Universitat Oberta de Catalunya

uoc.edu

ARQUITECTURA Y DISEÑO DE SEGURIDAD DE APLICACIONES EN LA NUBE PÚBLICA

Autor: Lucas Díez Huertas

Máster en Seguridad de las Tecnologías de la Información y de las Comunicaciones

TFM - Seguridad en la Internet de las cosas

Consultor: Manel Jesús Mendoza Flores

Profesor/a responsable de la asignatura: Víctor García Font

Junio 2020

FICHA DEL TRABAJO FINAL

Título del trabajo:	*Arquitectura y Diseño de Seguridad de Aplicaciones en la nube pública*
Nombre del autor:	*Lucas Díez Huertas*
Nombre del consultor/a:	*Manel Jesús Mendoza Flores*
Nombre del PRA:	*Víctor García Font*
Fecha de entrega (mm/aaaa):	06/2020
Titulación:	Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones
Área del Trabajo Final:	TFM - Seguridad en la Internet de las cosas
Idioma del trabajo:	*Español*
Palabras clave	*Cloud, Security, Design, Governance (nube, seguridad, diseño, gobierno)*

Resumen del Trabajo:

Debido a la transformación digital de las empresas más el incremento provocado por la inesperada pandemia del COVID-19, muchas organizaciones se han planteado migrar sus aplicaciones desplegadas en sus CPD a entornos de nube pública y así facilitar el acceso de sus aplicaciones de negocio a todos sus empleados sin necesidad de exponer sus CPD con bajos niveles de seguridad, y poder así evitar fugas de información, que provocarían perdidas de reputación empresarial y en otros casos multas por parte de los reguladores.

Con este TFM planteo una forma de trabajo desde el punto de vista de la seguridad de la información, basado en el gobierno, arquitectura y diseño de la seguridad obteniendo así una metodología de trabajo en la que se recogen requisitos de seguridad que han de seguir las aplicaciones para alcanzar unos estándares de seguridad aceptables y conseguir que la información que se encuentra en las aplicaciones desplegadas sea del tipo que sea esté protegida y a salvo de aquellos que quieran obtenerla utilizando brechas de seguridad o fallos provocados por el diseño y despliegue de la aplicación en cualquier entorno.

Abstract :

Due to the digital transformation of companies plus the increase caused by the unexpected COVID-19 pandemic, many organizations have considered migrating their deployed applications on their CPDs to public cloud environments to facilitate access of their business applications to all their employees without exposing their CPDs with low levels of security, thus avoiding information leaks , which would result in loss of business reputation and in other cases fines by regulators.

With this TFM I propose a framework from the point of view of information security, based on government, architecture and security by design, thus obtaining a working methodology that collects security requirements, that must be followed by applications to achieve acceptable security standards and to ensure that the information found in the applications is of the type protected and safe from those you want to get it using security breaches or failures caused by the design and deployment of the application in any environment.

Índice

Lista de figuras

1. Introducción

1.1 Contexto y justificación del Trabajo

Dentro de la transformación digital que se está llevando actualmente en la mayoría de las organizaciones, unos de los aspectos que se trata es el de utilizar la nube pública como repositorio de estas nuevas aplicaciones. El objetivo de este trabajo fin de master, a partir de ahora TFM, es el de crear un guía/metodología para que las aplicaciones que se desplieguen en estos proveedores de nube pública cumplan los estándares básicos de seguridad así como establecer el gobierno sobre la computación en la nube.

1.2 Objetivos del Trabajo

Los objetivos del trabajo son establecer un estándar de diseño de seguridad para las aplicaciones que se van a desplegar en las nubes publicas analizando las herramientas de seguridad que nos ofrecen los principales proveedores de computación en la nube AWS, Azure y Google.

1.3 Enfoque y método seguido

Como el objetivo es crear una guía o estándar la estrategia es crear un documento de diseño que sea fácilmente entendible por personal técnico de seguridad de la información para que sea capaz de interpretarlo y poder seguir estas buenas prácticas y hacer que estas aplicaciones en la nube estén desplegadas en un entorno seguro bajo un gobierno optimo del cómputo contratado.

1.4 Planificación del Trabajo

A continuación, se incluye un diagrama de Gantt en el que se desglosan las principales actividades para abordar el proyecto.

A parte del anteproyecto, y de la elaboración del vídeo, el resto de la planificación se ha dividido en tres hitos fundamentales, y que se han hecho coincidir con las entregas de las tres PECs.

Como es un TFM teórico en el primero hito trataremos la definición de requisitos de seguridad y un estudio del estado del arte de las posibilidades que nos ofrecen los proveedores principales de cómputo en la nube. En el segundo hito trataremos la definición de requisitos de seguridad para arquitecturas mixtas y el gobierno óptimo de la nube.

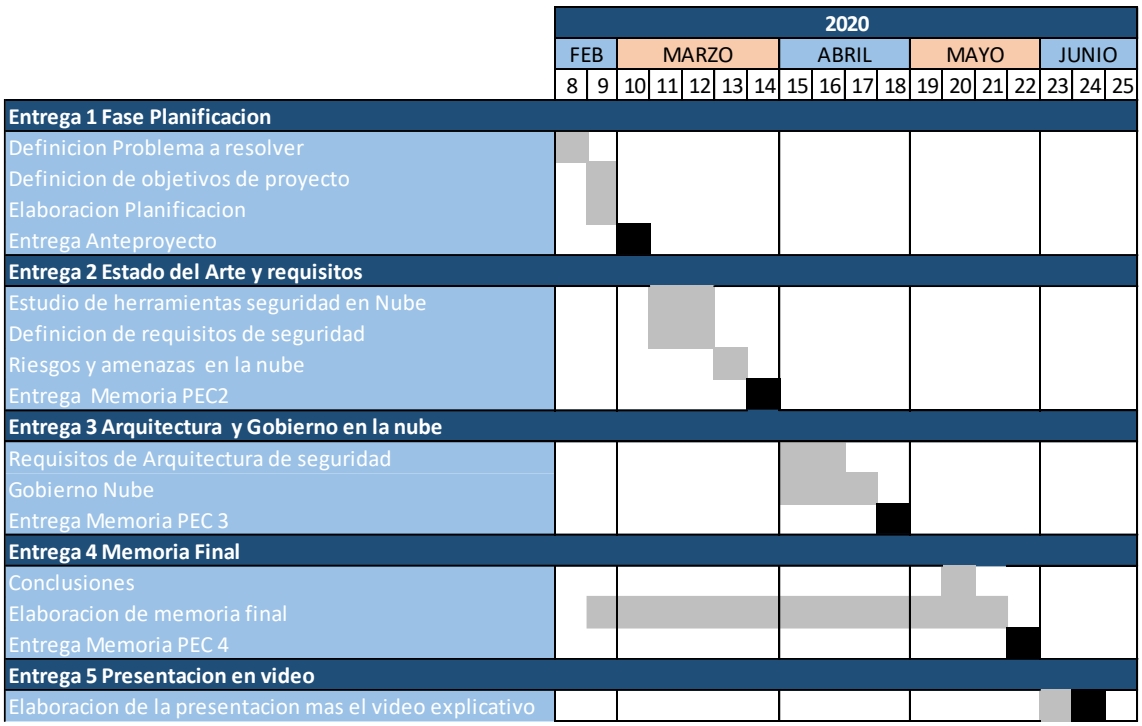


Ilustración 1 – Planificación

2. Riesgos y Amenazas en Cloud Computing

Para poder definir una guía de buenas prácticas de seguridad a la hora desplegar aplicaciones en la nube pública debemos basarnos en los riesgos y amenazas más conocidas para poder así crear una lista de requisitos que han de cumplir las aplicaciones para poder considerarlas seguras dentro de los estándares principales. Para ello vamos a detallar las amenazas y riesgos más comunes detectados por CSA y Gartner.

2.1 Amenazas Según CSA (Cloud Security Alliance, 2020)

Cloud Security Alliance (CSA), la organización dedicada a definir estándares, certificaciones y mejores prácticas con las que ayudar a garantizar un entorno de computación en la nube seguro, anunció en Las Vegas el 6 de agosto de 2019 (última revisión en abril de 2020) el lanzamiento de la última versión de las *Top Threats to Cloud Computing: The Egregious Eleven*, un nuevo informe que reexamina los riesgos inherentes a la seguridad en la nube, examinando los problemas inherentes a la configuración y la autenticación, en lugar del enfoque tradicional en las vulnerabilidades y el malware.

Este año último informe se han calificado 11 amenazas, riesgos y vulnerabilidades sobresalientes en la nube.

2.1.1 Pérdida o Fuga de Información

La pérdida o fuga de información es un incidente de ciberseguridad en el que la información protegida o confidencial es liberada, vista, robada o utilizada por una persona no autorizada.

La pérdida de información puede ser el objetivo principal de un ataque dirigido o simplemente el resultado de errores humanos, vulnerabilidades de aplicación o prácticas de seguridad inadecuadas.

La fuga de información implica cualquier tipo de información que no estaba destinada a la divulgación pública, incluyendo, pero no limitado a, información de salud personal, información financiera, información de identificación personal (PII), secretos comerciales y propiedad intelectual.

Ilustración 2 - Fuga Información

El impacto que puede tener en el negocio puede ser muy elevado tanto en la reputación y valor de la empresa como con la confianza de los clientes, y puede llegar a derivar en problemas contractuales y gastos financieros extras debido a la respuesta a incidentes y forenses.

La responsabilidad a nivel de seguridad de este problema de suele ser compartida tanto por el cliente como por el proveedor de la nube pública.

Ejemplo: Uber reveló que su cuenta de Amazon Web Services (AWS) fue hackeada a finales de 2016, comprometiendo la información personal de 57 millones de usuarios en todo el mundo.

2.1.2 Configuración incorrecta y control de cambios inadecuado

La configuración incorrecta se produce cuando los activos informáticos no se configuran correctamente, lo que hace lo que a menudo los deja vulnerables a actividades malintencionadas. La configuración incorrecta podría permitir la eliminación o modificación de recursos que podría conllevar a la interrupción del servicio.

Ilustración 3 - configuración Incorrecta

Ejemplos relacionados con una configuración incorrecta serían:

- Contenedores de almacenamiento de datos no seguros
- Permisos excesivos
- Las credenciales predeterminadas y los ajustes de configuración no han cambiado
- Controles de seguridad estándar deshabilitados.

Al diferir tanto las metodologías de computación en la nube con las metodologías de las tecnologías de le información tradicional ocasiona que los cambios sean más complicados de controlar. En la nube el ciclo de vida de los cambios se realiza en segundos por eso requiere un enfoque ágil para el control de cambios.

El impacto empresarial de un elemento mal configurado puede ser grave dependiendo de la naturaleza de la configuración incorrecta y la rapidez con la que se detecta y mitiga

Ejemplo: En 2018, una base de datos Elasticsearch no segura propiedad de Exactis resultó en otra violación masiva que contenía datos altamente personales de 230 millones de Estados Unidos. consumidores. El servidor de bases de datos estaba configurado para ser accesible al público.

2.1.3 Falta de arquitectura y estrategia de seguridad en la nube

El mayor desafío durante la migración de partes de su infraestructura de TI a nubes públicas es la implementación de una arquitectura de seguridad adecuada para resistir los ciberataques. La migración de entornos TI a nube no consiste solo en implementar los mismos controles de seguridad que se tienen en la TI a la nube, y hay que comprender que subir información a la nube es un modelo de responsabilidad compartida.

Ilustración 4 - Falta de estrategia

Al pretender hacer estos cambios de una forma rápida suele repercutir en la seguridad lo que conlleva una falta de arquitectura y estrategia de seguridad en la nube, lo que hace que las organizaciones sean vulnerables a ataques cibernéticos exitosos.

La estrategia de seguridad adecuadas son elementos necesarios para mover, implementar y operar de forma segura en la nube. Los ciberataques exitosos pueden tener un impacto severo en las empresas, incluyendo pérdidas financieras, daños a la reputación, repercusiones legales y multas sin importar el tamaño que tenga la empresa.

Ejemplo: Los investigadores del Centro de Seguridad De Kromtech descubrieron un grupo de datos pertenecientes a la aplicación Honda Connect, que fue expuesto en línea. Los datos se almacenaron en dos buckets de Amazon AWS S3 no seguros, de acceso público y desprotegidos.

2.1.4 Identidad, Credenciales, Acceso y Administración de Claves Insuficientes

La computación en la nube introduce varios cambios en las prácticas tradicionales de administración interna del sistema relacionadas con la gestión de identidades y acceso (IAM). En la configuración de la nube pública y privada, se debe administrar IAM sin comprometer la seguridad.

Ilustración 5 - Identidad y CA

Los incidentes de seguridad y las violaciones de datos pueden ocurrir debido a lo siguiente:

- Protección inadecuada de las credenciales.
- Falta de rotación automatizada regular de claves criptográficas, contraseñas y certificados.

- Falta de sistemas escalables de administración de identidad, credenciales y acceso.
- Error al utilizar la autenticación multifactor.
- No usar contraseñas seguras.

La falta de una correcta gestión de la identidad puede permitir el acceso no autorizado a los datos y lo que causaría daños potencialmente catastróficos a las organizaciones o a los usuarios finales.

Ejemplo: En diciembre de 2018, un estudiante de German hackeó datos protegidos por contraseñas débiles y compartió la información utilizando una plataforma en la nube.

2.1.5 Robo de credenciales

El robo de credenciales es una amenaza en la que los atacantes malintencionados obtienen acceso a cuentas con privilegios o sensibilidad. En entornos en la nube, las cuentas con mayores riesgos son cuentas de servicio en la nube o suscripciones. Este tipo de robo de credenciales pueden ocasionar:

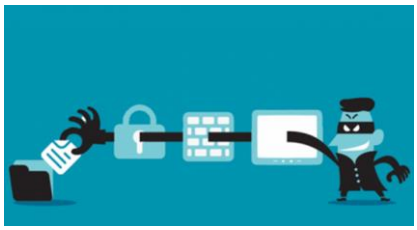


Ilustración 6 - Robo de credenciales

- Perdida de datos
- interrupción servicio de la nube
- Perdida de activos

Estos riesgos dependen del modelo de entrega de servicios en la nube, así como el de su organización y gobierno.

Ejemplo: En 2014, la cuenta de AWS de Code Spaces, una antigua empresa de servicios de alojamiento de código, se vio comprometida cuando no pudo proteger su consola administrativa con autenticación multifactor. El negocio se vio obligado a cerrar después de la destrucción de sus activos.

2.1.6 Amenaza Interna de información privilegiada

Un *CERT* define una amenaza de información privilegiada como *"la posibilidad de que una persona que tiene o tuvo acceso autorizado a los activos de una organización utilice su acceso, ya sea de forma malintencionada o involuntaria, para actuar de una manera que podría afectar negativamente a la organización".*

Ilustración 7 - Amenaza interna

Las amenazas internas pueden ocasionar:

- Pérdida de información.
- Tiempo de inactividad del sistema. Además, la pérdida de datos u otros daños Reducir la confianza en los servicios de la empresa.

Ejemplo: Los servidores en la nube mal configurados, los incidentes de backup en red y otros sistemas configurados incorrectamente fueron responsables de la exposición de más de 2 mil millones de registros.

2.1.7 Interfaces y API inseguras

Los proveedores de servicios en la nube exponen un conjunto de interfaces de usuario de software (UI) y API para permitir a los clientes administrar e interactuar con los servicios en la nube. La seguridad y la disponibilidad de los servicios generales en la nube dependen de la seguridad de estas API.

