌	2✅ 2❌

En cuanto a operación, si valoramos únicamente el resultado de la aplicación de la metodología parecería que, en términos absolutos, a nivel de operación los servicios son iguales, sin embargo es importante tener en cuenta los siguientes matices:

- ACM no permite la modificación de los certificados, por lo que en caso de necesitar modificar un certificado habría que emitir uno nuevo. Esto facilita que el usuario alcance la cuota máxima de emisión de certificados definida por ACM, no obstante, se debe tener en cuenta que AWS permite que los usuarios soliciten una ampliación de dicha cuota.
- Con respecto a la notificación por email cuando un certificado importado está a punto de caducar, es cierto que AWS no facilita el envío de dicho email, aunque el usuario sí podría configurar dicho envío utilizando cloudwatch. En este sentido, destaca la funcionalidad que tiene KV para definir políticas sobre los certificados, ya que contiene toda la información necesaria con respecto al certificado para que Azure pueda gestionar el ciclo de vida. De esta manera, la capacidad de Azure para enviar un email al usuario cuando el certificado está a punto de expirar se configura fácilmente a través de la política asociada al certificado, sin necesidad de tener que construir procesos adicionales.

Teniendo en cuenta estos matices de ACM, se podría salvar las diferencias con respecto a no poder modificar el certificado o tener que trabajar un poco más para notificar al usuario cuando un certificado está próximo a caducar. Así, se podría aprovechar la facilidad que ofrece ACM para generar un certificado, que además reduce riesgos de operación, y la bondad del servicio que impide que los usuarios puedan eliminar un certificado si está siendo utilizado, para reducir fallos en la operación del servicio.

4.2 Servicios que permiten implementar PKI privadas

En las siguientes tablas se puede ver el resultado de la implementación de la metodología sobre los servicios ACM PCA y GCP Certificate Authority. Para simplificar el resultado se eliminarán de la tabla los criterios que cumplan ambos servicios para facilitar la valoración.

Criterios de Seguridad	AWS	GCP
Almacenamiento de las claves privadas		
Las claves privadas de los certificados se almacenan en un HSM gestionado por el proveedor cloud	✅	❌
Admite el uso de un servicio de gestión de claves propio del cloud para proteger las claves privadas de los certificados emitidos	❌	✅ (KMS)
Consulta de estado de vigencia de un certificado		
Admite OCSP para consultar las listas de revocación de certificados	✅	❌
Total	7✅ 1❌	6✅ 2❌

Con respecto a la seguridad el servicio de implementación de PKI de AWS genera especial interés, ya que por defecto, y de forma totalmente transparente al usuario, gestiona las credenciales asociadas a los certificados en HSMs gestionados por AWS. Además, admite OCSP como método adicional a CRLs para consultar el estado de un certificado.

Por otro lado, GCP no proporciona OCSP ni almacenamiento de credenciales en HSM, pero sí utiliza su solución de gestión de claves para almacenar cifradas las claves asociadas a los certificados, y además proporciona CRL como solución para comprobar el estado de un certificado. Son criterios que también se consideran suficientemente seguros a la hora de implementar una PKI privada, por lo que, desde el punto de vista de seguridad, lo que haga que un usuario se decante por una opción o por otra, dependerá de cuánta atención quiera ponerle a las claves privadas de sus certificados.

Si se busca maximizar la seguridad, sin duda el claro ganador sería ACM PCA que ofrece almacenamiento de claves privadas en HSMs gestionados.

Criterios de Operación	AWS	GCP
El servicio permite aprovechar capacidades de integración con otros servicios del cloud para facilitar el despliegue y ciclo de vida de los certificados	✅	❌
Renueva los certificados de servidor emitidos de forma automática	✅	❌
Notifica al usuario (vía email) cuando un certificado cliente o servidor emitido por la PKI está próximo a su vencimiento	✅	❌
Es capaz de emitir un certificado sin que el usuario tenga que importar un CSR	❌	✅
Total	8✅ 1❌	6✅ 3❌

Con respecto a los criterios de operación, de nuevo destaca ACM PCA frente a GCP ya que proporciona funcionalidades que facilitan la gestión del ciclo de vida de los certificados con las que Certificate Authority no cuenta. No obstante, Certificate Authority también cuenta con una funcionalidad que simplifica bastante el proceso de generación de certificados, ya que permite generar un certificado sin necesidad de que el usuario genere previamente el CSR. En el caso de ACMP PCA, para poder emitir el certificado, el usuario deberá generar siempre el CSR previamente.

