ANÁLISIS ESTRATÉGICO DEL SECTOR DE COMPUTACIÓN EN LA NUBE

GRADO EN INGENIERÍA INFORMÁTICA DEL SOFTWARE

TRABAJO DE FIN DE GRADO

Autora

María Teresa Fernández Coro

Tutora

María Begoña López Fernández

Cotutor

Clayson Cosme Da Costa Pimenta

2024

Resumen

El análisis estratégico del sector de computación en la nube revela un entorno altamente dinámico, en constante evolución y muy competitivo, impulsado por la innovación tecnológica y la creciente demanda de servicios flexibles y escalables. Este sector es cada vez más importante en la economía digital global. Factores políticos, económicos, sociales, tecnológicos, ecológicos y legales (PESTEL) influyen significativamente en su desarrollo, mientras que el Modelo de las Cinco Fuerzas de Porter destaca la intensa rivalidad entre competidores, la amenaza de nuevos entrantes y productos sustitutos, y el poder de negociación de proveedores y clientes. Las empresas líderes, como Amazon Web Services (AWS), se distinguen por su capacidad de innovación continua y robustez de servicios, aunque deben enfrentar desafíos críticos en seguridad y conformidad normativa para mantener la confianza del mercado y asegurar un crecimiento sostenible.

Índice

Índice de Ilustraciones

Capítulo 1. Introducción

Motivación

La computación en la nube, una de las tecnologías más revolucionarias de la última década, ha cambiado la forma en que las empresas administran sus recursos informáticos y prestan servicios digitales. Este paradigma tecnológico permite a las organizaciones acceder a recursos informáticos bajo demanda a través de una infraestructura escalable y flexible, lo que ofrece una serie de beneficios significativos en términos de eficiencia operativa, agilidad empresarial y reducción de costos.

Este estudio analiza el panorama actual del sector de la computación en la nube e identifica las tendencias emergentes y desafíos estratégicos que enfrentan las empresas que operan en este entorno. En un mundo cada vez más digitalizado y competitivo, es fundamental que las empresas comprendan cómo aprovechar al máximo las oportunidades que ofrece la computación en la nube, de modo que puedan tomar decisiones estratégicas informadas.

Objetivos

El objetivo general de este trabajo es el de contribuir al conocimiento del sector de la computación en la nube ofreciendo una visión comprensiva de su estado actual, perspectivas de futuro e implicaciones estratégicas para las empresas que operan en el sector. Para alcanzar ese objetivo se plantean los siguientes objetivos específicos:

- ✓ Comprender el sector de la computación en la nube.
- ✓ Conocer las tecnologías emergentes.
- ✓ Analizar en profundidad el caso del líder del sector, Amazon Web Services.
- ✓ Analizar la seguridad y el cumplimiento normativo en la nube.

Capítulo 2. Marco teórico

¿Qué es la Computación en la Nube?

Del inglés Cloud Computing, se puede definir como el suministro de recursos informáticos (servidores, almacenamiento de datos, bases de datos, redes, software y más) bajo demanda a través de Internet, que ha transformado el panorama digital ofreciendo una alternativa flexible, escalable y costo-eficiente a la infraestructura tradicional. Ali Sunyaev (2020) define la computación en la nube como la evolución de las tecnologías de la información y el modelo de negocio dominante para proporcionar recursos informáticos escalables bajo demanda.

Cloud computing is an evolution of information technology and a dominant business model for delivering IT resources. With cloud computing, individuals and organizations can gain on-demand network access to a shared pool of managed and scalable IT resources, such as servers, storage, and applications.

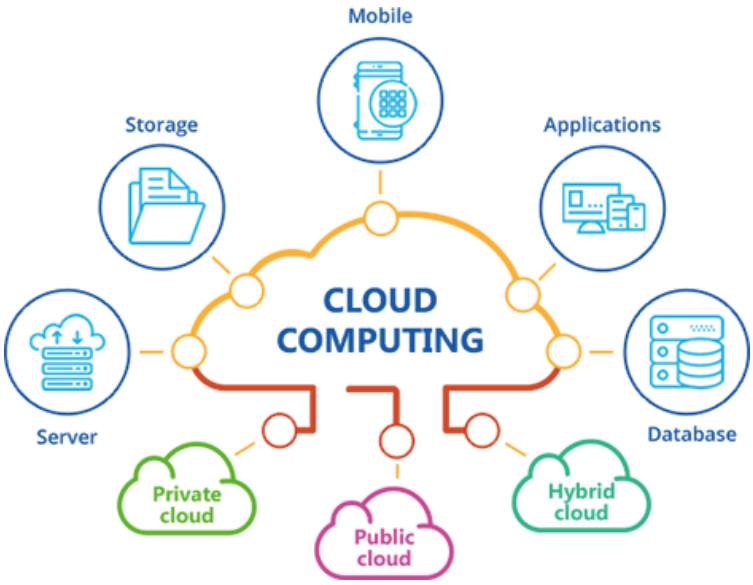

Ilustración 1. Cloud Computing. Fuente: Quizlet

Los servicios en la nube se alojan en un centro de datos del proveedor de servicios en la nube o *Cloud Service Provider* (en adelante CSP). Su objetivo principal es ofrecer una innovación más rápida, recursos flexibles y economías de escala.