Ilustración 8 - Apis Inseguras

Desde la autenticación y el control de acceso hasta el cifrado y la supervisión de la actividad, estas interfaces deben diseñarse para protegerse contra intentos accidentales y malintencionados de eludir la directiva de seguridad. Las API mal diseñadas podrían provocar un uso indebido o, lo que es peor, una pérdida de datos.

Aunque la mayoría de los proveedores de servicios en la nube se esfuerzan por garantizar que la seguridad esté bien integrada en sus modelos de servicio, es fundamental que los consumidores de esos servicios comprendan las implicaciones de seguridad asociadas con el uso, la administración, la orquestación y la supervisión de estos.

Ejemplo: Facebook anunció una violación significativa de datos que afecta a más de 50 millones de cuentas el 28 de septiembre de 2018.

2.1.8 Panel de Control Escaso

Cuando se realizan proyectos para pasar de una solución on-premise a la nube se plantean algunos desafíos para crear un programa de protección y almacenamiento de datos los suficientemente robusto, por lo que el usuario ahora debe desarrollar nuevos procesos para la duplicación de datos, la migración y el almacenamiento de datos y, si

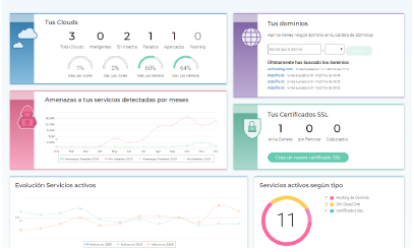


Ilustración 9 - Panel de control escaso

utiliza varias nubes, se vuelve aún más complicado. La mejor solución para abordar este desafío es la de disponer de un panel de control que permita la seguridad y la integridad de los datos.

Si el panel de control es débil significa que la persona a cargo ya sea un arquitecto del sistema o un ingeniero de DevOps, no tiene el control total de la lógica, la seguridad y la verificación de la infraestructura de datos, en el que no conoce la configuración de seguridad, cómo fluyen los datos y dónde existen puntos ciegos arquitectónicos y puntos débiles. Estas limitaciones podrían provocar daños en los datos, falta de disponibilidad o fugas.

Ejemplo: El plano de administración de un servicio en la nube es muy crítico y debe estar adecuadamente protegido por los controles de identidad y acceso.

2.1.9 Fallos de infraestructura y aplicación

Los proveedores de servicios en la nube a la hora de publicar sus servicios y querer hacer que el acceso sea lo más fácil para los consumidores tienden a cometer errores en la infraestructura de acceso a la nube, como por ejemplo en las APIS, que son las que proporcionan el acceso al servicio que proporciona la nube, y una implementación deficiente de estas, ofrece a los atacantes la oportunidad de interrumpir a los clientes en la nube interrumpiendo la confidencialidad, integridad o disponibilidad del servicio.

Ilustración 10 - Fallos de infraestructura

También se comete el error de pensar que las aplicaciones que funcionan en entornos *on-premise* van a funcionar en entornos de nube sin hacer ninguna rediseño de esta.

Ejemplo: Muchas organizaciones todavía se basan únicamente en nombres de usuario y contraseñas, ignorando las capacidades de seguridad actualizadas, como el inicio de sesión único (SSO), la federación de identidades y la autenticación multifactor (MFA).

2.1.10 Visibilidad limitada del uso de la nube

La visibilidad limitada del uso de la nube se produce cuando una organización no posee la capacidad de visualizar y analizar si el uso del servicio en la nube dentro de la organización es seguro o malintencionado.

Ilustración 11 - Visibilidad limitada uso nube

Los riesgos son generalizados, pero pueden resumirse con los siguientes puntos:

- Falta de gobierno.
- Falta de conciencia.
- Falta de seguridad.

Ejemplo: Según la investigación de 2018 llevada a cabo por la empresa de seguridad en la nube Lacework: "Más de de 22.000 sistemas de orquestación de contenedores y gestión de API están desprotegidos o disponibles públicamente en Internet.

2.1.11 Abuso y uso nefasto de servicios en la nube

Los actores malintencionados pueden aprovechar los recursos de computación en la nube para dirigirse a usuarios, organizaciones u otros proveedores de nube. Para hacer uso indebido de los recursos de las nubes para :

Ilustración 12 - Abuso y uso nube

- Hospedar malware
- Lanzamiento de ataques DdoS
- Campañas de spam y phishing por correo electrónico
- "Minería" para moneda digital
- Fraude de clics automatizado a gran escala
- Ataques de fuerza bruta de bases de datos de credenciales robadas
- Alojamiento de contenido malicioso o pirateado.

Ejemplo: La variante Zepto de la Locky ransomware se propaga a través de servicios en la nube como Microsoft OneDrive, Google Drive y Box mediante el intercambio de un archivo malicioso con las víctimas potenciales.

2.2 Riesgos Detectados por Gartner (Gartner, 2008)

Gartner desde su posición de analista de las tecnologías de la información, también ha realizado recientemente el informe "*Assessing the Security Risks of Cloud Computing"* sobre los principales riesgos en servicios en la nube.

2.2.1 Accesos con Usuarios Privilegiados

El procesamiento o tratamiento de datos sensibles fuera de las instalaciones de la empresa conlleva un riesgo inherente, ya que es posible que estos servicios externos sorteen los controles físicos, lógicos y humanos siendo, por este motivo, necesario conocer quién maneja dichos datos. Por tanto, se hace obligatorio consensuar con el proveedor los usuarios que tendrán acceso a esos datos, para minimizar así los riesgos de que haya usuarios con elevados privilegios que no deberían tener acceso a los datos.

Ilustración 13 - Acceso Usuarios Privilegiados

2.2.2 Cumplimento normativo

Los clientes son en última instancia responsables de la seguridad e integridad de sus datos, aunque estos se encuentren fuera de las instalaciones y gestionados por un proveedor de servicios en la nube. Los prestadores de servicios tradicionales se hallan sujetos a auditorías externas y certificaciones de seguridad, por lo tanto los proveedores de servicios en la nube también deben acogerse a este tipo de prácticas. Si se negasen a este tipo de auditorías no se les debería confiar los datos sensibles de la empresa. Es la denominada responsabilidad compartida.

Ilustración 14 - Cumplimiento normativo

2.2.3 Localización de los datos

Al utilizar entornos en la nube no se conoce de forma exacta en qué país están alojados. Se debe consultar con los proveedores cuál es el marco regulatorio aplicable al almacenamiento y procesado de datos, siendo una buena práctica cerrar un acuerdo con el proveedor para que el tratamiento de los datos se subyugue al marco legal del país del suscriptor del servicio.

Ilustración 15 - localización datos

2.2.4 Aislamiento de datos

Los datos en los entornos en la nube comparten infraestructura con datos de otros clientes. El proveedor debe garantizar el aislamiento de los datos de los respectivos clientes. El prestador del servicio debe garantizar que los datos en reposo estarán correctamente aislados y que los procedimientos de cifrado de la información se realizarán por personal experimentado, ya que el cifrado de los datos mal realizado también puede producir problemas con la disponibilidad de los datos o incluso la pérdida de los mismos.

Ilustración 16 - aislamiento de los datos

2.2.5 Recuperación

Los proveedores de servicio deben tener una política de recuperación de datos en caso de desastre. Asimismo, es muy recomendable que los datos sean replicados en múltiples infraestructuras para evitar que sean vulnerables a un fallo general. Se debe exigir a los proveedores los datos sobre la viabilidad de una recuperación completa y el tiempo que podría tardar.

Ilustración 17 - Recuperación

2.2.6 Soporte investigativo

La investigación de actividades ilegales en entornos de la nube puede ser una actividad casi imposible, porque los datos y logs (registros de actividad) de múltiples clientes pueden estar juntos e incluso desperdigados por una gran cantidad de equipos y centros de datos. Lo recomendable será que el proveedor garantice que los logs y los datos de los incidentes se gestionan de una forma centralizada.

Ilustración 18 - soporte investigativo

2.2.7 Viabilidad a largo plazo

En un entorno ideal un proveedor de servicios en la nube siempre permanecerá en el mercado dando un servicio de calidad y con una disponibilidad completa, pero el mercado es cambiante y cabe la posibilidad de que el proveedor sea comprado o absorbido por alguno con mayores recursos. El cliente debe asegurarse que podrá recuperar sus datos.

Ilustración 19 - viabilidad a largo plazo

3. Requisitos Seguridad en la nube pública

Después de conocer los riesgos y amenazas que se encuentran hoy en día los servicios en la nube, a continuación, se especifican las referencias de recomendaciones y buenas prácticas derivadas de estándares internacionales, relativos al diseño arquitectura y gobierno de la seguridad en la nube, con el fin de evitar estos riesgos y amenazas.

Para ello vamos a definir un *marco de trabajo* de requisitos de seguridad donde detallaremos requisitos de seguridad para cada uno de los dominios más característicos a nivel de seguridad para crear una aplicación en una nube publica, que son gobierno, arquitectura y diseño de seguridad.

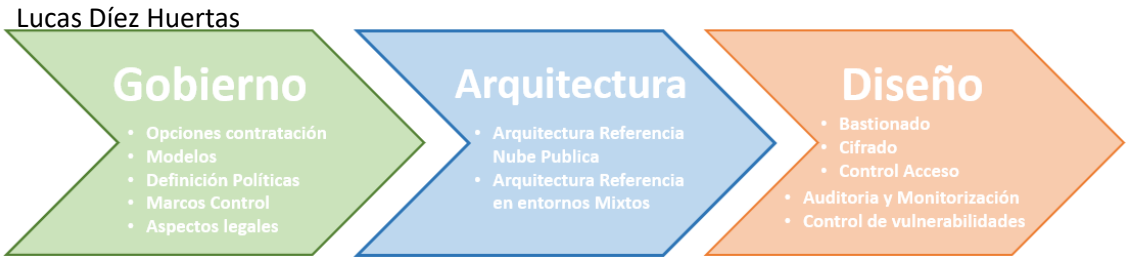


Ilustración 20 - Marco de trabajo para diseño de seguridad en la nube

A continuación se muestra desarrollado el *marco de trabajo* de requisitos de seguridad que se ha creado tanto para aplicaciones que se quieran desplegar en un entorno virtual clásico como para otras aplicaciones que se quiera utilizar a tecnología de contenedores.

3.1 Gobierno de la seguridad en la nube

3.1.1 ¿Qué es gobierno en la nube?

Se puede definir como gobierno al conjunto de políticas y normas basadas en la evaluación del riesgo dentro de un marco acordado representado por procedimientos de auditoría, medición y presentación de informes.

Ilustración 21 - Que es Gobierno en la nube?

En un entorno en la nube pública, los participantes acuerdan promover y establecer expectativas conjuntas de seguridad y niveles de servicio. El gobierno también definirá el proceso para cualquier respuesta a una violación del protocolo, y quienes son los responsables de la mitigación y la comunicación de esta.

3.1.2 La necesidad de gobierno en la nube

La introducción de la computación en la nube en una organización afecta a roles, responsabilidades, procesos y métricas. Sin un gobierno de la nube para proporcionar directrices y adquirir y operar eficientemente los servicios, una organización puede encontrarse frente a estos problemas comunes:

- No estar alineados con los objetivos empresariales
- Revisiones frecuentes de excepciones a políticas
- Proyectos estancados
- Sanciones regulatorias por falta de cumplimiento
- Excesos presupuestarios
- Evaluaciones de riesgos incompletas

3.1.3 Opciones de contratación

Se ofrecen tres opciones de contratación o tipos de servicio en la nube: (Evaluando Cloud, 2020)

a) **SaaS** (*Software as a Service*) o software como servicio, directo para su consumo por los usuarios finales. Por ejemplo CRM, ERP o correo electrónico bajo demanda, escritorio virtual, comunicación, Juegos. Esta modalidad ofrece la ventaja de reducir costes, tiempos de despliegue, escalabilidad y facilidad de uso, pero en contra tiene la desventaja de la dificultad de integrarse con aplicaciones ya existentes en la organización, la gran dependencia con el proveedor de nube y la desconfianza que crea la nube de por sí.

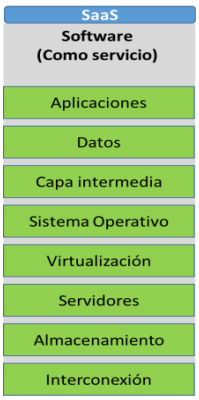


Ilustración 22 - SaaS

b) **PaaS** (*Platform as a Service*) o plataforma como servicio el proveedor entrega una plataforma al cliente con hardware, sistema operativo y middleware o APIS necesarias para actividades de desarrollo o despliegue de aplicaciones como servidores web, herramientas de desarrollo, bases de datos, Big Data, para que el cliente pueda un servicio web o una aplicación. Este modelo nos ofrece la ventaja de poder administrar fácilmente la plataforma e integrarse con el resto así como hacer desarrollos propios en la propia plataforma.

Ilustración 24 - PaaS

c) **IaaS** (*Infrastructure as a Service*) o infraestructura como servicio para administradores TIC: el proveedor de nube entrega al cliente acceso a la infraestructura de la nube para que despliegue máquinas virtuales, servidores, almacenamiento, balanceadores de carga, equipos de comunicaciones, cortafuegos, a demanda en función de las necesidades del cliente. Este modo tiene la ventaja de que el cliente tiene la capacidad de elegir toda la infraestructura que necesite, con una rápida instalación y facilidad para desplegar aplicaciones. Pero por el contrario es un servicio externalizado es más complejo solucionar algún problema grave de forma rápida ya que se depende del proveedor del servicio

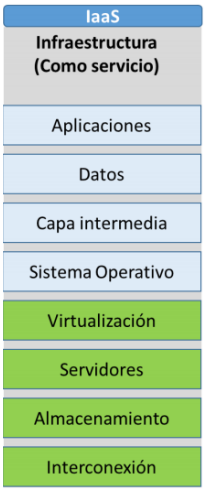


Ilustración 23 - IaaS

3.1.4 Modelos de despliegue

(Evaluando Cloud, 2020)

a) **Nube Publica:** El proveedor ofrece el mismo servicio a muchos clientes desde el mismo centro de datos de forma que comparten recursos (de almacenamiento, de proceso). Esto hace posible una gran escalabilidad y eficiencia y generalmente un precio asequible. Los clientes utilizan los servicios que son procesados en el mismo servidor y pueden compartir espacio en disco u otras infraestructuras de red con otros clientes.

Ilustración 25 - Nuble pública

b) **Nube Privada:** Son servicios en los que los recursos se entregan de forma exclusiva, privada, al cliente, al que se lo ofrece el control sobre el servicio que alquila. En estos casos seguimos disfrutando de la flexibilidad de escalar el servicio si necesitamos contratar más recursos. Además, al ser un servicio privado, el

Ilustración 26 - Nube privada

proveedor garantiza la separación de los recursos que alquilamos y de los que alquilan otros clientes.

c) **Nube Hibrida:** Combinan servicios en nube pública y en nube privada con una administración única, es decir, gestionados desde un mismo panel de gestión. También se integran con servicios en nuestras oficinas (on-premise). Con la mezcla entre servicios públicos y privados se consiguen reducir costes frente a la nube privada. Un ejemplo de servicios en nube híbrida se da cuando una empresa contrata un servicio de CRM en la nube pública pero el servicio de ERP e la nube privada. De este modo nuestros datos sensibles permanecen bajo nuestro estricto control mientras que el servicio CRM puede ser administrado por el proveedor que se encarga de mantenerlo online, vigilar que tenga suficientes recursos para soportar los picos de usuarios, etc.

Ilustración 27 - Nube hibrida

3.1.4 Como implementar Gobierno en la nube

Para implementar el gobierno de la seguridad en la nube de un entorno IaaS, vamos a basarnos en una publicación Gartner. (Richard Watson, 2019)

Alinear el gobierno con la estrategia en la nube de su organización

La creación de una estrategia integral en la nube puede ayudar a maximizar los beneficios empresariales de la nube y de mantener el control en una era de servicios bajo demanda. La estrategia en la nube de cada organización será única, basada en los objetivos de negocio y los requisitos técnicos.