5. Conclusiones

5.1 Servicios de gestión de certificados

Teniendo en cuenta los resultados obtenidos al aplicar la metodología en 3.2.1, se evidencia la importancia de realizar una valoración de los resultados. Resulta complicado elegir ACM frente a KV sin tener en cuenta el caso de uso y el entorno para el que se busca dicha solución.

Si en el caso de uso prima, por encima de cualquier cosa, maximizar la seguridad en un primer momento se elegiría la opción de Azure Key Vault, porque permite configurar HSMs para el almacenamiento seguro de las claves asociadas a los certificados. Sin embargo, cuando se accede a valorar el resto de funcionalidades, nos encontramos con malas prácticas en la operación del servicio que ponen en riesgo la seguridad. Como por ejemplo, la descarga del CSR en local y el certificado en local durante el proceso de emisión del certificado si se utiliza la integración con GlobalSign. Por contra, si se utiliza la integración con DigiCert, se debe configurar en Azure las credenciales de acceso a la cuenta de DigiCert, lo que también implica cierta manualidad en la operación relacionada con las credenciales, que de nuevo incurre en un riesgo de operación que amenaza la seguridad (podrían producirse una revelación de credenciales y que todo el sistema de emisión de certificados fuese vulnerado).

Por todo esto que se acaba de argumentar, es preferible el uso de AWS Certificate Manager para la gestión de certificados. Esto implica prescindir del uso de un HSM para almacenar las claves, sin embargo, ACM ofrece funcionalidades de seguridad bastante buenas para proteger las claves mediante software. Además, ACM elimina los riesgos de operación que posee KV en el momento de emitir los certificados, ya que no necesita integrarse con ningún proveedor porque tiene su propia CA.

5.2 Servicios que permiten implementar PKI privadas

En este caso, debido a los resultados obtenidos en 4.2, se hace más fácil la valoración y elección de uno de los servicios de gestión de PKI privada.

Se ve fácilmente que las ventajas que proporciona ACM PCA sobre Certificate Authority mejoran bastante la seguridad y la operación y además lo hacen de forma transparente al usuario.

Por un lado, al utilizar HSM gestionados por AWS el usuario se beneficia de las bondades de utilizar almacenamiento de secretos en hardware sin tener que gestionar el mismo. A efectos del usuario, la experiencia es la misma que si estuviera utilizando un almacenamiento de tipo software, tal como hace Certificate Authority, sin embargo, se está beneficiando del almacenamiento de secretos en hardware.

Por otro lado, para los certificados de servidor puede configurar la renovación automática de los mismos o que se notifique al usuario mediante un email cuando el certificado está a punto de expirar. Esto es posible porque ACM PCA está integrado con ACM, por lo que utiliza las capacidades de éste último para efectuar dichas funcionalidades. Así, se facilita al usuario la renovación de certificados de tipo servidor.

6. Glosario de Términos

- **Centro de Proceso de Datos (CPD):** espacio en el que una empresa almacena los recursos informáticos y electrónicos necesarios para llevar a cabo su actividad.
- **Infraestructura de Clave Pública o Public Key Infrastructure (PKI):** conjunto de componentes y servicios informáticos que permiten establecer un sistema de comunicación basado en autenticar a los componentes mediante certificado digital.
- **Certificado digital:** fichero informático firmado electrónicamente por una autoridad reconocida, que permite al componente (persona o máquina) que lo posee autenticarse ante cualquier sistema que admite este tipo de autenticación. Todo certificado digital tiene asociadas un par de claves criptográficas, conocidas como clave pública y clave privada.
- **Autoridad de Certificación (CA):** entidad de confianza responsable de emitir y revocar los certificados digitales.
- **Autoridad de Registro (RA):** comprueba la veracidad de la información que se quiere incluir en el certificado.
- **Petición de firma del certificado (CSR):** es un fichero que consta de la información que el usuario quiere incluir en el certificado y de la clave pública que se quiere asociar al mismo.
- **Autoridad de validación (VA):** es el sistema de la PKI encargado de almacenar el listado de certificados revocados.
- **Lista de revocación de certificados (CRL):** es un fichero, firmado con la clave pública de la CA, que contiene el listado de los certificados que carecen de validez.
- **Online Certificate Status Protocol (OCSP):** es un protocolo utilizado para determinar el estado de vigencia de un certificado.
- **Transport Layer Security (TLS):** protocolo que permite establecer el cifrado del canal en la capa de transporte, con el objetivo de que los datos transmitidos en la comunicación no sean visibles a los usuarios de la red que estén escuchando las comunicaciones.