El CSP elimina la necesidad de las empresas de obtener, configurar o administrar recursos por su cuenta; de esta forma, solo han de pagar por aquello que quieran utilizar. Esta cualidad permite que las organizaciones escalen con mayor rapidez y eficiencia reduciendo el coste de compra y mantenimiento de sus propios centros de datos físicos y servidores. También permite que se adapten a mercados y métricas cambiantes con mayor facilidad.

Inicios del sector

Los inicios de la computación en la nube se remontan a los años 50, cuando surgieron los *mainframes*[1] o servidores como primeros precursores, permitiendo el acceso de múltiples usuarios a un ordenador central. En 1960, John McCarthy propuso que algún día la informática sería realizada por *«empresas de servicios públicos a nivel nacional»*, momento en el que se origina el concepto de "cloud computing".

En aquellos años, el adelantado informático Licklider tuvo la idea para la computación en la nube antes de que se dispusiese de los medios para su desarrollo. En 1969 se desarrolló ARPANET[2], era una red de computadoras construida como un medio resistente para enviar datos militares y conectar principales grupos de investigación a través de los Estados Unidos. En 1999, fue la llegada de Salesforce, empresa pionera en el concepto de la entrega de aplicaciones empresariales a través de una página web simple.

Posteriormente, en 2006 Amazon lanza Amazon Web Services, marcando el inicio de la era moderna de la computación en la nube. En 2010 Microsoft lanza Azure, y es en 2011 cuando Google lanza Google Cloud Platform. En ambos casos se trata de empresas procedentes del sector de distribución y no de la industria informática como es el caso de otros competidores tales como Google o Microsoft.

A continuación, se presenta un diagrama de línea de tiempo que ilustra la evolución de la computación en la nube desde sus inicios. El diagrama destaca los hitos más importantes que marcaron el desarrollo de esta tecnología revolucionaria.

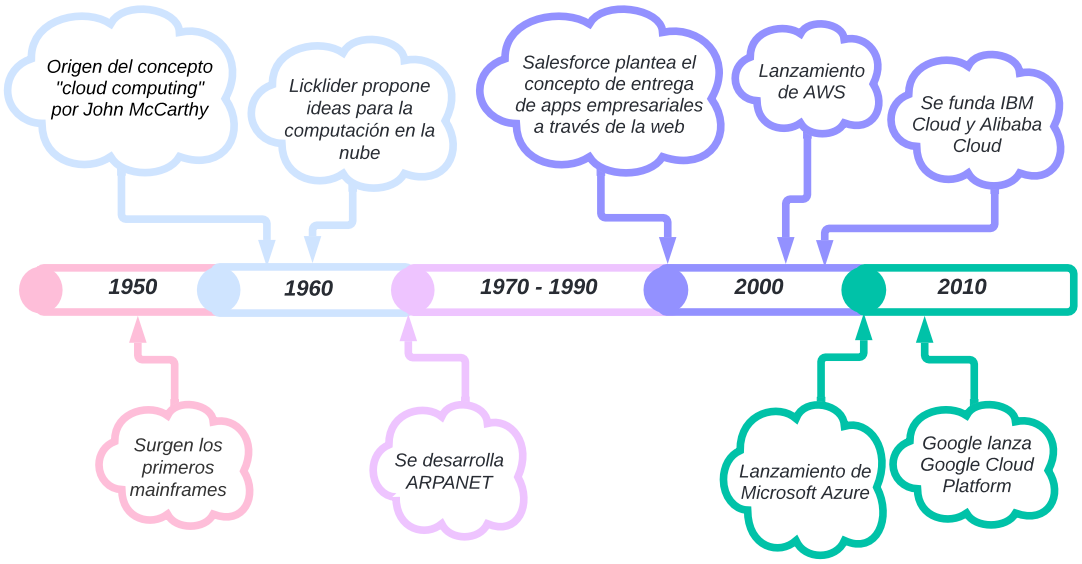

Ilustración 2. Línea de tiempo del inicio del sector. Fuente: Elaboración propia

El diagrama de línea de tiempo sirve como una guía visual para comprender la trayectoria de la computación en la nube. Sin embargo, es importante recordar que la evolución de esta tecnología ha sido un proceso complejo y dinámico, con numerosos actores e innovaciones que han contribuido a su desarrollo actual.

[1] Computadoras de alto rendimiento con grandes cantidades de memoria y procesadores que procesan miles de millones de cálculos y transacciones simples en tiempo real

[2] Advanced Research Projects Agency Network o Red de Agencias de Proyectos de Investigación Avanzada

Pero ¿quiénes pueden utilizar la Computación en la Nube?

Al ser una tecnología versátil puede ser utilizada por una amplia gama de usuarios, como empresas de todo tipo, tamaño y sector, e incluso individuos. Cada proveedor ofrece una gama de servicios y precios diferentes, por lo que el usuario u organización deberá escoger aquel que mejor se adapte a sus necesidades.