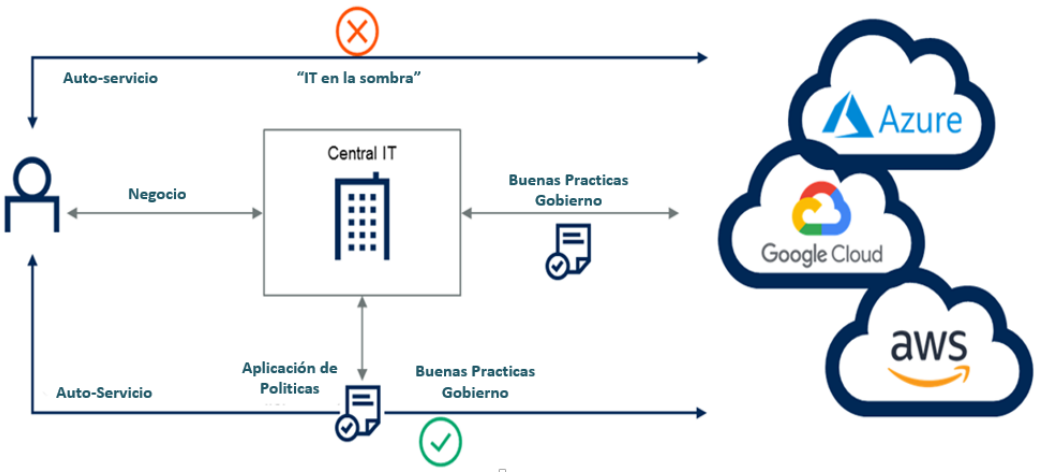


Ilustración 28 - alineación gobierno en la nube

Sus políticas de gobierno no deben ser el lugar para definir el uso de la nube o no, más bien, deben asegurarse de que se está implementando una estrategia

integral en la nube de la manera que protege a la organización, que es una de las misiones principales de *"el gobierno"* de la tecnología de cualquier tipo evitando la construcción de sistemas en la nube que no estén bajo las políticas diseñadas por el equipo de gobierno, los denominados "*equipos de IT en la sombra".*

Formar el equipo de gobierno

Una de las primeras cosas que los departamentos de TI deben hacer es crear un equipo encargado de investigar, definir e implementar los cambios de gobierno necesarios dentro de la organización. Para hacer un uso seguro, eficiente y conforme de la computación en la nube se requerirán nuevas estructuras de equipo, a menudo con enfoques multidisciplinares.

Ilustración 29 - Formar gobierno

Este equipo de gobierno en la nube tendrá que ser utilizado como una entidad estable dentro de la organización, no solo como un equipo de proyecto que se reúne y luego se disuelve después de un período de tiempo. Por lo tanto, las responsabilidades de este grupo de gobierno deben recaer en un grupo de "centro de excelencia en la nube" dentro de la organización.

Describir sus principios de gobierno en la nube

Los principios de gobierno en la nube se basarán en los principios generales de gobierno de TI, pero obtendrán un uso muy específico del consumo de servicios de proveedores en la nube. Para la definición de estos principios hay que tener en cuenta el servicio de nube publica que se contrata ya que ofrecen servicios tan diversos.

Para definir estos principios de gobierno en la nube tenemos que basarnos en:

- Definir la política antes de pensar en cómo aplicarla automáticamente con una herramienta nativa del proveedor de la nube.
- Se debe utilizar la nube de una manera de autoservicio, usando consolas web de proveedores de nube, API e interfaces de línea de comandos (CLI) directamente, y no tener acceso mediado por un catálogo de servicios o una herramienta diseñada por su organización.
- Las políticas deben ser independientes del proveedor.
- Los mecanismos que funcionan para 10 cuentas y docenas de recursos no funcionarán para cientos de cuentas y miles de recursos.

Alinear su organización con la terminología

Se define un marco de trabajo para poder alinear la organización con la terminología cumpliendo los siguiente pasos:

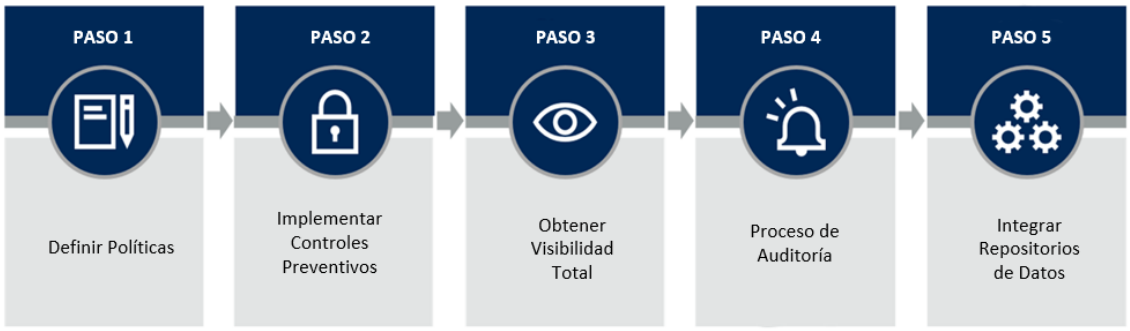


Ilustración 30 - Alinear organización y terminología

Paso 1 - Definir políticas

Antes de pasar a desarrollar este apartado vamos a definir el termino política. Entendemos por política la declaración de reglas e intenciones que no deben estar abiertas a la interpretación, por ello se tienen que escribir en lenguaje común utilizando términos de forma coherente.

El equipo de gobierno de la organización tendrá que definir un conjunto de políticas e implementar la automatización para garantizar los resultados de gobierno deseados. El enfoque de la organización de TI debe centrarse en permitir que la empresa use tantos servicios en la nube como sea necesario, pero solo de una manera que signifique que tiene visibilidad y control sobre quién está haciendo qué, en la nube pública. Las tareas principales que se tienen que realizar en este punto son:

a) Definir los objetivos para las políticas de gobierno en la nube.
b) Escribir sus políticas y asignar a los dominios de la plataforma de administración en la nube.
c) Asignar responsables y tomar decisiones que impacten las políticas.
d) Definir estrategia de excepción de política

a) Definir sus objetivos para las políticas de gobierno en la nube

Los objetivos son una declaración de lo que está tratando de lograr con las políticas de gobierno. Su estrategia en la nube incluirá objetivos de adopción de la nube. Estos objetivos de gobierno en la nube son más específicos que impulsarán cada una de sus políticas. Los objetivos ayudan a las personas a entender por qué la política es necesaria y ayudan a obtener la aceptación de restricciones que algunos preferirían no cumplir. Algunos de los objetivos de gobierno comunes son:

- Expansión de la cuenta de control
- Impedir el acceso no autorizado
- Proteger los datos confidenciales y los recursos en la nube
- Cumplir con las regulaciones de la industria y regionales
- Prevenir la TI en la sombra
- Control de la expansión de activos
- Cumplir con los acuerdos de nivel de servicio (SLA), maximizar la disponibilidad y minimizar el tiempo de recuperación
- Asegurar que la capacidad no sea una restricción para el negocio
- Atribuir los costos con precisión a la unidad organizativa utilizando el recurso
- Minimizar el gasto de recursos despilfarrador
- Aislar un problema de gobernanza (limitar el "radio de explosión")
- Implementar un principio de seguridad de privilegios mínimos.

b) Escribir sus políticas y asignar a los dominios de la plataforma de administración en la nube.

Los dominios que vamos a definir para este apartado son :

- Identidad, seguridad y cumplimiento: Administrar y proteger el acceso a los servicios en la nube, para aplicar una línea de base de configuración de seguridad.
- Inventario y clasificación: descubrir y mantener un inventario de recursos en la nube, así como la capacidad de supervisar los cambios y administrar las configuraciones.
- Migración en la nube, copia de seguridad y recuperación ante desastres: capacidad de replicar datos para migrar cargas de trabajo, implementar arquitecturas de continuidad del negocio o recuperación ante desastres, o proteger los datos contra eliminaciones accidentales o actividades maliciosas.

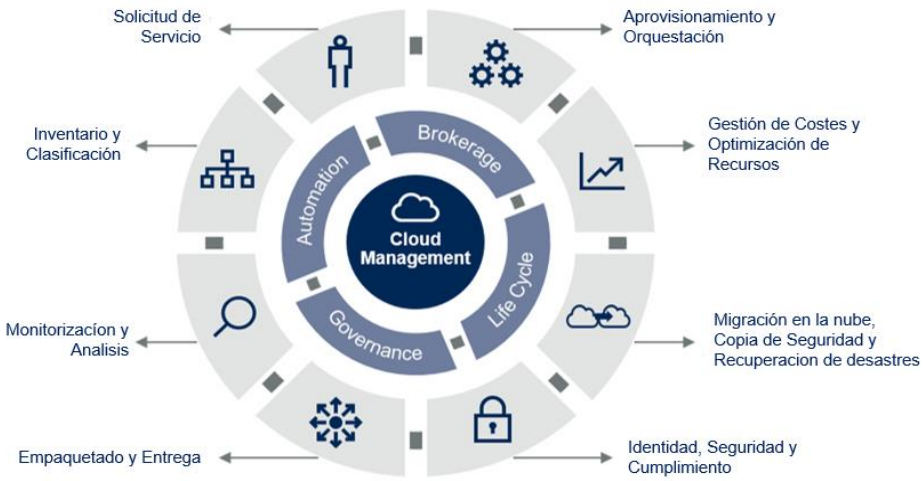


Ilustración 31 - Escribir políticas y asignar dominios

- Aprovisionamiento y orquestación: utilizadas para crear, modificar y eliminar recursos y para organizar los flujos de trabajo de aprovisionamiento y las operaciones de administración.

- Gestión de costes y optimización de recursos: tareas necesarias para realizar un seguimiento y optimizar el gasto de forma continua.
- Monitorización y análisis: recopilación de métricas de rendimiento y disponibilidad, así como la inteligencia para analizar datos para evitar incidentes o automatizar la resolución de estos.
- Solicitud de servicio: tareas necesarias para recopilar y satisfacer las solicitudes de los usuarios internos para acceder a los servicios en la nube
- Empaquetado y entrega: proporcionar que funcionalidad de administración de la nube esté disponible para los usuarios finales.

c) Asignar responsables y tomar decisiones que impacten las políticas

Definir políticas es importante, pero estas son papel mojado sin personas responsables que las implementen, y el proceso de gobierno no consiste únicamente en redactar una lista de políticas, también es responsabilidad del equipo de gobierno asignar personas responsables de las políticas dentro del equipo de gobierno o centro de excelencia en la nube y sobre todo crear los procesos necesarios para implementar esas políticas.

d) Definir estrategia de excepción de política

La implementación del gobierno en la nube también debe cubrir qué hacer con los escenarios de excepción a las directivas. Puede haber adenda a cada directiva especificando las circunstancias en las que las excepciones son permitidas.

Paso 2 - Implementar controles preventivos

En este paso se tienen que realizar las siguientes tareas:

a) Identificar las políticas para las que puede implementar controles preventivos.

Los controles preventivos evitan las acciones que no desea que se lleven a cabo en su entorno de nube. Son políticas que impiden acciones que sabemos que probablemente sean perjudiciales para nuestros objetivos de gobierno en la nube y suelen ser principalmente políticas relacionadas con el aprovisionamiento de cuentas, la administración de roles y el control de acceso porque se trata de actividades de alto riesgo.

b) Configurar políticas en las herramientas nativas del proveedor de nube

Debe configurar directivas en las herramientas nativas o el formato de código del proveedor de nube para automatizar su aplicación. La implementación de directivas en entornos de nube tiene distintas etapas de "crear" y "asignar". Cada

proveedor tiene un lenguaje específico para poder definir las directivas para generar las políticas.

c) Definir el flujo de trabajo de creación de cuentas de usuario

Para asegurarse de que las directivas preventivas se asignan sistemáticamente a cuentas de usuario, identidades o suscripciones, debe automatizar el proceso de creación de la cuenta. Cada vez que un nuevo usuario solicita acceso a un servicio de proveedor de nube, el proceso automatizado debe asignar el conjunto correcto de directivas preexistentes en función de los privilegios del usuario

d) Automatizar el flujo de trabajo de creación de cuentas y adjuntar políticas.

Cada proveedor tiene una forma diferente en la que las directivas se asocian con las cuentas de acceso, por lo que hay que entender como lo realiza cada uno para poder automatizar el flujo de creación de cuentas.

Paso 3 - Obtener visibilidad total

Cuanta más visibilidad se tiene, aumenta la capacidad de gobernar mejor el consumo de servicios en la nube. Sin embargo, es imposible gobernar las implementaciones en la nube que no sabe que existen. Por lo tanto, es fundamental que haya visibilidad de qué proveedores y qué servicios se están utilizando. Es posible que los proveedores no tengan de forma nativa un proceso de detección o alerta de activos para nuevas implementaciones y, si lo hacen, es posible que no estén habilitados o configurados de forma predeterminada. Por lo tanto, deberá establecer un proceso para la detección de activos.

Una vez que tenga visibilidad de todo el uso de la nube, puede supervisar el consumo, lo que le permite administrar y optimizar mejor las implementaciones en la nube. Una ventaja de una gobernanza bien organizada (por ejemplo, etiquetado detallado y bien pensado) es que le permite optimizar sus implementaciones y ahorrar dinero.

La visibilidad también va más allá de los cambios discretos y deliberados del entorno, para incluir métricas de disponibilidad, métricas de estado, registros de flujo de red, métricas de rendimiento, métricas de costos y métricas de seguridad, entre otros. Habilitar el nivel de visibilidad más detallado es fundamental porque establecerá directivas que especifiquen valores de métricas y desencadenadores para decidir si se infringe una directiva.

Paso 4 - Crear un proceso de auditoría para implementar controles retrospectivos.

a) Establecer auditoría automatizada continua

Un proceso de auditoría automatizado continuo es fundamental para permitir el gobierno de la nube pública en su conjunto y la operación de autoservicio en particular. Con los usuarios finales ganando más autonomía en la gestión de sus propios recursos, es obligatorio que el departamento de TI administre el riesgo y

el cumplimiento mediante la auditoría de configuraciones y la corrección de las infracciones de las políticas establecidas.

El departamento de IT supervisa la actividad de los usuarios en la nube, audita las configuraciones y las compara con una línea base para que a través de políticas de identidad los usuarios que consumen los servicios de la nube no puedan realizar operaciones que no tengan permitidas.

b) Mapear las políticas restantes a herramientas que pueden automatizar las comprobaciones de políticas y la aplicación

Implementar controles preventivos para las políticas que no puede permitir que sean violadas de ninguna manera, dentro de los límites que establezcan las herramientas del proveedor de nube.

c) Definir resultados de corrección.

En el momento en que la auditoría encuentra una infracción de política, se debe definir lo que sucede en cada caso:

"Remediación suave": envíe una alerta, incluido el aviso de una acción que un usuario debe realizar para volver a cumplir la política que ha incumplido.

Remediación dura": se aplican automáticamente el cumplimiento realizando una acción en el entorno de la nube.

"Período de gracia": es una combinación de corrección suave y dura, que especifica una acción requerida dentro de un período de tiempo antes de que se imponga una corrección dura.

d) Implementar el flujo de trabajo de corrección automatizada.

Cada vez que un usuario o servicio inicia un cambio en un recurso en la nube.