- **Certificado de servidor:** este tipo de certificado está orientado a garantizar la identidad del nombre de dominio de un sitio web.
- **Certificado cliente:** este tipo de certificado está orientado a garantizar la identidad de un cliente que se conecta a un servidor. Puede ser utilizado tanto para identificar personas, como para identificar sistemas o aplicaciones cuando estas actúan como cliente en la comunicación.
- **Domain Name System (DNS):** sistema de nombres de dominio de Internet, en líneas generales, es el sistema que permite traducir los nombres de dominio en IPs. Un registro DNS contiene información relacionada con el nombre de dominio.
- **Certificado X.509:** es un formato estándar para certificados que asocian de forma segura pares de claves criptográficas con identidades.
- **Domain Validated (DV):** un certificado de validación de dominio es un certificado de clave pública X.509 en el que el nombre de dominio del solicitante se valida pidiendo al usuario que solicita el certificado que demuestre que tiene el control sobre el dominio en cuestión.
- **Fully Qualified Domain Names (FQDN):** es un nombre de dominio completo que incluye tanto el dominio de nivel superior, el nombre de dominio y el nombre de host.
- **WHOIS:** directorio público (https://who.is/) mediante el que se puede saber quién es el propietario de un dominio o dirección IP.
- **Organization Validation (OV):** un certificado con validación de organización es un certificado de clave pública X.509 en el que además de validar el nombre de dominio se validan también los datos de la empresa, para verificar que la empresa existe, se encuentra en la dirección provista y es propietaria del dominio para el que solicita expedir el certificado.
- **Extended Validation (EV):** los certificados con validación extendida también verifican la identidad de la organización, igual que los certificados de validación de organización, sin embargo las validaciones realizadas por EV requieren verificaciones de validación más rigurosas.
- **FIPS 140-2:** es el acrónimo de Federal Information Processing Standard, que es un estándar de seguridad de ordenadores del gobierno de EEUU para la acreditación de módulos criptográficos.

- **OAuth2:** es un estándar utilizado para autorizar el acceso a recursos, se define en el RFC 6749.

7. Bibliografía

[1] **Tracy Pierce, Aravind Kodandaramaiah, Rafael Koike, Alex Rosa.** “AWS Certified Security Specialty All-in-One Exam Guide”, McGraw-Hill, 2021.

[2] **Karl Ots.** “Azure Security Handbook: A Comprehensive Guide for Defending Your Enterprise Environment”, Apress,2021.

[3] **Mustafa Toroman, Tom Janetscheck (2020).** “Mastering Azure Security”, Packt Publishing, 2020.

[4] AWS Certificate Manager documentation. URL: https://docs.aws.amazon.com/acm/index.html#lang/en_us

[5] AWS Private Certificate Authority documentation https://docs.aws.amazon.com/acm-pca/latest/userguide/PcaWelcome.html

[6] Niveles de validación de certificados de clave pública. URL: https://en.wikipedia.org/wiki/Public_key_certificate#Validation_levels

[7] SSL en Cloud Load Balancing, GCP. URL: https://cloud.google.com/load-balancing/docs/ssl-certificates

[8] Servicio Certificate Authority, GCP. URL: https://cloud.google.com/certificate-authority-service/docs

[9] Servicio Azure Application Gateway, Azure. URL: https://docs.microsoft.com/en-us/azure/application-gateway/overview

[10] Servicio App Service, Azure. URL: https://docs.microsoft.com/en-us/azure/app-service/overview

[11] Servicio SQL server, Azure. URL: https://docs.microsoft.com/en-us/sql/sql-server/?view=sql-server-ver15