Características

El NIST[3] destaca las siguientes características esenciales:

- *Autoservicio bajo demanda*: Un consumidor puede obtener prestaciones informáticas de forma automática sin necesidad de interacción humana con el proveedor de servicios.
- *Amplio acceso a la red*: Las prestaciones están disponibles a través de la red y se pueden acceder a través de mecanismos estándar que favorecen el uso de plataformas heterogéneas.
- *Agrupación de recursos*: Los recursos informáticos del proveedor de servicios se agrupan y se asignan y reasignan dinámicamente en función de la demanda de los consumidores. Existe un sentido de independencia de la ubicación en el sentido de que el cliente generalmente no tiene control o conocimiento sobre la ubicación exacta de los recursos proporcionados, pero puede ser capaz de especificar la ubicación a un nivel superior de abstracción (por ejemplo, país, estado o centro de datos).
- *Rápida elasticidad*: Los recursos pueden aprovisionarse y liberarse elásticamente en función de la demanda. Las prestaciones disponibles para el aprovisionamiento del consumidor suelen parecer ilimitadas, por lo que pueden apropiarse de ellas en cualquier cantidad y momento.
- *Servicio medido*: Los sistemas en la nube controlan y optimizan automáticamente el uso de los recursos, lo que proporciona transparencia tanto al proveedor como al consumidor del servicio utilizado.

Ventajas

- ✓ Ahorro en costes: Permite optimizar los costes, ya que elimina la inversión de capital necesaria para la adquisición de hardware y software, así como para la configuración y ejecución de centros de datos locales.
- ✓ Velocidad: La mayoría de los servicios se ofrecen como autoservicio, se aprovisiona espacio al instante, lo que aporta una gran flexibilidad.
- ✓ Flexibilidad: Permite escalar los recursos de forma elástica y global, es decir, proporciona los recursos adecuados en el momento necesario y desde la ubicación geográfica adecuada.
- ✓ Productividad: Elimina la necesidad de realizar muchas tareas de administración de TI[4] que requieren mucho tiempo, dejando así que los equipos de TI se dediquen a otras tareas.
- ✓ Rendimiento: Se consigue una latencia de red menor para las aplicaciones y mayores economías de escala en comparación con un único centro de datos corporativo, ya que los mayores servicios informáticos en la nube se ejecutan en una red mundial de centros de datos seguros.
- ✓ Fiabilidad: Facilita y abarata la creación de copias de seguridad de datos, y su recuperación ante desastres, al poderse reflejar los datos en varios sitios redundantes en la red del CSP.

[3] National Institute of Standards and Technology
[4] Tecnología de la Información

- ✓ Seguridad: Refuerzan la situación general de seguridad frente a posibles amenazas ofreciendo tecnologías, directivas y controles.

Empresas de todas las industrias migran a la nube debido a una serie de tendencias. La forma actual de impulsar el negocio para una empresa puede no brindar la agilidad necesaria para crecer o la flexibilidad para competir. Por ello, las soluciones de nube ayudan a las empresas a afrontar los desafíos de la era digital pudiendo adaptarse rápidamente a las situaciones comerciales y reducir los costos, lo que permite que las empresas alcancen su máximo potencial comercial.

Limitaciones

Uno de los principales desafíos de la computación en la nube es la seguridad y privacidad de los datos. Los usuarios y organizaciones confían sus datos a proveedores de servicios externos que pueden no contar con las medidas adecuadas de protección de datos contra el acceso, la destrucción o la divulgación no autorizada. Es muy importante el cumplimiento, por parte tanto de los CSP como de las organizaciones, de ciertas regulaciones o estándares de protección de datos. Además, la computación en la nube puede estar sujeta a diferentes regulaciones en diferentes países.

Las empresas son dependientes de su CSP, y por ello pueden verse afectadas en su capacidad para acceder a sus datos y aplicaciones si el proveedor sufre algún problema.

Otro aspecto a tener en cuenta por las empresas es el plan de migración de datos y aplicaciones a la nube, así como el consumo de energía y recursos de los distintos CSP según su compromiso con la sostenibilidad.

Toda empresa, al comprender estas limitaciones y tomar las medidas oportunas para superarlas, podrá aprovechar al máximo esta tecnología.

Modelos de implementación

En función de las necesidades de la organización los CSP ofrecen distintas formas de implementar los servicios en la nube. Los modelos más comunes son la nube pública, privada e híbrida, pero también existen otros modelos como la nube comunitaria o la multinube, en auge actualmente.