1 Ejecute una comprobación cada vez que una nueva entrada en una herramienta de registro en la nube notifique un cambio en el entorno.
2 Compruebe el nuevo estado del entorno con la lista completa de directivas, actualizando una base de datos de directivas en una de las herramientas nativas del proveedor.
3 Si se ha infringido una de las directivas, compruebe qué resultado de corrección se requiere para cada directiva.
4 Si se ha infringido una de las directivas, compruebe qué resultado de corrección se requiere para cada directiva.

Paso 5 - Implementar la estrategia de integración de herramientas

a) Integrar repositorios de datos

Cada herramienta que se utiliza para implementar la gobernanza administra una base de datos interna donde almacena el inventario y el estado de los recursos. Para evitar la desalineación del estado, las organizaciones deben elegir una *única fuente de confianza* y asegurarse de que todas las demás herramientas de administración *apunten* y sincronicen con ella y una vez establecida esta fuente de confianza, todas las demás herramientas deben ser capaces de supervisar el cambio de estado de los recursos, detectarlo y reflejarlo en su almacén de datos interno tan pronto como se produzca.

b) Identidad federada y Habilitar SSO

Múltiples herramientas que vamos a utilizar para el control de la seguridad en nuestra nube vienen también con múltiples consolas de administración basadas en web y portales, por lo que los miembros del equipo de operaciones en la nube tendrán que saltar constantemente de un portal a otro para realizar una serie de tareas operativas, con lo que las organizaciones deben garantizar la accesibilidad de todos los portales de administración con una única credencial para cada miembro del equipo.

Para conseguir este objetivo se puede implementar una arquitectura federada que delegará la autenticación en un proveedor de identidad externo y permitirá la implementación de SSO (Single Sign-On), así como un registro de auditoria de los accesos realizados por el equipo de operaciones.

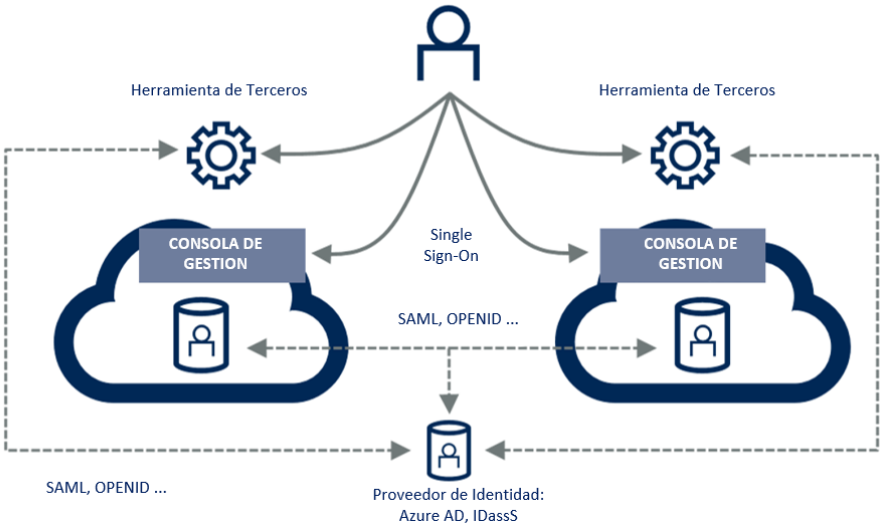


Ilustración 32 - Identidad federada y habilitar SSO

3.1.5 Marcos de Control

Para poder implementar el gobierno en la nube se pueden seguir los siguientes marcos de control:

Certificación CSA STAR : La certificación (CSA STAR, 2019) garantiza , por un tercero independiente, la seguridad de un proveedor de servicios Cloud, basándose en el cumplimiento de la norma ISO/IEC 27001 y el conjunto de criterios especificados en la Matriz de Controles en la Nube (Cloud Controls Matrix), esta matriz tiene 133 controles divididos en las siguientes áreas:

Seguridad de aplicaciones e interfaces
- Auditoría y Cumplimiento
- Gestión de la Continuidad del Negocio y Resiliencia Operativa
- Control de cambios y gestión de la configuración
- Seguridad de datos y gestión del ciclo de vida
- Seguridad del centro de datos
- Cifrado y gestión de claves
- Gobierno y gestión de riesgos
- Recursos humanos
- Gestión de acceso e identidades
- Seguridad de la infraestructura y la virtualización
- Interoperabilidad y portabilidad
- Seguridad móvil
- Gestión de incidentes de seguridad, E-Discovery y Cloud Forensics
- Amenazas y vulnerabilidades

ISO 270017 (ISO/IEC JTC 1/SC 27, 2015)**:** Código de prácticas para controles de seguridad de la información para servicios de computación en nube basados en 37 controles de la norma ISO/IEC 27002 (ISO/IEC 27002:2013, 2015), además Incluye siete nuevos controles que tratan:

- La definición de responsabilidades entre el proveedor y el consumidor
- La eliminación de activos cuando un contrato finaliza
- Protección y separación del entorno virtual del cliente
- Como configurar una máquina virtual
- Operaciones y procedimientos relacionados con el entorno en la nube
- Seguimiento de la actividad de clientes en la nube
- Alineación del entorno de la red virtual y en la nube

(**NIST Special Publication 800-146, 2012**):

Cubre los siguientes dominios

Ilustración 33 -Marco Regulatorio NIST

3.1.6 Aspectos legales y contractuales (Cloud Security Alliance, 2018)

Cuando se decide implementar una solución en la nube es necesario tener en cuenta el marco legal existente, tanto del país donde reside la organización como del país del proveedor del servicio en la nube. En el caso de España será de aplicación la Ley Orgánica de Protección de Datos (LOPD), que se cumple gracias a la actuación de la Agencia Española de Protección de Datos.

En un mundo donde los datos circulan de manera global, las empresas tienen que prestar atención a la protección de la privacidad, pues todas en mayor o menor medida tratan con datos personales, ya sean de clientes o de empleados. Es decir, se trata con información considerada como sensible y son datos que deben ser protegidos.

Por ello tenemos que considerar dónde están ubicados los centros de datos del proveedor de servicios de la nube, ya que la legislación sobre seguridad y privacidad varía de unos países a otros. En concreto, para cumplir la legislación en materia de protección de datos personales, los proveedores con centros de datos en el espacio económico europeo nos ofrecen más garantías en materia de protección de datos.

No debemos olvidar que la empresa, si utiliza datos personales es la “responsables del tratamiento” según la RGPD, incluso aunque contratemos a proveedores de servicios en la nube algún servicio en el que se manejen estos datos.

En caso de que estén fuera de la UE podría tratarse de una transferencia internacional de datos, y en este caso sería necesario asegurar que dicho país ofrece unos niveles jurídicos de protección de datos equivalentes a las del espacio económico europeo.

Las transferencias internacionales de datos tienen que contar con la autorización expresa del Director de la Agencia Española de Protección de Datos.

Como en todo acuerdo empresarial, la relación entre el proveedor de servicios en la nube y el cliente debe estar regulada por un contrato y en muchos casos por un Acuerdo de Nivel de Servicio o ANS (o, en inglés, SLA Service Level Agreements). Estos documentos deben definir claramente la posición de cada una de las partes así como sus responsabilidades y obligaciones.

En el contrato se fijará el servicio contratado, su duración, condiciones de finalización y desistimiento, precio y otras condiciones. Entre ellas, las condiciones de uso son una parte importante y de obligada lectura. Definen las características del servicio y su forma de entrega, el uso aceptable que se espera del cliente, la descarga de responsabilidad y la legislación aplicable en caso de conflicto.

3.2 Arquitectura de Seguridad

3.2.1 Arquitectura de Seguridad en la Nube Pública

Antes de definir las formas de conexión entre nubes privadas y nubes públicas o entorno *on-premise*, vamos a definir unos criterios de arquitectura de seguridad para el despliegue de aplicaciones en nuestra nube publica para que siguiendo estos requisitos podamos considerar la arquitectura de estas aplicaciones como seguras, en entornos en los que no utilizaremos contenedores para el despliegue de nuestras aplicaciones ya que en el apartado anterior hemos definido requisitos de seguridad para el despliegue de contenedores y la interconexión entre proyectos y microservicios.

La arquitectura Lógica desde el punto de vista de seguridad está diseñada en base a la definición de 3 grandes zonas, siendo Internet la puerta de entrada a las aplicaciones que van a residir en nuestro entorno de nube pública.

- Zona Frontend.
- Zona Backend.
- Zona Gestión.

Zona Frontales

Es una zona a la que se accede tras pasar por un elemento de seguridad. Accederán los usuarios que tengan privilegios de acceso a las aplicaciones. En esta zona típicamente residirán servicios que necesitan ser protegidos por un elemento de seguridad y que necesitan de la Zona de Backend para proporcionar el servicio.

Zona Backend

Zona a la que se accede tras pasar por un elemento de seguridad. Únicamente accederán las máquinas de la zona Frontal. En esta zona típicamente residirán bases de datos y equipos de lógica de negocio de las aplicaciones, como servidores de aplicaciones, que no debe ser accedida nunca directamente por los usuarios.

Zona Gestión

Zona a la que se accederá para la operación y mantenimiento de todos los servicios y equipamientos del nodo. Para este entorno de nuble publica no se permitirá el acceso directamente desde internet a la red de gestión, se recomienda el despliegue de una maquina denominada “bastión” que sea el punto único de entrada para la operación y mantenimiento y que cumpla las reglas de bastionado indicadas en el punto anterior de requisitos de seguridad.

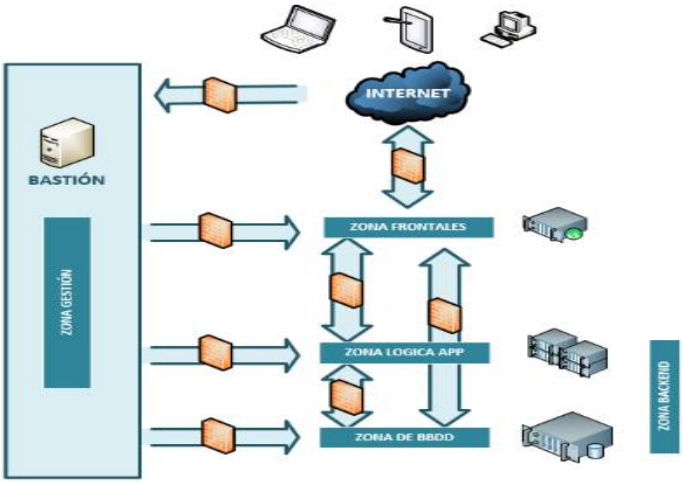


Ilustración 34 - Modelo Arquitectura de seguridad estándar

3.2.2 Arquitectura de seguridad para entornos Mixtos o Híbridos.

La nube híbrida es un tipo de servicio en la nube, que se caracteriza por la combinación de varios entornos de la nube pública y la nube privada. Los distintos recursos virtuales que ofrece una nube híbrida se administran entre los servidores de la empresa que provee el servicio y los servidores de la empresa que utiliza la nube.

Los datos y los procesos que se van a migrar a la nube privada y a la nube pública son organizados por un software de administración y automatización al que los usuarios pueden acceder desde cualquier dispositivo con conexión a Internet. La nube pública y la nube privada que orquestan una nube híbrida son individuales, pero se pueden ejecutar migraciones entre ambas entidades a través de interfaces de programación de aplicaciones (API). Este tipo de arquitectura TI permite que las empresas gestionen cargas en las nubes y extraigan recursos de estas cuando lo necesiten.

También es posible crear una nube híbrida conformada por varias nubes públicas administradas por distintos proveedores. La nube híbrida brinda a las empresas lo mejor de ambas infraestructuras del servicio proporcionado por la nube: es mucho más segura, permite ahorrar costes y ofrece a la organización que la utiliza mayor control de su data.

Definimos 3 casos de uso para conectar estos entornos híbridos o Mixtos.

Caso 1 mediante VPN por internet.

Se contrata un servicio de VPN entre la nube elegida y nuestro entorno de CPD y se establece un canal de comunicación seguro. Este caso solo nos garantiza que el canal es seguro entre nuestra nube publica y nuestro entorno *on-premise*.

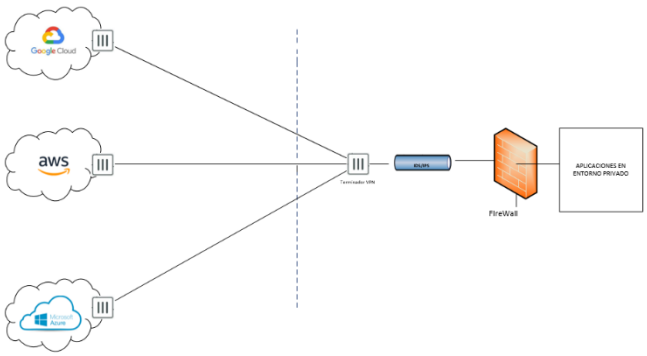


Ilustración 35 - VPN por internet

Caso 2 utilizando herramientas de conectividad proporcionadas por los proveedores de nube. (AWS, 2020), (Google Cloud, 2020), (Microsft, 2020)

En este segundo caso de uso solo tenemos soluciones para AWS y Azure, ya que Google Cloud no ofrece este servicio en su market.

En esta solución utilizamos 2 herramientas que nos ofrecen AWS y Azure para la interconexión entre la nube y el entorno CPD.

Para AWS contratamos el servicio Direct Connect, que vincula su red interna con una ubicación de AWS Direct Connect a través de cable estándar Ethernet de fibra óptica. Un extremo del cable se conecta a su router y el otro al router de AWS Direct Connect. Con esta conexión, puede crear interfaces virtuales directamente en servicios públicos de AWS.

Y para Azure contratamos el servicio ExpressRoute, que se utiliza para conectar una red virtual de Azure y una red local. Una puerta de enlace de red virtual tiene dos propósitos: intercambiar las rutas de IP entre las redes y enrutar el tráfico de red.

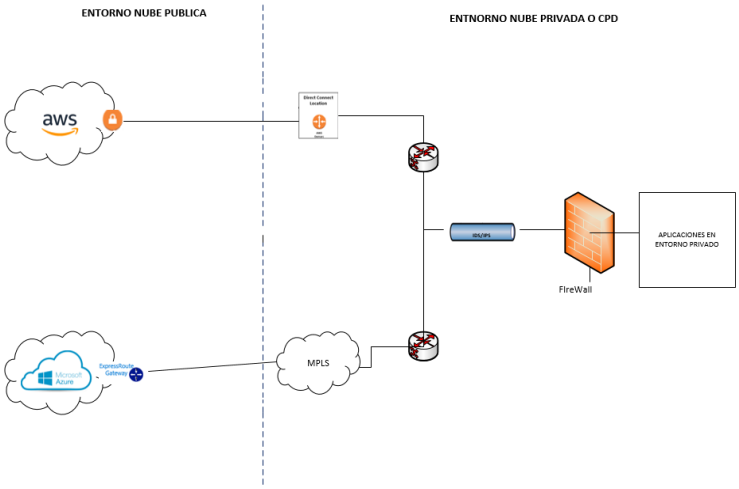


Ilustración 36 - Herramientas de conectividad nube

Caso 3 Fortinet Cloud + Proveedores Cloud (Fortinet, 2020), (AWS, 2020)

Para este tercer caso de uso se han buscado soluciones adicionales a las que ofrecen los proveedores de nube, adaptando estas soluciones para conseguir un mayor nivel de seguridad entre nuestra nube publica y nuestro entorno CPD para eso recurrimos a estudiar la solución de Fortinet, que es la que más se puede adaptar a nuestro ejemplo para este TFM. Esta solución para la seguridad de la nube publica que ofrece soluciones para las nubes de Google AWS y Azure.

Fortinet además de ofrecer una solución de comunicaciones cifrada entre los 2 entornos ofrece además una serie de servicios para proteger tanto la nube como el entorno *on-premise* o con comunicaciones con otras nubes.

Los servicios que se ofrecen son:

- Crear rápidamente políticas para permitir o restringir el acceso a aplicaciones o a categorías enteras de aplicaciones.
- Protege su organización al bloquear el acceso a sitios web maliciosos, pirateados o inapropiados.
- Detección de amenazas avanzadas que realiza análisis dinámicos para identificar malware desconocido anteriormente
- Protege contra los más recientes virus, spyware y otras amenazas a nivel de contenido.
- IPS que protege contra las últimas intrusiones de red al detectar y bloquear las amenazas antes de que lleguen a los dispositivos de red.
- Detecta y detiene las amenazas de malware que se descubren entre las actualizaciones de firmas antes de que puedan propagarse en toda la organización
- Procesa todos los archivos entrantes, los deconstruye y elimina todos los elementos que no coinciden con las políticas del firewall.

- CASB: proporciona visibilidad, cumplimiento, seguridad de datos y protección frente a amenazas para sus servicios basados en la nube.
- Protección de servicio de seguridad industrial: SCADA (control de supervisión y adquisición de datos) e ICS (sistemas de control industrial).
- Realiza comprobaciones contra su red habilitada y proporciona puntajes y recomendaciones a sus equipos operativos.
- Consolida la protección integral necesaria para proteger y defenderse de todos los canales de ataques cibernéticos desde el endpoint hasta la nube.

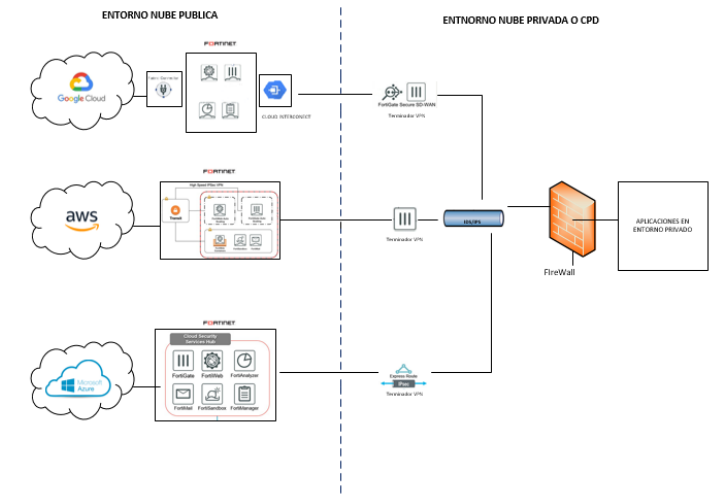


Ilustración 37 - Fortinet Cloud + Proveedores nube pública

3.3 Diseño de seguridad en la nube

3.3.1 Requisitos De Seguridad Generales Para Aplicaciones Estándar

Tal y como hemos visto en los marcos de control para el gobiernos de la nube las normas como la ISO 27000 (ISO/IEC 27002:2013, 2015), guías del NIST (NIST Special Publication 800-146, 2012) y CIS (CIS , 2020), referidas al diseño y desarrollo de aplicaciones que son aplicables a la implementación de la seguridad de estas aplicaciones

Dividiremos en 3 grandes bloques los requisitos de seguridad para las aplicaciones que queremos desplegar en un entorno virtual, *arquitectura de seguridad y bastionado, autenticación y autorización, y monitorización y auditoría*.

Ilustración 38 - Requisitos De Seguridad Generales Para Aplicaciones Estándar

3.3.1.1 Arquitectura de seguridad y bastionado

a) Segmentación

- Limitación del acceso a los activos restringiendo que orígenes podrán acceder a los equipos.
- Los elementos de una aplicación deberán estar segmentados en diferentes ámbitos en función de su nivel de riesgo y exposición.
- Los frontales estarán protegidos por firewalls, y la comunicación de frontales y backend será protegida por un firewall también.
- Para acceder a los activos se hará a través de un frontal que autentique a los usuarios, para que el backend no se exponga directamente a los usuarios finales.
- Definimos 2 frontales diferentes:
  - Frontal Intranet : para el acceso desde redes internas
  - Frontal Extranet: para el acceso desde redes externas (internet)
  - Estos 2 frontales podrán acceder al backend, únicamente a los activos que sean necesarios para el funcionamiento de la aplicación.
- Establecer mecanismos de filtrado para asegurar la separación entre interfaces.

- Deshabilitar el ip_forwarding (tanto para IPv4 como para IPv6) en todos los nodos que no lo necesiten.
- Separar los entornos de productivos y no productivos en las aplicaciones.
- El tráfico entre entornos productivos debe estar aislado de los entornos no productivos.
- En caso de que se requiera conectividad con Internet:
  - Un Frontal Extranet podrá hacerlo directamente
  - Un Backend requerirá hacerlo a través de un proxy, y solo se permitirá tráfico de salida.
  - Un Frontal Intranet no podrá acceder a Internet

b) Bastionado

- Los equipos sobre los que se desplegará el sistema o servicio deberán estar correctamente bastionados, empleando Guías de Bastionado de algún organismo de referencia como el CCN-CERT (CCN-CERT, 2020), CIS (CIS , 2020), NIST (NIST Special Publication 800-146, 2012), etc.

c) Seguridad de los datos y las comunicaciones

- Los datos personales o sensibles deberán estar cifrados, tanto cuando estén almacenados como durante su transmisión, teniendo en cuenta el proceso que se está haciendo con el dato, si se está almacenando, intercambiado u operando con él.
- Los algoritmos de cifrado simétrico recomendados son XSalsa20, ChaCha20, y AES con longitudes de clave de al menos 256 bits, y con un modo de cifrado autenticado como GCM o CCM.
- Se permite el uso de las funciones resumen SHA-2 y SHA-3 para la generación de firmas digitales. No se permite el uso de MDS para este fin.
- Solo se permitirán mecanismos de intercambio de claves con la propiedad de Forward Secrecy, como Diffie-Hellman (DH) con un grupo de 2048 bits o más (no se usarán los parámetros DH estándar, sino que se generarán números primos aleatoriamente para cada servidor), o mecanismos basados en criptografía de curva elíptica seguros como x25519.
- Para la generación de claves, tokens de sesión o cualquier otro parámetro criptográfico se empleará un generador de números pseudoaleatorios criptográficamente seguro (CSPNRG*).
- Los algoritmos de criptografía de clave pública permitidos son:
  - RSA con claves de más de 2048 bits.
  - padding OAEP.
  - RSA-PSS para firma digital.
  - ECDSA con curvas elípticas seguras (ECDSA, 2020), como Ed25519.

- Cifrar las comunicaciones para garantizar la integridad, empleando protocolos seguros como SSH-2 y TLS (TLSv1.2 o TLSv1.3). (Mozilla SSL Configurator Generator, 2020) .
- En caso de que los protocolos de comunicaciones ofrezcan la posibilidad de negociar la utilización de seguridad (p.ej. opciones STARTTLS de SMTP o FTP), se requerirá realizar una conexión segura por defecto
- EL tiempo máximo de vida de los certificados digitales emitidos por la PKI será de 13 meses siguiendo recomendaciones del CAB Forum
- En la distribución de los certificados de la PKI, estos certificados tienen que enviarse junto a la cadena de certificados completa, incluyendo la autoridad de certificación raíz.
- Si se emplean certificados públicos, no será necesario que la cadena de certificados incluya la autoridad de certificación raíz.
- En caso de que el activo tenga relación con medios de pago con tarjetas de crédito, estará sujeto a la normativa PCI

3.3.1.2 Autenticación y autorización

a) Identificación

- Se proporcionará acceso a los activos a los usuarios para cuyo uso hayan sido específicamente autorizados.
- Los accesos, deberán realizarse con usuario nominal con los permisos necesarios para poder desempeñar la tarea que tenga encomendada.
- Lo usuarios con privilegios para un proceso automatizados, se crearán teniendo en cuenta los siguientes requisitos:
    - El responsable del proceso automático justificará y documentará la necesidad de dicho usuario con privilegios
    - Este tipo de usuario tendrá un tiempo de expiración inferior a 3 meses, y se renovará del responsable del usuario privilegiado.
    - Se le asignaran los permisos necesarios para realizar las operaciones necesarias controlando el origen por IP.
    - Se deberá garantizar la trazabilidad de las acciones que se realicen y las personas que lo utilizan en cada momento.
- Se aplicará la solución de un segundo factor de autenticación (2FA) en los siguientes casos:
    - A todas las aplicaciones con información sensible.
    - Sistemas basados en Single Sign-On (SSO)
    - Accesos de administradores

b) Política de contraseñas

- Las contraseñas solo podrán transmitirse por un medio seguro.
- Para facilitar el uso de gestores de contraseñas, ningún sistema o servicio deberá impedir el pegado de contraseñas.
- Las contraseñas nunca deberán almacenarse en texto claro. En su lugar, se deberá utilizar una función resumen (hash) «lenta» como argon2i, scrypt o bcrypt, con un número de iteraciones suficientemente elevado, y utilizar un valor de sal (salt) aleatorio y/o único para cada usuario.
- Las contraseñas deberán tener una longitud mínima de 8 caracteres (recomendada 12) y deberán contener al menos un número, una letra mayúscula y otra minúscula.
- Se deberán permitir espacios, para fomentar el uso de frases de paso (passphrases). Igualmente, se deberá permitir la introducción de caracteres especiales (_*+-$, etc.), aunque no se forzará su uso.
- Se deberán permitir contraseñas de hasta 64 caracteres.
- Las contraseñas no podrán incluir datos fácilmente accesibles sobre el usuario (NIF, nombre, …).
- Se establecerá una lista negra para prevenir el uso de las contraseñas más comunes.
- Las cuentas de usuario con perfil de administrador y las cuentas de usuario privilegiadas deberán tener contraseñas distintas cada una; estas contraseñas deberán constar de un mínimo de 16 caracteres elegidos aleatoriamente y estar formadas por mayúsculas, minúsculas y números.
- Las contraseñas de las cuentas de usuario con perfil de administrador deberán almacenarse de manera cifrada en un gestor de contraseñas.
- Las contraseñas deberán expirar en un ciclo definido de 75 días.
- No se permitirá reutilizar las últimas 10 contraseñas.
- Se deberá pedir y verificar la contraseña antigua antes de continuar con el cambio, exceptuando el caso de cambio por olvido de la misma, en el que se deberá verificar la validez temporal del token enviado al usuario
- Se deberá pedir doble confirmación de la nueva contraseña antes de proceder al cambio, para evitar posibles errores de escritura.
- Se deberá verificar la política de composición, lista negra, y reutilización de la nueva contraseña antes de proceder al cambio.

c) Autorización

- Los permisos de acceso a los diferentes partes de la aplicación se deberán gestionar en base a roles o perfiles, que además deberán estar documentados.
- Siempre deberán configurarse los permisos mínimos necesarios para evitar accesos no autorizados y los usuarios deberán tener un perfil de acceso distinto según las acciones que vayan a realizar, siguiendo el principio de privilegios mínimos.

- La aplicación deberá pedir una nueva autenticación o el uso de un segundo factor de autenticación (2FA), antes de permitir la realización de una operación especialmente sensible.

d) Revisión de privilegios de acceso

- Todos los accesos de un usuario a cualquier aplicación a la que tenga acceso deberán revocarse en el momento que el usuario cause baja o que ya no necesita acceso al activo.
- Se hará una revisión periódica de los usuarios y sus perfiles de acceso a las aplicaciones.
- Los identificadores de usuario que cumplan un periodo de inactividad de 60 días serán deshabilitados y transcurridos 30 días adicionales desde la fecha de desactivación sin que exista ninguna reclamación, el identificador será borrado.

3.3.1.3 Auditoría y monitorización

a) Registro de logs de seguridad

- Tanto los accesos (exitosos y fallidos) como las acciones relevantes de usuario (tanto a nivel de aplicativo como de sistema operativo) deberán registrarse y enviarse el log correspondiente a una plataforma SIEM.
- Los logs de auditoría deberán registrar la siguiente información:
  - La actividad de los administradores.
  - Los accesos de los usuarios, tanto los satisfactorios como los fallidos.
  - Los cambios en los parámetros de configuración.
  - La activación/desactivación o cambios en la configuración de los mecanismos que generan los logs.
  - Los errores en el funcionamiento.
  - Los cambios en los privilegios de acceso: alta, baja y modificación de usuarios, cambios en los perfiles, etc.
  - Los eventos relacionados con el acceso o manipulación de datos de carácter sensible.
- Los registros de auditoría deberán contener toda la información necesaria para la reconstrucción y contabilización de los eventos de seguridad producidos. Dichos logs deberán incluir, al menos:
  - Activo en el que se ha producido el evento
  - Código identificador del usuario, programa o elementos que origina el evento, incluyendo la dirección IP origen desde la que accede.
  - Fecha y hora en que se produce el evento, con precisión mínima de segundos
  - Descripción o motivo del evento que se registra .

- Los mecanismos de generación de registros de auditoría no permitirán que los usuarios puedan modificar los registros de auditoria.
- Se deberá generar un evento de seguridad en caso de que se trate de modificar el contenido de los registros de auditoria de la plataforma de forma no autorizada.
- Todo activo deberá estar sincronizado por NTP con una fuente de reloj autorizada.

b) Monitorización de alertas de seguridad

- Los logs de actividad que se manden al SIEM deberán permitir que se configuren alarmas sobre la actividad de los usuarios y los administradores.
- Se deberá disponer de alarmas sobre la actividad anómala de los usuarios y de los gestores (operaciones no autorizadas, repetidos intentos de acceso fallidos, accesos, consultas masivas, etc.), así como las acciones que el servicio o sistema haya definido como críticas (caída de un sistema, error, etc.).

3.3.2 Requisitos De Seguridad Generales Para Contenedores

Como lo más común en las aplicaciones que se desplieguen en entorno de nube pública sea que se utilicen tecnologías de contenedores y orquestadores y otras plataformas asociadas, pasamos a definir una guía de requisitos básicos de seguridad para el despliegue de las mismas, teniendo en cuenta siempre que los requisitos mencionados en el aparatado anterior también aplican a este, ya que solo nos vamos a centrar en la *arquitectura de seguridad y bastionado de los contenedores* ya que para la gestión de usuarios y la trazabilidad y monitorización seguirán aplicando los requisitos anteriores.