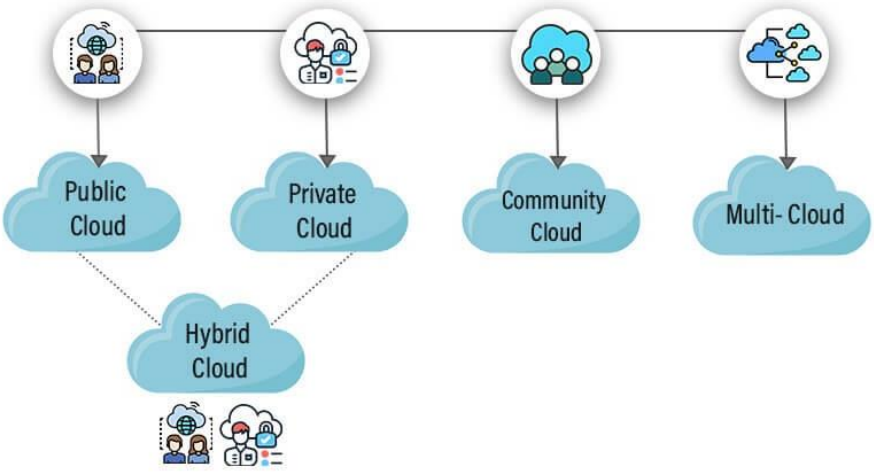

Ilustración 3. Modelos de implementación cloud. Fuente: EDUCBA

A continuación, se describen los modelos de implementación cloud descritos por el NIST:

Nube pública

Toda su infraestructura es propiedad del proveedor de servicios en la nube y se encuentra ubicada en sus instalaciones. Este presta sus servicios a los clientes a través de Internet de forma gratuita, o según modelos de precios basados en suscripción o de pago por uso.

La nube pública es un entorno multiusuario. Todos los clientes de la nube pública comparten la infraestructura del centro de datos del proveedor de la nube.

Las principales nubes públicas son Amazon Web Services (AWS), Google Cloud Platform (GCP), IBM Cloud, Microsoft Azure y Oracle Cloud.

Muchas empresas migran partes de su infraestructura de TI a la nube pública porque los servicios de nube pública son flexibles y fácilmente escalables a los flujos de trabajo. Otra ventaja es la reducción del costo al pagar, en la mayoría de los casos, solo por lo que utilizan y no tener que invertir en la configuración y mantenimiento de su propia infraestructura local. Lo que se suele llamar, Pago por Uso.

La seguridad y la privacidad pueden ser desventajas respecto a esta nube, además, los clientes no tienen tanto control sobre la infraestructura como en otros modelos.

Dentro de estas nubes podemos encontrar englobadas las nubes privadas virtuales o VPC[5], las cuales se caracterizan por ser un entorno de computación aislado y seguro dentro de la nube pública. Se crean utilizando tecnologías de virtualización para dividir la infraestructura de la nube pública en múltiples redes privadas. Mejoran la seguridad de los datos al encriptarlos a través de la implantación de una VPN[6].

Nube privada

La infraestructura y servicios de este modelo de nube es accesible por un solo cliente, y se aloja de forma privada en su propio centro de datos, lo que comúnmente se conoce como “local”, aunque algunas compañías pagan a proveedores de servicios externos para que hospeden su nube privada. Las entidades que optan por este tipo de sistemas son aquellas que tienen un alto nivel de complejidad y necesitan centralizar sus recursos, como pueden ser las grandes corporaciones o administraciones públicas.

Proporciona mayor control, seguridad y privacidad de datos que la nube pública, aunque puede ser más costosa al requerir más recursos y experiencia para administrarla.

Actualmente, uno de los sistemas más empleados por las empresas para llevar a cabo este despliegue es OpenStack, líder en nubes privadas. Se trata de un software de código abierto que permite producir una plataforma de cloud computing que se caracterice por ser ubicua, flexible y adaptable, fácil de implementar y altamente escalable.

OpenStack proporciona soporte API nativo para varios sistemas de programación, también distintas opciones de almacenamiento y ofrece la gama máxima de software de virtualización, compatible con hipervisor KVM, QEMU, Hyper-V, contenedor Linux (LNC), etc.

[5] Virtual Private Cloud
[6] Red Privada Virtual o Virtual Private Network

Nube híbrida

Esta implementación combina modelos de nube pública y privada, lo cual permite a las empresas aprovechar los servicios de nube pública y mantener las capacidades de seguridad y cumplimiento que suelen encontrarse en las arquitecturas de nube privada. Ambas se encuentran enlazadas mediante una tecnología que permite compartir datos y aplicaciones entre ellas aportando una gran flexibilidad y más opciones de desarrollo.

Este tipo de servicios también se pueden realizar a través de Openstack. De hecho, según un informe de OpenStack (2022), el 80% de los encuestados están adoptando un enfoque híbrido combinando el uso de nubes públicas y privadas y, en muchos casos, están empleando despliegues de OpenStack, lo que se refleja en el uso de este software que ha aumentado del 77% al 80% respecto al año anterior. Entre las empresas que lo utilizan se encuentra la NASA.

Multi-Nube

Este modelo combina el uso de dos o más nubes de dos o más proveedores de nube diferentes.

Muchas organizaciones optan por este tipo de implementación para evitar posibles bloqueos de proveedores, pudiendo operar en otras nubes cuando una falle. Sin embargo, al poseer varias nubes y de distintos proveedores puede resultar más complicado llevar a cabo una buena gestión de estas. Las plataformas de administración multi-nube facilitan esta cuestión por medio de un panel central donde se permite su gestión.