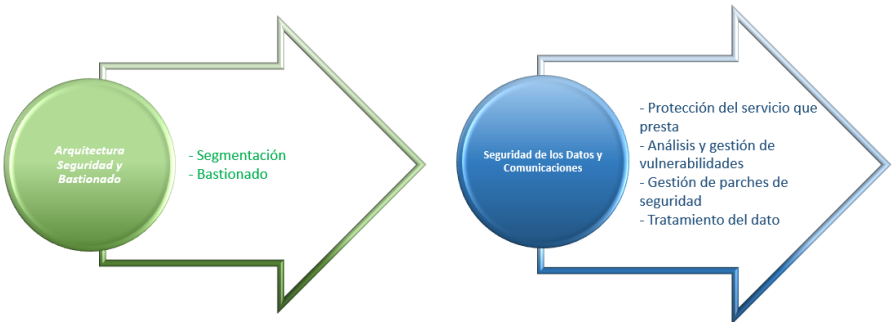


Ilustración 39 - Requisitos De Seguridad Generales Para Contenedores

3.3.2.1 Arquitectura de seguridad y bastionado

a) Segmentación

- Se deberá emplear, al menos, un *namespace* distinto por cada proyecto, aplicación y entorno.
- En cada *namespace* se crearán pods separando funciones de Backend (datos y lógica de negocio) y de frontal de acceso.
- La gestión de los contenedores deberá realizarse mediante las herramientas y comandos que ofrece, y no desplegando servidor SSH dentro del contenedor.
- No se deberá utilizar el flag *–net=host* al ejecutar un contenedor, para garantizar la segmentación entre el contenedor y la máquina anfitriona a nivel de pila de red.
- No se deberá utilizar el flag *--uts=host*, para garantizar la segmentación entre el contenedor y la máquina anfitriona a nivel de *namespace*.
- No se deberá utilizar el flag *--userns=host*.
- No se recomienda la apertura de todas las comunicaciones entre pods dentro de un mismo proyecto.
- Para las comunicaciones entre diferentes proyectos de diferentes topologías tendrán que hacerse a través de un firewall, entendiendo por un firewall un elemento que proporcione las siguientes capacidades:
    - Filtrado de paquetes dependiendo de origen, destino, puerto
    - Descarte de paquetes malformados
    - Stateful Inspection.
    - Inspección de paquetes.
    - Validación de protocolo.
    - Control de gestión de cambios.
    - Validación de modificación de reglas.
- Pero si son proyectos de la misma topología, las comunicaciones entre pods, deberán realizarse haciendo uso de la funcionalidad de la plataforma denominada “Network Policies”.

b) Bastionado

- Se deberá utilizar una herramienta de evaluación de configuración segura de contenedores como, por ejemplo, Docker Bench Security. (https://github.com/docker/docker-bench-security)
- Nunca se deberán ejecutar contenedores como *root*.
- Se podrá utilizar el comando *exec* para ejecutar comandos con privilegios dentro del contenedor, liberando así los privilegios del usuario.
- En caso de que sea necesario utilizar el programa *systemd* para iniciar la aplicación dentro del contenedor, en el archivo de unidad correspondiente se

deberán configurar los servicios para que se ejecuten como usuarios no *root* siempre que sea posible.

- En los contenedores deberán definirse usuarios sin privilegios, pues el usuario por defecto es el usuario *root*. Al definir la imagen Docker, en el fichero Dockerfile se deberá crear usuario no *root*, que será el que deba utilizarse para ejecutar el contenedor (y, por tanto, todo lo que se ejecute dentro de él).
- Solo se deberán utilizar imágenes confiables. Tanto la imagen base como el resto de las capas construidas a partir de ella no estando permitido utilizar imágenes/capas sin soporte oficial de un fabricante.
- Se deberá controlar de forma centralizada qué imágenes y registros son confiables, utilizando para ello una herramienta de escaneo de imágenes.
- Solo se deberán instalar en el contenedor los paquetes que sean estrictamente necesarios.
- No se deberá hacer bind de un servicio Docker sobre un puerto TCP. Se deberá mantener el valor predeterminado de binding y no utilizar un puerto en el rango 49153 - 65535.
- No está permitido el uso de los siguientes flags
    - *flag --privileged* al ejecutar un contenedor. En caso de que sea necesario disponer, dentro de un contenedor, de alguna capacidad de Linux o de un dispositivo concreto, se deberán emplear los *flags --cap-add y -device,* para habilitar acceso exclusivamente a sus recursos.
    - flag --cgroup-parent al ejecutar un contenedor.
    - *flag --publish-all.*

3.3.2.2 Seguridad de los datos y las comunicaciones

- Se deberán utilizar canales seguros para las comunicaciones desde/hacia los registros de imágenes (Docker registry). Para ello, se deberá habilitar el Docker Content Trust, que habilita el uso de firma digital en las comunicaciones con el Registry.

a) Protección del servicio que presta

- Definir el mecanismo de comprobación del estado de salud de los contenedores.
- Se deberá controlar el uso de recursos de memoria y CPU del contenedor.
- Al definir la política de reinicio del contenedor (flag --restart), no se deberá utilizar la política always. En el caso de utilizar la política on-failure, se deberá establecer siempre un número máximo de intentos (por ejemplo, 5).

b) Análisis y gestión de vulnerabilidades

- El desarrollo de nuevas imágenes deberá seguir las indicaciones de desarrollo seguro en imágenes Dockers
- Se deberá comprobar periódicamente que las imágenes utilizadas siguen las indicaciones de desarrollo seguro en imágenes Dockers.
- Se deberá comprobar periódicamente que las capacidades que no sean necesarias en un contenedor se han eliminado.

c) Gestión de parches de seguridad

- Se deberá realizar una correcta gestión de las imágenes, que contemple la revisión periódica de vulnerabilidades y el parcheado de las mismas, volviendo a construir nuevas imágenes parcheadas e instanciando nuevos contenedores con las vulnerabilidades corregidas.
- Al lanzar un nuevo contenedor, siempre se deberán utilizar las últimas versiones de las imágenes publicadas en el contenedor de imágenes.
- Se deberá comprobar periódicamente que las versiones de las imágenes utilizadas son las últimas publicadas en el contendor de imágenes.
- Al reiniciar contenedores suspendidos o apagados durante un tiempo, se debe garantizar que la imagen que utilizan está completamente actualizada, con el último nivel de parcheado y sin vulnerabilidades de seguridad conocidas.

d) Tratamiento del dato

- Las imágenes que dejen de utilizarse deberán eliminarse, y se deberá garantizar que todos los datos manejados son debidamente borrados y no quedan accesibles. Del mismo modo, se deberán eliminar en cascada las estructuras de comunicaciones no necesarias tras la eliminación de una imagen.

4 Herramientas de Seguridad en la Nube

El objetivo de este apartado es hacer un estudio de las opciones y herramientas de seguridad que tenemos en los proveedores de nube más utilizados con el fin de tener una visión general de las soluciones de seguridad que ofrecen cada uno de los proveedores, vamos a dividir los productos o herramientas de seguridad de cada una de las 3 nubes principales en 4 dominios diferentes, ***seguridad del dato***, ***identidad y control de accesos***, ***protección de infraestructuras*** y ***detección de amenazas*** y ***monitorización.***

En el apartado de Anexos podemos encontrar una descripción un poco más detallada de cada una de las herramientas de seguridad asociadas a cada uno de los dominios para cada uno de los proveedores de servicios en nube que estamos analizando en este apartado. (AWS, 2020) (Google Cloud, 2020) (Microsft, 2020)

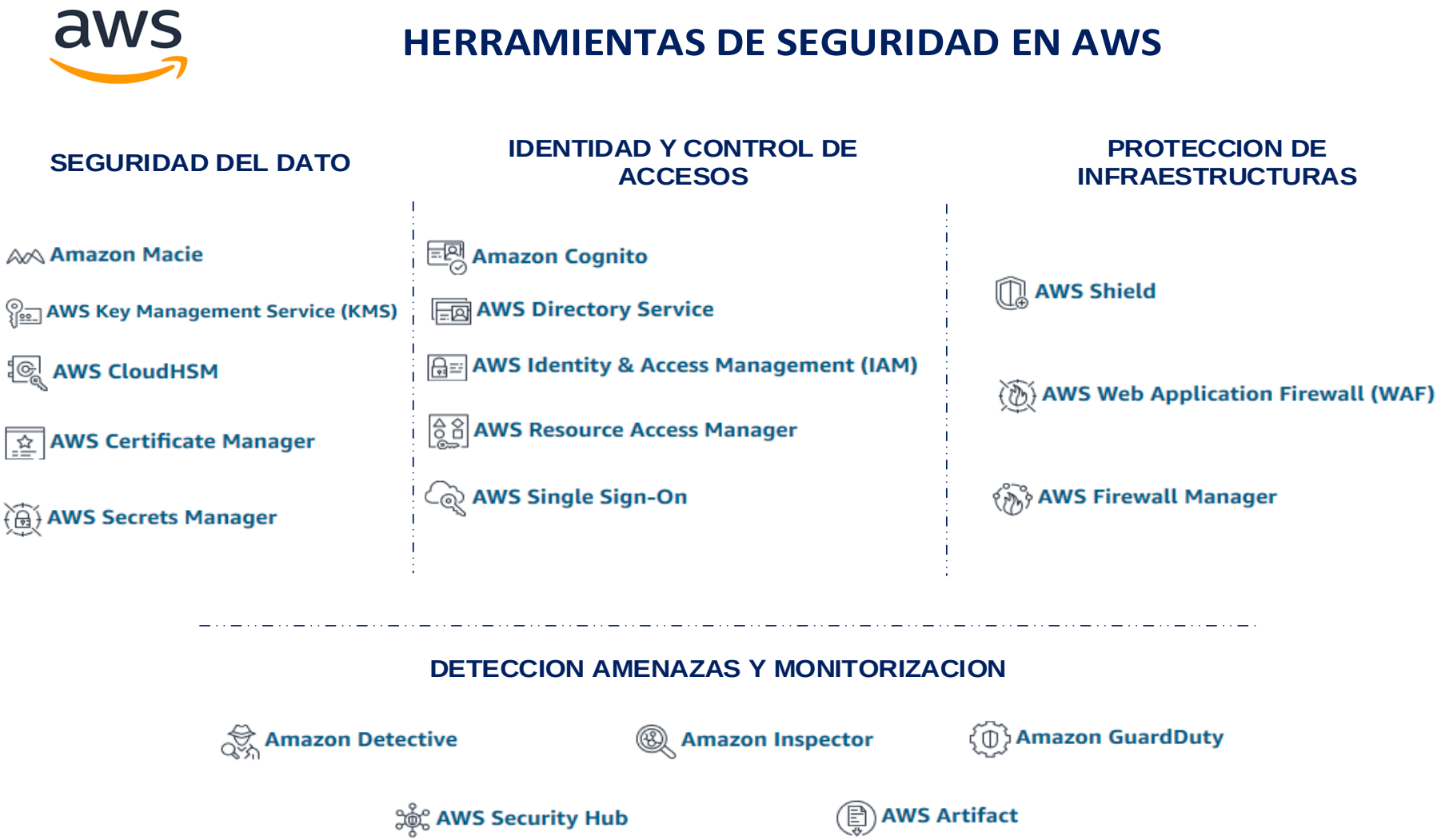


Ilustración 40 - Herramientas de seguridad en AWS

HERRAMIENTAS DE SEGURIDAD EN AZURE

SEGURIDAD DEL DATO

Azure Sentinel

Azure Dedicated HSM

Azure Information Protection

Azure SQL Database

Storage Service Encryption

Disk Encryption

IDENTIDAD Y CONTROL DE ACCESOS

Azure AD

Azure Active Directory Domain Services

Multi-Factor Authentication

PROTECCION DE INFRAESTRUCTURAS

Azure Application Gateway

VPN Gateway

Azure DDoS Protection

Network Security Groups

Just intime (JIT) VM Access

DETECCION AMENAZAS Y MONITORIZACION

Security Center

Azure Sentinel

Microsoft Operation Management Suite

Ilustración 41 - Herramientas de seguridad Azure

HERRAMIENTAS DE SEGURIDAD EN GOOGLE CLOUD

SEGURIDAD DEL DATO

- Cifrado en reposo
- Cloud KMS
- Cloud Data Loss Prevention
- Cloud HSM
- Controles de servicio de VPC

IDENTIDAD Y CONTROL DE ACCESOS

- Cloud Identity
- Identity Platform
- Cloud IAM
- Policy Intelligence
- Cloud Identity-Aware Proxy
- Security Key Enforcement
- Llave de seguridad Titan
- Cloud Resource Manager:
- Servicio gestionado para Microsoft AD

PROTECCION DE INFRAESTRUCTURAS

- Cloud Load Balancing
- Cifrado en transito
- Seguridad de transporte en la capa de aplicación
- Cloud Armor
- Apigee
- Cloud Security Scanner

DETECCION AMENAZAS Y MONITORIZACION

- Cloud Security Command Center
- Centro de seguridad de G Suite
- Inventario de recursos de Cloud
- Centro de alertas de G Suite
- Transparencia de acceso de G Suite
- Registros de auditoría de Cloud
- Backstory
- Transparencia de acceso

Ilustración 42 - Herramientas de seguridad Google Cloud

5 Ejemplos y Resoluciones con Buenas Prácticas

Para poder poner en practica los puntos anteriores desarrollados en este TFM, vamos a poner varios ejemplos de brechas de seguridad en grandes compañías, que hemos encontrado en (Cloud Security Alliance, 2020) indicando como se hubieran evitado la perdida de información y de reputación de estas empresas si se hubieran tomado las medidas de seguridad adecuadas, a la hora de hacer el diseño y el gobierno de la aplicación en la nube antes de decidir su migración a esta.

Ejemplo 1

Uber reveló que su cuenta de Amazon Web Services (AWS) fue hackeada a finales de 2016, comprometiendo la información personal de 57 millones de usuarios en todo el mundo.

Esta brecha de seguridad es un caso de responsabilidad compartida entre cliente proveedor de servicios en la nube, que ocasionó un impacto de reputación y confianza de los clientes que utilizan el servicio, perdida de propiedad intelectual y implicaciones regulatorias que pueden impactar en perdidas monetarias.

¿Como hubiéramos conseguido mitigar esta brecha de seguridad?

Si se hubieran cumplido los requisitos de gobierno de seguridad en la nube, según hemos visto en el apartado *3.1* de este TFM, en el que se hubieran implantado las políticas adecuadas, donde se hubieran asignado los permisos correspondientes a los usuarios para acceder a la información, se hubieran implementado los requisitos de cifrado según lo expuesto en *los requisitos de seguridad de los datos y las comunicaciones* se hubiera conseguido mitigar el ataque, y si aun así se hubiera producido se hubiera podido reducir el impacto con un plan adecuado de respuesta a incidentes.

Ejemplo 2

En 2017, un bucket de almacenamiento en la nube de AWS Simple Storage Service (S3) mal configurado expuso datos detallados y privados de 123 millones de hogares estadounidenses. El conjunto de datos pertenecía a Experian, una oficina de crédito, que vendió los datos a una empresa de marketing y análisis de datos en línea llamada Alteryx. Fue Alteryx el que expuso el archivo.

Esta es una brecha de seguridad cuya responsabilidad es sobre todo del cliente que consume los servicios ya que la mala configuración de los recursos en la nube es una de las principales causas de las violaciones de datos.

¿Como hubiéramos conseguido mitigar esta brecha de seguridad?

Aplicando correctamente los dominios de seguridad expuestos en el punto 3, concretamente los de arquitectura y diseño de seguridad, aplicando los requisitos de cifrado y control de acceso recomendados, así como estableciendo unas políticas adecuadas de seguridad de gobierno en la nube.

Ejemplo 3

En 2018, una base de datos Elasticsearch no segura propiedad de Exactis dio lugar a otra violación masiva que contenía datos altamente personales de 230 millones de consumidores estadounidenses. El servidor de bases de datos se configuró para que sea accesible públicamente.

Este es un claro caso de perdida de reputación y confianza de una empresa que ocasionó cuantiosas pérdidas económicas

¿Como hubiéramos conseguido mitigar esta brecha de seguridad?

Algo tan sencillo como implementar una correcta política de gestión de acceso a la información acompañada de las políticas de seguridad adecuada hubieran mitigado esta brecha de seguridad

Ejemplo 4

En 2018, Level One Robotics, una empresa de ingeniería especializada en procesos y montajes de automatización expuso información patentada altamente sensible perteneciente a más de 100 empresas manufactureras, incluyendo Volkswagen, Chrysler, Ford, Toyota, General Motors, Tesla y ThyssenKrupp. En este caso, el activo mal configurado era un rsync(backup) server that allowed unauthenticated data transfer to any rsync client.

En este caso no importa como de grande o pequeña sea la empresa, la arquitectura y la estrategia de seguridad adecuadas son elementos necesarios para, implementar y operar de forma segura en la nube.

¿Como hubiéramos conseguido mitigar esta brecha de seguridad?