En una encuesta realizada por Gartner (2023) a usuarios de nubes públicas, el 81% de los encuestados afirmaron trabajar con varios proveedores cloud. La nube híbrida sigue siendo la más popular según el estudio, un 45% de las empresas la utilizan, pero la adopción de la multi-nube se encuentra en auge con un 30% de empresas utilizándola.

El estudio Cloud Security Report de Cybersecurity Insiders y Fortinet (2024) obtuvo que un 78% de las organizaciones prefieren utilizar modelos híbridos, el 43%, y multi-nube, el 35%, antes que la nube única, únicamente el 22%.

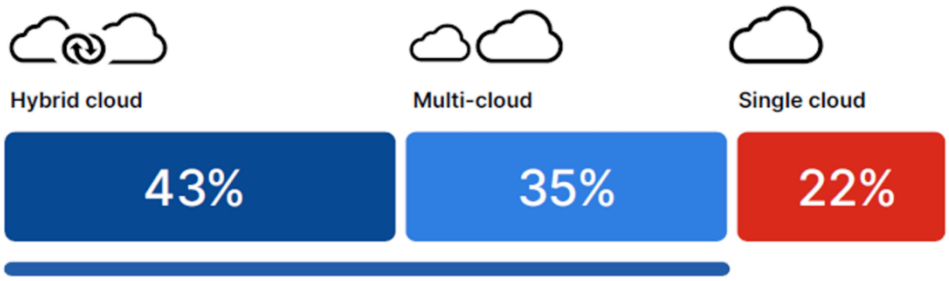

Ilustración 4. La preferencia de la nube híbrida y multi-nube continúa. Fuente: Fortinet

Nube comunitaria

La infraestructura de este modelo de nube se suministra para el uso exclusivo de una comunidad específica de consumidores de organizaciones que comparten intereses, es decir, se organiza con la finalidad de servir a una función o propósito común (seguridad, política…). Puede ser propiedad y estar gestionada por una o varias organizaciones de dicha comunidad, por un tercero o por una combinación de ellas, y puede existir dentro o fuera de sus instalaciones.

Tipos de servicios

SaaS [7](Software como servicio)

También conocido como software basado en la nube o aplicaciones en la nube, es un software de aplicación alojado en la nube, al que los usuarios acceden a través de un navegador web, o cualquier aplicación diseñada para tal efecto. El usuario no posee control sobre este, sino que es el proveedor SaaS quien se encarga de ejecutarlo y administrarlo. Un ejemplo típico es el correo electrónico basado en web.

En la mayoría de los casos, los usuarios pagan una cuota de suscripción mensual o anual, aunque algunos proveedores pueden ofrecer precios de pago por uso en función de su uso real.

Además de los beneficios de ahorro de costos, tiempo de amortización y escalabilidad de la nube, SaaS ofrece actualizaciones automáticas y protección contra la pérdida de datos.

Es el principal modelo de entrega para la mayoría del software comercial hoy en día. Un ejemplo es Amazon Web Services con su servicio de compras online (sitios web y tiendas virtuales para tiendas online) o Dropbox con su sistema de backup (para copia de seguridad de archivos y almacenamiento de datos).

Aplicaciones que una plataforma SaaS puede ofrecer incluyen servicios empresariales como aplicaciones de tipo ERP, CRM, facturación, ventas y recursos humanos como Salesforce, software de gestión de proyectos ágiles como Jira, plataformas de mensajería instantánea como Slack o soluciones en la nube para la gestión de nóminas o rendimiento como Workday.

PaaS[8] (Plataforma como servicio)

Ofrece a los desarrolladores de software todos los recursos de hardware y software necesarios para ejecutar, desarrollar y administrar aplicaciones en la nube sin el costo, la complejidad y la inflexibilidad de mantener la infraestructura subyacente.

Hoy en día, PaaS suele basarse en contenedores, un modelo de cómputo virtualizado a un paso de los servidores virtuales. Los contenedores virtualizan el sistema operativo, permitiendo a los desarrolladores empaquetar la aplicación solo con los servicios del sistema operativo que necesita ejecutar en cualquier plataforma, sin modificación y sin necesidad de middleware.

Ejemplos de PaaS son AWS Elastic Beanstalk (despliegues en un conjunto de Servicios de AWS), Heroku (admite varios lenguajes de programación y una alta escalabilidad) y Red Hat OpenShift (basada en Kubernetes, permite usar Git para desplegar aplicaciones Web en diferentes lenguajes).

IaaS[9] (Infraestructura como servicio)

Ofrece acceso bajo demanda a recursos informáticos como servidores físicos y virtuales, redes y almacenamiento en Internet sobre la base de pago por uso. En comparación con otros modelos de computación en la nube, IaaS ofrece a los usuarios el mayor control sobre los recursos informáticos.

Algunos ejemplos de IaaS son los proveedores de nube pública como AWS, Microsoft Azure y Google Cloud.

Estos tipos de servicios suelen representarse en capas de una pila, que ofrecen distintos niveles de abstracción. No obstante, estas capas no son necesariamente interdependientes.