Con un correcto diseño de la arquitectura de seguridad y de las comunicaciones cumpliendo los requisitos que se mencionan en el apartado 3.2 y cumpliendo los requisitos de cifrado de comunicaciones, así como estableciendo unos requisitos de control de acceso adecuados en función del tipo de dato expuesto.

Y podríamos seguir enumerando ejemplos como los que vemos a continuación que se podrían haber mitigado e incluso evitado si se hubiera seguido una guía de buenas practicas de diseño de seguridad en la nube pública.

Ejemplo 5

Investigadores del Centro de Seguridad Kromtech descubrieron una serie de datos pertenecientes a la aplicación Honda Connect, que fue expuesto en línea. Los datos se almacenaron en dos buckets de Amazon AWS S3 no seguros, de acceso público y desprotegidos

Ejemplo 6

En diciembre de 2018, un estudiante alemán hackeó datos protegidos por contraseñas débiles y compartió la información utilizando una plataforma en la nube. El jugador de 20 años utilizó contraseñas como "Iloveyou" y "1234" para hackear cuentas en línea de cientos de legisladores y personalidades cuyas posturas políticas no le gustaban. Funcionarios alemanes de ciberseguridad revelaron que los números de teléfono, mensajes de texto, fotografías, números de tarjetas de crédito y otros datos relacionados con 1.000 miembros del parlamento, periodistas y otras figuras públicas habían sido robados, recopilados y difundidos a través de Twitter y otras plataformas en línea.

Ejemplo 7

El 31 de mayo de 2017, un actor de amenazas utilizó las claves de AWS de OneLogin para obtener acceso a la plataforma de AWS de la empresa a través de una interfaz de programación de aplicaciones (API) desde un host intermedio con otro proveedor de servicios más pequeño en EE. UU. OneLogin, que proporciona servicios de administración de identidades y contraseñas, detectó la intrusión y cerró los sistemas afectados (y las claves de AWS comprometidas) para detener la intrusión en cuestión de minutos. También confirmaron que no había otras amenazas activas.

Ejemplo 8

Facebook anunció una violación significativa de datos que afecta a más de 50 millones de cuentas el 28 de septiembre de 2018. Según se informa, una vulnerabilidad de robo de credenciales se introdujo en el código de Facebook en julio de 2017, más de un año antes. La compañía admitió que no sabía qué información fue robada, ni cuántas otras cuentas de usuario se vieron comprometidas como resultado de la violación.

6.Conclusiones

Cuando empecé a cursar este master en febrero del pasado año 2019, ya me planteé sobre que temática quería realizar el TFM del master, y debido a la transformación digital a la actualmente la mayoría de las organizaciones están realizando, no tuve duda de que tenía que hacer un TFM relacionado con la seguridad de las aplicaciones en la nube pública, y está idea se vio reforzada después de todo lo que estamos viviendo estos meses con la inesperada pandemia del COVID-19.

Los servicios que ofrece la nube pública pueden ser la mejor solución para que las organizaciones se puedan adaptar rápidamente a ofrecer soluciones de teletrabajo a sus empleados y así evitan exponer su CPD, muchas veces con unas medidas precarias de seguridad de la información, a internet sin un reduciendo costes y utilizando un entorno que ha sido diseñado con los máximos estándares de seguridad y está preparado para alojar aplicaciones y desplegarlas de una manera rápida, sencilla y con ahorro de costes considerables.

He planteado este TFM enfocándolo desde los riesgos, vulnerabilidades y brechas de seguridad más comunes que se han producido estos años en el entorno de la nube pública, ya que creo que es la mejor manera de ilustrar los pasos a seguir por un responsable de TI cuando plantea con su equipo de seguridad la migración o creación de nuevas aplicaciones en el entorno de la nube pública.

La idea ha sido describir una metodología, detallando los requisitos de seguridad deseables para la creación o migración de una aplicación, ya que, para los temas relacionados con la continuidad del negocio, análisis de vulnerabilidades y demás dominios de la seguridad de la información, son ya soluciones que ofrecen los proveedores de servicios en la nube per se.

Por eso esta metodología se basa en requisitos de seguridad relacionados con el gobierno de la seguridad, los modelos de despliegue, aspectos legales y marcos regulatorios que nos podemos apoyar para realizar el diseño y arquitectura de seguridad desde el punto de vista de las aplicaciones, para finalizar con el estado actual de las herramientas de seguridad que ofrecen los principales proveedores de nube pública, Azure, AWS, y Google Cloud.

Este TFM se ha concluido de forma satisfactoria cubriendo los objetivos planteados en la planificación inicial, por lo tanto, se ha empleado una metodología adecuada, y en el caso de haber dispuesto de más tiempo podríamos haber simulado un caso práctico del despliegue de una aplicación en algún proveedor de nube publica empleando la metodología desarrollada en este TFM. Por eso únicamente hemos incluido un apartado de ejemplos de brechas

o vulnerabilidades de seguridad detectadas en el pasado y como se podrían haber evitado o mitigado siguiendo la metodología planteada.

7. Glosario

2FA : Segundo factor de autenticación

AES : Advanced Encryption Standard, esquema de cifrado

API : application programming interface, conjunto de subrutinas que ofrece cierta biblioteca para ser utilizado por otro software.

AWS: Amazon Web Services, servicio en la nube de Amazon.

AZURE: Servicio en la nube de Microsoft.

BACKUP: se refiere a la copia y archivo de datos de la computadora de modo que se puede utilizar para restaurar la información original después de una eventual pérdida de datos.

BCRYPT :función de hash de contraseña

BIND : Berkeley Internet Name Daemon, es el servidor de DNS más comúnmente usado en Internet

CAB FORUM : es un consorcio voluntario de autoridades de certificación, proveedores de software de navegador

CCM : Es un cifrado autenticado algoritmo diseñado para proporcionar tanto la autenticación y la confidencialidad

CCN_CERT : es el organismo español, creado en 2006, encargado de contribuir a la ciberseguridad de la administración pública.

CHACHA20 : mecanismo de cifrado de flujo desarrollados por Daniel J. Bernstein

CLI : interfaz de línea de comandos

CPD : Centro de proceso de datos

CSA : Cloud Security Alliance

CSPNRG : Generador de números pseudoaleatorios criptográficamente seguro

DDOS : Ataque de denegación de servicio.

DEVOPS : es una práctica de ingeniería de software que tiene como objetivo unificar el desarrollo de software y la operación del software.

DIFFIE-HELLMAN (DH) : es un protocolo de establecimiento de claves entre partes que no han tenido contacto previo, utilizando un canal inseguro y de manera anónima

DIRECT CONNECT : es una solución de servicio en la nube que facilita el establecimiento de una conexión de red exclusiva entre el entorno local y AWS.

DOCCKER : es un proyecto de código abierto que automatiza el despliegue de aplicaciones dentro de contenedores de software, proporcionando una capa adicional de abstracción y automatización de virtualización de aplicaciones en múltiples sistemas operativos

ECDSA : Elliptic Curve Digital Signature Algorithm, es una modificación del algoritmo DSA que emplea operaciones sobre puntos de curvas elípticas en lugar de las exponenciaciones que usa DSA.

ENDPOINT : Una punto final de comunicación es un tipo de nodo de red de comunicación.

EXEC : es una funcionalidad de un sistema operativo que ejecuta un archivo ejecutable en el contexto de un proceso ya existente, reemplazando el ejecutable anterior

EXPRESSROUTE : es un servicio de Azure que permite crear conexiones privadas entre los centros de datos de Microsoft y la infraestructura local o en una instalación de múltiples ubicaciones.

FLAG : se refiere a uno o más bits que se utilizan para almacenar un valor binario o código que tiene asignado un significado

FORWARD SECRECY : es la propiedad de los sistemas criptográficos que garantiza que el descubrimiento de las claves utilizadas actualmente no compromete la seguridad de las claves usadas con anterioridad

FRONTEND : consiste en la conversión de datos en una interfaz gráfica para que el usuario pueda ver e interactuar con la información de forma digital usando HTML, CSS y JavaScript

FTP : El Protocolo de transferencia de archivos es un protocolo de red para la transferencia de archivos entre sistemas conectados a una red TCP, basado en la arquitectura cliente-servido

GCM : fue un servicio de notificación móvil desarrollado por Google que permite a los desarrolladores de aplicaciones de terceros enviar datos o información

HASH : es una función computable mediante un algoritmo que tiene como entrada un conjunto de elementos, que suelen ser cadenas, y los convierte en un rango de salida finito, normalmente cadenas de longitud fija

IAAS : Infraestructura as a service, infraestructura como servicio

IAM : Identity and Access management.

ICS : sistemas de control industrial

IP_FORWARDING : Es una vulnerabilidad que permite el reenvío de paquetes a través del host.

ISO : Organización Internacional de Normalización

LOGS : grabación secuencial en un archivo o en una base de datos de todos los acontecimientos que afectan a un proceso particular.

MDS : algoritmo de cifrado

MFA : Multi Factor authentication, lo mismo que 2FA

NAMESPACE : es una capa de abstracción que hace que parezca que los procesos dentro de un determinado espacio de usuario tengan aislados sus propios recursos hardware

NIST : Instituto nacional de estándares y tecnología de estados unidos.

NTP : protocolo de Internet para sincronizar los relojes de los sistemas informáticos.

ON-PREMISE : software local se instala y se ejecuta en computadoras en las instalaciones de la persona u organización

PAAS : Plataforma como servicio o plataforma de aplicación como servicio

PCI : Es el Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago

PII : la información que puede usarse para identificar, contactar o localizar a una persona en concreto

PKI : infraestructura de clave pública es una combinación de hardware, software, y políticas y procedimientos de seguridad, que permiten la ejecución con garantías de operaciones criptográficas

PODS : representa un conjunto de contenedores que comparten almacenamiento y una única IP.

REPOSITORIO: Un repositorio es un espacio centralizado donde se almacena, organiza, mantiene y difunde información digital.

ROOT : super usuario en sistemas Unix

RSA : sistema criptográfico de clave pública

SAAS : Software as a Service, software como servicio.

SALT : comprende bits aleatorios que se usan como una de las entradas en una función derivadora de claves

SCADA : un software para ordenadores que permite controlar y supervisar procesos industriales a distancia

SCRIPT : término informal que se usa para designar a un programa relativamente simple

SHA-2 : es un conjunto de funciones hash criptográficas diseñadas por la Agencia de Seguridad Nacional publicada en 2001

SHA-3 : es un conjunto de funciones hash criptográficas diseñadas por la Agencia de Seguridad Nacional publicada el 5 de agosto de 2015

SIEM : sistema de gestión de información y eventos de seguridad

SLA : Un acuerdo de nivel de servicio

SMTP : protocolo para transferencia simple de correo es un protocolo de red utilizado para el intercambio de mensajes de correo electrónico

SSO : Single Sign-On, es un procedimiento de autenticación que habilita a un usuario determinado para acceder a varios sistemas con una sola instancia de identificación

STARTTLS : es una extensión a los protocolos de comunicación de texto plano, que ofrece una forma de mejorar desde una conexión de texto plano a una conexión cifrada en lugar de utilizar un puerto diferente para la comunicación cifrada

TI : Tecnologías de la información

TLS : Seguridad de la capa de transporte que proporciona comunicaciones seguras por una red, comúnmente Internet.

VPN : Virtual net protocol

XSALSA20 : mecanismo de cifrado

8. Bibliografía

ISO/IEC JTC 1/SC 27. (Diciembre de 2015). Code of practice for information security controls based on ISO/IEC 27002 for cloud services.

AWS. (Marzo de 2020). *aws.amazon.com*. Obtenido de https://aws.amazon.com/es/products/security/?nc=sn&loc=2

CCN-CERT. (Marzo de 2020). *Centro criptologico Nacional*. Obtenido de https://www.ccn-cert.cni.es/

CIS . (Marzo de 2020). *CIS Controls Cloud Companion Guide*. Obtenido de https://www.cisecurity.org/white-papers/cis-controls-cloud-companion-guide/

Cloud Security Alliance. (2018). *Guia de Seguridad Areas Criticas para la computación en la nube.* Obtenido de DOMINIO 3 Cuestiones Legales, Contratos: https://cloudsecurityalliance.org/artifacts/securityguidance-v4/

Cloud Security Alliance. (8 de 4 de 2020). *CSA Alliance.* Obtenido de https://cloudsecurityalliance.org/press-releases/2019/08/09/csa-releases-new-research-top-threats-to-cloud-computing-egregious-eleven/

CSA STAR. (9 de Abril de 2019). *Cloud security Alliance.* Obtenido de https://cloudsecurityalliance.org/star/levels/

ECDSA. (Marzo de 2020). Obtenido de https://safecurves.cr.yp.to

Evaluando Cloud. (Abril de 2020). *Evaluando Cloud.com.* Obtenido de https://evaluandocloud.com/modelos-de-implementacion-del-cloud/

Evaluando Cloud. (Abril de 2020). *Evaluando Web.* Obtenido de https://evaluandocloud.com/modelos-de-servicios-de-cloud-computing/

Fortinet. (Abril de 2020). *Seguridad en la nube publica*. Obtenido de https://www.fortinet.com/lat/products/public-cloud-security.html

Gartner. (3 de Junio de 2008). *Gartner*. Obtenido de https://www.gartner.com/document/685308

Google Cloud. (Marzo de 2020). *Cloud google*. Obtenido de https://cloud.google.com/security/products?hl=es

ISO/IEC 27002:2013. (Julio de 2015). ISO/IEC 27002:2013.

Microsft. (Marzo de 2020). *Azure Security*. Obtenido de https://azure.microsoft.com/en-us/product-categories/security/

Mozilla SSL Configurator Generator. (Abril de 2020). *Mozilla SSL Configurator Generator*. Obtenido de https://mozilla.github.io/server-side-tls/ssl-config-generator/

NIST Special Publication 800-146. (Mayo de 2012). *https://csrc.nist.gov/publications/detail/sp/800-146/final.* Obtenido de https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-146.pdf

Richard Watson, M. M. (25 de Enero de 2019). *Gartner.* Obtenido de Implementing Governanve for Public Cloud: https://gartner.com

9. Anexos

9.2 Productos De Seguridad En Cloud

Seguridad AWS

Amazon Web Services, a partir de ahora AWS, ofrece servicios seguridad estructurados en 5 bloques diferentes :

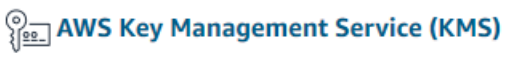
Protección de datos

AWS proporciona servicios que le ayudan a proteger sus datos, cuentas y cargas de trabajo del acceso no autorizado. Los servicios de protección de datos de AWS proporcionan cifrado y administración de claves y detección de amenazas que monitorizan y protegen continuamente sus cuentas y cargas de trabajo.

Las herramientas con las que cuenta AWS para la protección del dato son:

Amazon Macie es un servicio de seguridad que utiliza el aprendizaje automático para detectar, clasificar y proteger información confidencial automáticamente en AWS, reconoce los datos confidenciales, como la información personalmente identificable (PII) o la propiedad intelectual, y le proporciona paneles de control y alertas que aportan visibilidad acerca de cómo se están trasladando estos datos o se está accediendo a ellos.

Este servicio monitorea la actividad de acceso a los datos constantemente en busca de anomalías y genera alertas detalladas cuando detecta el riesgo de acceso no autorizado.



Creación y control administrados de claves de cifrado, permite crear y administrar con facilidad las claves y controlar el uso del cifrado en una amplia variedad de servicios de AWS y en sus aplicaciones. AWS KMS presenta un solo punto de control para administrar claves y define políticas de manera coherente a través de diferentes servicios integrados de AWS y sus propias aplicaciones. El usuario controla el acceso a sus datos cifrados al definir permisos para utilizar claves mientras que AWS KMS aplica sus permisos y se ocupa de la durabilidad y la seguridad física de sus claves.

Almacenamiento de claves en hardware a efectos de conformidad normativa, permite generar y usar con facilidad sus propias claves de cifrado en la nube.

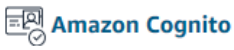
Aprovisionamiento, administración e implementación de certificados de capa de conexión segura/seguridad de la capa de transporte (SSL/TLS) públicos y privados para su uso con servicios de AWS y recursos internos conectados

Alterne, administre y recupere y recupere fácilmente credenciales de bases de datos, claves de API y otros datos confidenciales durante todo su ciclo de vida.

Identity & Access Management

Los servicios de AWS Identity le permiten administrar identidades, recursos y permisos de forma segura y a escala. En el caso de las aplicaciones que se ejecutan en AWS, puede usar controles de acceso específicos para conceder a empleados, aplicaciones y dispositivos el acceso que necesitan a los recursos y servicios de AWS dentro de límites de gobernanza de fácil implementación. Los servicios de AWS Identity ofrecen opciones flexibles acerca de dónde y cómo administrar las identidades de empleados, socios y clientes, lo que permite migrar cargas de trabajo existentes a AWS de forma segura.

Las herramientas con las que cuenta AWS para la IDM son:

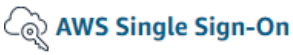


Administración de identidades para las aplicaciones. permite, de manera rápida y sencilla, incorporar a sus aplicaciones web y dispositivos móviles funcionalidades como el control de acceso, la inscripción y el inicio de sesión de los usuarios.

Microsoft Active Directory administrado en la nube de AWS.

puede administrar el acceso a los servicios y recursos de AWS de manera segura. Además, puede crear y administrar usuarios y grupos de AWS, así como utilizar permisos para conceder o negar el acceso de estos a los recursos de AWS

Servicio simple y seguro para compartir recursos de AWS.



Permite administrar de forma centralizada el acceso a múltiples cuentas de AWS y aplicaciones empresariales, además de proporcionar a los usuarios un acceso de inicio de sesión único a todas las aplicaciones y cuentas asignadas desde un mismo lugar

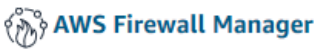
Protección de infraestructuras

AWS protege las aplicaciones web al filtrar el tráfico en función de las reglas que cree. Por ejemplo, puede filtrar las solicitudes web por direcciones IP, encabezados HTTP o cadenas URI, lo que permite bloquear patrones de ataque comunes, como la inyección de código SQL y las secuencias de comandos entre sitios.

Las herramientas con las que cuenta AWS para la protección de infraestructuras son :

es un servicio de protección contra ataques de denegación de servicio distribuidos (DDoS).

es un firewall para aplicaciones web que ayuda a proteger sus aplicaciones web o API contra ataques web comunes que pueden afectar la disponibilidad, poner en riesgo la seguridad o consumir demasiados recursos.



administración de seguridad que permite la configuración y administración centralizadas de reglas de firewall en todas sus cuentas y aplicaciones en AWS.

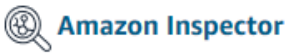
Detección de amenazas y monitorización continua

AWS identifica las amenazas mediante el monitoreo continuo de la actividad de la red y del comportamiento de la cuenta dentro del entorno de su nube.

Las herramientas con las que cuenta AWS para la detección de amenazas y monitorización

Centro unificado de seguridad y conformidad, permite ver de manera integral las alertas de seguridad de alta prioridad y el estado de conformidad en todas las cuentas de AWS.

servicio de detección de amenazas que monitoriza de forma constante para detectar actividades maliciosas y comportamientos no autorizados con el fin de proteger sus cargas de trabajo y cuentas de AWS



servicio automático de evaluación de asuntos de seguridad que ayuda a mejorar el nivel de seguridad y conformidad de las aplicaciones que se implementan en AWS. Amazon Inspector evalúa automáticamente las aplicaciones en busca de exposiciones, vulnerabilidades y desviaciones en relación con las prácticas recomendadas

facilita el análisis, la investigación y la rápida identificación de la causa raíz de posibles problemas de seguridad o actividades sospechosas.

Conformidad y privacidad de datos

AWS le ofrece una visión integral de su estado de conformidad y monitoriza continuamente su entorno utilizando comprobaciones de conformidad automatizadas basadas en las prácticas recomendadas de AWS y en los estándares del sector que sigue su organización.

Las herramientas con las que cuenta AWS para conformidad son:

Proporciona acceso bajo demanda a los informes de seguridad y conformidad de AWS y acuerdos online seleccionados

Seguridad Azure

Microsoft y su solución de nube Azure, a nivel de seguridad dispone de las siguientes herramientas, divididas en los siguientes bloques:

Protección de datos

Key Vault: permite a los suscriptores de Azure proteger y controlar claves criptográficas y otros secretos usados por aplicaciones y servicios en la nube

Azure Dedicated HSM: ofrece almacenamiento de claves criptográficas en Azure. Cumple los requisitos de seguridad más estrictos ofreciendo soluciones para dispositivos validados con la certificación FIPS 140-2 nivel 3 y un control completo y exclusivo del dispositivo HSM.

Azure Information Protection: controla y ayuda a proteger el correo electrónico, los documentos y los datos confidenciales que comparte fuera de su compañía, usándolo desde una clasificación sencilla hasta etiquetas y permisos insertados para mejorar la protección de los datos en todo momento, independientemente de dónde estén almacenados o con quién los comparta.

Azure SQL Database: es un cifrado de datos transparente que ayuda a proteger los datos en el disco y protege contra el acceso no autorizado al hardware. Realiza el cifrado y descifrado en tiempo real de la base de **datos,** las copias de seguridad asociadas y los archivos de registro de transacciones en reposo sin necesidad de realizar cambios en la aplicación.

Storage Service Encryption es una funcionalidad de Azure Storage diseñada para proporcionar cifrado AES de 256 bits sin cambios adicionales en las aplicaciones.

Disk Encryption: proporciona protección para los datos en reposo. Permite el cifrado para discos de máquina virtual de Azure de Windows y Linux.

Azure Sentinel: es una solución de administración de eventos de información de seguridad (SIEM) y respuesta automatizada de orquestación de seguridad (SOAR) que es escalable y nativa de la nube. Azure Sentinel ofrece análisis de seguridad inteligente e inteligencia frente a amenazas en toda la empresa, de forma que proporciona una única solución para la detección de alertas, la visibilidad de amenazas, la búsqueda proactiva y la respuesta a amenazas.

Identity & Access Management

Azure AD: es un servicio de administración de identidades y acceso basado en la nube de Microsoft que ayuda a los empleados a iniciar sesión y acceder a

recursos como Microsoft Office 365, Azure Portal y miles de otras aplicaciones SaaS, o aplicaciones de la red corporativa y la intranet, junto con todas las aplicaciones en la nube desarrolladas por su propia organización.

Azure Active Directory Domain Services: proporciona servicios de dominio administrados como, por ejemplo, unión a un dominio, directiva de grupo, protocolo ligero de acceso a directorios (LDAP) y autenticación Kerberos/NTLM, que son totalmente compatibles con Windows Server Active Directory. Puede usar estos servicios de dominio sin necesidad de implementar o administrar los controladores de dominio de la nube, ni de aplicarles revisiones

Multi-Factor Authentication: proporciona una capa adicional de seguridad al requerir una segunda forma de autenticación a través de una serie de opciones de verificación sencillas (llamada telefónica, Sms, código de aplicación móvil, tokens OATH de 3a parte): esto ayuda a evitar el acceso no autorizado al entorno de nube de Azure.

Protección de infraestructuras

Azure Application Gateway: es un balanceador de carga de tráfico web que permite administrar el tráfico a las aplicaciones web, y puede tomar decisiones de enrutamiento basadas en atributos adicionales de una solicitud HTTP, puede enrutar el tráfico en función de la dirección URL entrante.

VPN Gateway: es un tipo específico de puerta de enlace de red virtual que se usa para enviar tráfico cifrado entre una red virtual de Azure y una ubicación local a través de la red pública de Internet. También puede usar una instancia de VPN Gateway para enviar tráfico cifrado entre las redes virtuales de Azure a través de la red de Microsoft. Cada red virtual solo puede tener una instancia de VPN Gateway. Sin embargo, puede crear varias conexiones a la misma instancia. Al crear varias conexiones a la misma instancia de VPN Gateway, todos los túneles VPN comparten el ancho de banda disponible de la puerta de enlace.

Azure DDoS Protection: Herramienta que protege contra ataques de denegación de servicio. Azure proporciona los siguientes niveles de servicio:

Básico: La supervisión continua del tráfico y la reducción en tiempo real de los ataques a nivel de red más comunes.

Estándar: ofrece funciones adicionales de reducción de ataques en comparación con el nivel de servicio básico, realizando la supervisión del tráfico dedicado con algoritmos de Machine Learning.

Network Security Groups: son reglas que restringen el tráfico de red en una red virtual al permitirlo o negarlo. Los NSG se pueden vincular a subredes o directamente a instancias de máquina virtual dentro de esa subred.

Just intime (JIT) VM Access: es una característica disponible en Azure Security Center (nivel estándar) que proporciona un acceso sencillo a los usuarios para conectarse a las máquinas virtuales de Azure mediante la creación de una regla de NSG. En lugar de simplemente dejar el acceso abierto a un puerto de administración, los profesionales de TI solicitan acceso a la máquina virtual, cuando es necesario, mediante este servicio.

Detección de amenazas y monitorización continua

Security Center: es un sistema unificado de administración de seguridad de la infraestructura que fortalece la posición de seguridad de los centros de datos y proporciona una protección contra amenazas avanzada de todas las cargas de trabajo híbridas que se encuentran en la nube, ya sea que estén en Azure o no, así como también en el entorno local.

Microsoft Operation Management Suite (OMS) es una colección de servicios de administración que se pueden utilizar para entornos en las instalaciones o en diferentes entornos de nube con una configuración mínima.

Seguridad Google Cloud

Google Cloud estructura sus herramientas de seguridad en la nube en 8 apartados, infraestructura, red, puntos de conexión, datos, gestión de identidad y accesos, aplicaciones, operaciones y supervisión, protección de usuarios, control de riesgos y cumplimiento.

Seguridad de los datos

Refuerza la protección de los datos sensibles con el descubrimiento y la gestión de datos, además de con los controles para impedir que se vean afectados por pérdidas, fugas y filtraciones externas, para ello la nube de Google dispone de las siguientes herramientas:

- **Encriptado en reposo:** cifra de forma predeterminada los datos almacenados en reposo de los clientes. Cuando se almacenan en Google Cloud Platform, los datos se dividen en fragmentos de subarchivos y cada fragmento se cifra con una clave de cifrado concreta en el propio almacenamiento.

Cloud KMS: es un servicio de gestión de claves alojado en la nube que te permite administrar las claves criptográficas de tus servicios en la nube, utiliza cifrados AES256, RSA 2048, RSA 3072, RSA 4096, EC P256 y EC P384.

Cloud Data Loss Prevention : DLP de Cloud te ayuda a identificar y gestionar mejor los datos sensibles detectando y ocultando automáticamente los datos sensibles de cualquier lugar.

Cloud HSM : es un servicio con el que se puedes alojar claves de cifrado y llevar a cabo operaciones criptográficas en HSMs que cuenten con el certificado FIPS 140-2 de nivel 3.

Controles de Servicio de VPC : Establece perímetros de seguridad virtuales para servicios basados en API

Identity & Access Management

Gestiona y protege las identidades, así como su acceso a las aplicaciones y a los datos, tanto en la nube como on-premise.

Cloud Identity: Una plataforma centralizada de gestión de identidades, accesos, aplicaciones y puntos de conexión (IAM/EMM).

Identity Platform: ofrece un servicio de autenticación directa y personalizable para el registro y el inicio de sesión de los usuarios.

Cloud IAM: los administradores autorizan quién puede realizar qué acciones en determinados recursos, lo cual les otorga un control y una visibilidad absolutos para gestionar los recursos en la nube de forma centralizada.

Policy Intelligence: Reduce el riesgo con controles de políticas automatizados

Cloud Resource Manager: proporciona contenedores de recursos para puedes fácilmente las características más habituales de tus recursos, como el control de acceso y los ajustes de configuración.

Cloud Identity-Aware Proxy: controla el acceso a las máquinas virtuales y las aplicaciones en la nube que ejecutas en Google Cloud Platform

Servicio gestionado para Microsoft Active Directory: El servicio gestionado para Microsoft Active Directory (AD).

Security Key Enforcement: La autenticación de dos factores con llave de seguridad FIDO utiliza la criptografía para realizar una verificación bidireccional: se asegura de que estás iniciando sesión en el servicio en el que se registró originalmente tu llave de seguridad y de que se trata de la llave correcta

Llave de seguridad Titan: Las llaves de seguridad Titan son dispositivos resistentes a la suplantación de identidad (phishing) que cuentan con la tecnología de la autenticación de dos factores.

Protección de infraestructuras

Cloud Load Balancing: Balanceo de carga escalable y de alto rendimiento en Google Cloud Platform

Cofrado en tránsito: se cifran y autentican los datos en tránsito en una o más capas de la red cuando estos salen de los límites físicos no controlados por la nube.

Seguridad de transporte en capa de aplicación: La seguridad de transporte en la capa de la aplicación (ALTS) es un sistema de autenticación mutua y de cifrado del transporte similar al TLS

Cloud Armor : Protege tus servicios ante los ataques web y de denegación de servicio

Cloud Security Scanner:

Apigee:

Detección de amenazas y monitorización continua

Supervisa la actividad en busca de acciones malintencionadas y gestiona los incidentes de seguridad. Además, puedes facilitar los procesos operativos que evitan, detectan y responden a las amenazas.

Cloud Security Command Center: una herramienta que te permitirá evitar y detectar amenazas más fácilmente, así como responder a ellas

Centro de seguridad de G Suite: Consulta información importante sobre el uso compartido de archivos con usuarios externos, sobre el spam y el software malicioso dirigido a usuarios de tu organización, y también métricas para comprobar la eficacia de tus medidas de seguridad

Centro de alertas de G Suite: Recibe alertas en tiempo real y consejos de seguridad sobre la actividad de tu dominio para que puedas tomar medidas. Protege tu organización frente a las nuevas amenazas para la seguridad

Transparencia de acceso : proporciona registros casi en tiempo real cuando los administradores de Google Cloud Platform (GCP) acceden a tu contenido.

Transparencia de acceso de G Suite : puedes utilizar la Transparencia de acceso y consultar registros de las tareas que han llevado a cabo miembros del personal de Google al acceder a contenido de usuarios. Consideramos contenido generado por usuarios el texto que se introduce en Gmail, Documentos, Hojas de cálculo, Presentaciones y otras aplicaciones

Event Threat Detection: Detecta amenazas de seguridad en los entornos de Google Cloud Platform

Registros de auditoría de Cloud: visibilidad sobre todas las actividades de los usuarios en la nube de Google y consulta quién hizo qué, cuándo y dónde.

Inventario de recursos de Cloud : inventario de metadatos que le permite ver, monitorizar y analizar todos sus activos de la nube de Google en proyectos y servicios.

Auditorías y certificaciones de terceros : La transición a la nube implica tener que proteger cargas de trabajo sensibles y, al mismo tiempo, cumplir y mantener la conformidad con complejos requisitos normativos, frameworks y directrices.

Cloud Data Loss Prevention: te ayuda a identificar y gestionar mejor los datos sensibles. Ofrece funciones de clasificación y ocultamiento rápidas y escalables de ese tipo de datos