[7] Software as a Service
[8] Platform as a Service
[9] Infrastructure as a Service

En la siguiente ilustración se pueden apreciar en color azul claro los niveles de la pila que son gestionados por el proveedor de servicios según el tipo de servicio proporcionado, y en un color más oscuro aquellos que han de ser gestionados por el cliente.

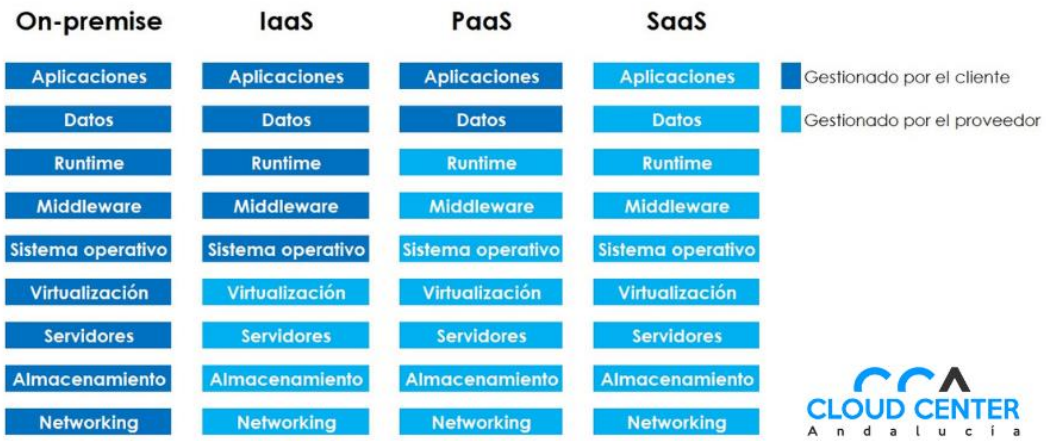

Ilustración 5. Diferencias entre los tipos de servicios. Fuente: Cloud Center Andalucía

La opción on-premise ha de ser gestionada por el cliente, tanto su instalación y mantenimiento como los costes asociados. Debido a esto, este modelo tradicional dispone de un coste asociado mayor al de los servicios en la nube, además de poseer una rigidez inherente pudiendo convertirse en una barrera para la innovación y la adaptabilidad a medida que evolucionan las demandas del mercado.

La ilustración muestra a la izquierda la inclusión de los costes operativos variables por operaciones además de las inversiones de capital fijo en un entorno de informática tradicional (on-premise), frente a los costes variables por operaciones en entornos de computación en la nube.

Debemos tener en cuenta que el coste fijo es el costo principal y podría reducirse ligeramente a medida que aumente el número de usuarios, sin embargo, los costes operativos pueden aumentar considerablemente con un mayor número de usuarios, por lo que el coste total aumenta rápidamente si el número de usuarios crece.

Por otra parte, la computación en la nube aplica un modelo comercial de pago por uso, por lo que al utilizar la nube no se tiene un coste inicial en adquisiciones de hardware de manera que únicamente se repercuten al usuario los costes variables, como se muestra en la figura.

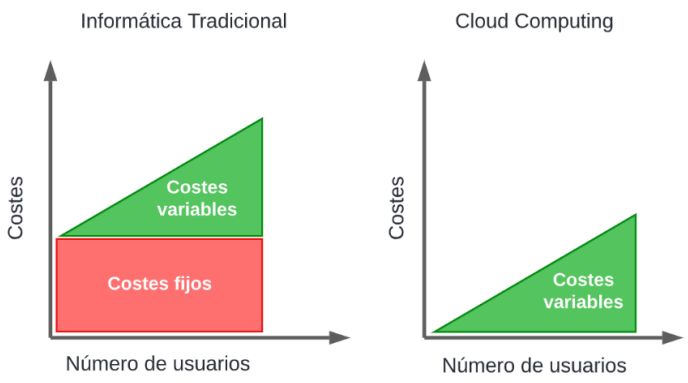

Ilustración 6. Costos asociados al modelo tradicional vs cloud computing. Fuente: Elaboración propia

En general, la computación en la nube reducirá los costes para los usuarios, produciendo un efecto liberador sobre todo para las empresas de nueva creación. El hecho de que los usuarios de la nube solo paguen los gastos de operación y no tengan que invertir en equipos permanentes es especialmente atractivo para un gran número de usuarios que no disponen de recursos suficientes para desplegar un centro de datos propio, incluyendo empresas de nueva creación o start-ups.

Gartner (2023) prevé que la infraestructura como servicio (IaaS) experimente el mayor crecimiento del gasto de los usuarios finales en 2024, con un 26,6%, seguida de la plataforma como servicio (PaaS), con un 21,5%.

Se espera que todos los segmentos del mercado de la nube crezcan en 2024. Si bien IaaS y PaaS impulsan el mayor crecimiento del gasto, SaaS sigue siendo el segmento más grande del mercado de la nube en términos de gasto del usuario final.

A continuación, se puede observar en la tabla el pronóstico de Gartner sobre el gasto en servicios de la nube pública por segmentos de mercado para 2022, 2023 y 2024. El pronóstico de este artículo muestra que el gasto en la nube pública seguirá creciendo a un ritmo saludable en los próximos años.

	2022	2023	2024
Cloud Application Infrastructure Services (PaaS)	119,579	145,320	176,493
Cloud Application Services (SaaS)	174,416	205,221	243,991
Cloud Business Process Services (BPaaS)	61,557	66,339	72,923
Cloud Desktop-as-a-Service (DaaS)	2,430	2,784	3,161
Cloud System Infrastructure Services (IaaS)	120,333	143,927	182,222
Total Market	**478,315**	**563,592**	**678,790**

BPaaS = business process as a service; IaaS = infrastructure as a service; PaaS = platform as a service; SaaS = software as a service
Note: Totals may not add up due to rounding.

Ilustración 7. Previsión del gasto mundial de los usuarios finales en servicios en la nube pública (millones de dólares estadounidenses). Fuente: Gartner

Tecnologías clave

Se destacan varias tecnologías que desempeñan un papel fundamental en el sector de computación en la nube al permitir la creación y mantenimiento de infraestructuras flexibles, escalables y eficientes.

Virtualización

Esta tecnología permite la creación de entornos virtuales que simulen un sistema operativo, servidores, redes o dispositivos de almacenamiento.

En el contexto de la computación en la nube, los CSP construyen y mantienen sus propios centros de datos empleando la virtualización, para ello crean diferentes entornos o máquinas virtuales (VM[10]) que son

[10] Virtual Machine

instancias virtuales de servidores físicos. Las VM pueden ejecutar sistemas operativos y aplicaciones de forma independiente del hardware físico subyacente.

De esta forma, la virtualización permite la ejecución multiplexada de varias máquinas virtuales sobre el mismo hardware de un ordenador anfitrión. Para ello, se requiere de un hipervisor o capa de virtualización en la máquina anfitrión, que puede ser de tipo 2 si realiza interacciones con el sistema operativo anfitrión o de tipo 1 si directamente interactúa con el hardware de la máquina.

Algunos ejemplos de hipervisores conocidos son: VMware ESXi, uno de los más demandados hoy en día, Microsoft Azure emplea Microsoft Hyper-V o, por ejemplo, el empleado por AWS, AWS Nitro Enclaves.

Además, esta tecnología ayuda a optimizar el uso de recursos, mejorar la eficiencia energética y facilitar la gestión y escalabilidad de infraestructuras de TI, sin olvidar que permite una rápida recuperación del acceso a la infraestructura ante desastres naturales o ciberataques. Aumentando así la resiliencia y permitiendo a las empresas continuar con sus operaciones.

Para poder llevar a cabo este proceso se requiere un hardware potente, tanto en recursos como en capacidad de procesamiento. Aun así, los beneficios de esta tecnología son mayores a sus desventajas.

Por tanto, se puede decir que la computación en la nube es impensable sin el aporte de la tecnología de virtualización.

Contenedores

Son otra forma de virtualización que permite empaquetar aplicaciones y sus dependencias en un entorno aislado, ligero, portátil y autosuficiente.

A diferencia de las máquinas virtuales, comparten el kernel del sistema operativo del host[11], lo que los hace más eficientes en términos de recursos y más portables. Otro beneficio de los contenedores es su facilidad de despliegue y gestión de aplicaciones en entornos de nube.

Las dos plataformas de contenedores más conocidas y utilizadas actualmente son Docker y Kubernetes.

IaC[12] (Infraestructura como Código)

Se trata de la gestión y aprovisionamiento de infraestructuras de TI mediante código en lugar de procesos manuales. Requiere la creación de archivos de configuración que contienen las especificaciones de la infraestructura a crear. Esto facilita la duplicación del entorno y la automatización de su gestión, evitando a su vez errores o cambios de configuración no documentados.

Algunos de los ejemplos más populares son Terraform, AWS CloudFormation y Ansible.

Redes Definidas por Software (SDN)

Se trata de un enfoque de la infraestructura de red que separa las funciones de control y reenvío de la red. Permite una gestión de la red flexible y ágil, facilitando la automatización y una mayor seguridad y control de la red.

Los componentes de SDM son un controlador (centraliza la gestión y configuración de la red), un hipervisor (software que permite la virtualización de recursos de red) y una API[13] (permite controlar la red).

Mientras que la virtualización de redes permite a las organizaciones segmentar diferentes redes virtuales dentro de una única red física, o conectar dispositivos en diferentes redes físicas para crear una única red

[11] Núcleo del sistema operativo de la máquina anfitriona
[12] Infrastructure as Code
[13] Application Programming Interface

virtual, las redes definidas por software permiten una nueva forma de controlar el enrutamiento de paquetes de datos a través de un servidor centralizado.

Skanska, empresa sueca líder en construcción y desarrollo de proyectos, desplegó en 2018 Cisco ACI, uno de los productos para la creación y mantenimiento de SDN mejor valorados actualmente. Estableció un modelo de nube híbrida y sentó las bases para la IaC. Gracias al uso de este enfoque la empresa aceleró sus despliegues de red de semanas a días.

Almacenamiento en la nube

Modelo de almacenamiento de datos accesible y escalable a través de Internet. Permite a las organizaciones almacenar grandes volúmenes de datos de manera segura y acceder a ellos desde cualquier lugar. Por ejemplo, Google Cloud Storage.

Plataformas de Gestión de Nube

Permiten gestionar y optimizar recursos en nubes públicas, privadas e híbridas. Un ejemplo es Morpheus, solución centralizada en orquestación[14] y gestión de aplicaciones en la nube que facilita la reducción de costos, aumenta la seguridad y hace posibles despliegues de nubes híbridas en tiempos reducidos.

Estas tecnologías impulsan el futuro de la computación en la nube, ya que no solo facilitan la creación y mantenimiento de infraestructuras de nube flexibles y escalables, sino que también optimizan su eficiencia operativa. Juntas, estas tecnologías forman el núcleo de las soluciones modernas en la nube, habilitando a las organizaciones para enfrentar los desafíos del entorno digital actual y futuro.

Tendencias y tecnologías emergentes

El mundo de la computación en la nube está en constante evolución, con nuevas tecnologías y tendencias que surgen a un ritmo acelerado y que la redefinen constantemente. Si bien las tecnologías que hemos discutido en el apartado anterior sientan las bases de la infraestructura en la nube moderna, es hora de adentrarnos en el futuro y explorar las innovaciones que están configurando el panorama.

Algunas estas tendencias y tecnologías emergentes de la computación en la nube son:

AIaaS[15] (Inteligencia Artificial como Servicio)

La Inteligencia Artificial, AI[16] en adelante, es un conjunto de tecnologías que permiten a un sistema informático realizar tareas que normalmente se asocian con la inteligencia humana, como el aprendizaje, el razonamiento y la resolución de problemas.

De esta forma, la AIaaS permite a los proveedores en la nube y empresas aprovechar el potencial de la AI para desarrollar soluciones sin la necesidad de conocimientos o infraestructura especializados en AI. Es común que los servicios de esta tecnología se construyan sobre proveedores basados en la nube como AWS utilizados como IaaS.

Es por ello, que la AIaaS desempeña un papel importante en la optimización de procesos, la personalización de servicios y la automatización de tareas.

[14] Automatización y coordinación de tareas para administrar y optimizar recursos en la nube. Facilitando así su gestión, mejorando la eficiencia y reduciendo costos.
[15] Artificial Intelligence as a Service
[16] Artificial Intelligence

Computación cuántica

La computación cuántica es capaz de ejecutar algoritmos de procesamiento de datos complejos, permitiendo así resolver problemas complejos en un menor tiempo. Además, gracias a la nube se facilita el aprovechamiento de su amplio potencial. Un ejemplo de esta tecnología es Google Quantum AI.

Industry Cloud Platforms (ICP)

Las ICP integran servicios IaaS, PaaS y SaaS en una plataforma unificada adaptada a diferentes sectores como salud o finanzas.

Gartner prevé que en 2027 más del 70% de las empresas utilizarán plataformas industriales en la nube para acelerar sus iniciativas empresariales, frente a menos del 15% en 2023.

NaaS[17] (Red como Servicio)

Modelo de servicio en la nube de infraestructura autónoma y gestión de red como servicio, en el cual los clientes adquieren servicios de red proporcionados por proveedores de nube en lugar de establecer su propia infraestructura de red. De este modo, las empresas gestionan sus propias redes sin necesidad de ningún tipo de hardware, solo requieren conexión a Internet, mientras que los proveedores son los encargados de mantener la red y lleva a cabo la gestión del hardware y el software.

Este modelo permite a los clientes ahorrar en costes al simplificar y automatizar la gestión de la red. Así como disponer de una mayor seguridad, al encargarse NaaS de la integración entre la red y la seguridad de la red.

Un ejemplo de este tipo de servicio es Cloudflare Magic WAN.

Estas tendencias y tecnologías emergentes se encuentran configurando el panorama de la computación en la nube. Sin embargo, la innovación en este campo no se detiene. Nuevos avances y soluciones surgen constantemente, impulsando la evolución del ecosistema cloud computing.

[17] Network as a Service

Capítulo 3. Análisis Externo

Sector Cloud

Una vez analizada la naturaleza y las características de los servicios de la computación en la nube, se puede delimitar el sector o industria[18] de la computación en la nube como aquellas empresas que ofrecen servicios en alguna de las tres categorías definidas en el apartado anterior (SaaS, PaaS e IaaS).

El sector de la computación en la nube se encuentra en un auge continuo. El gasto mundial en infraestructura cloud aumentó un 2,9% interanual en el tercer trimestre de 2023, según IDC[19], y continúa superando al segmento no relacionado con la nube, que cayó un 8,2% en dicho periodo.

A largo plazo, IDC predice que el gasto mundial en infraestructura de computación en la nube tendrá una tasa de crecimiento anual compuesta (CAGR) del 10,6% durante el período de 2022 a 2027, alcanzando los 152.000 millones de dólares en 2027. Esto representa el 68,8% del gasto total, como se puede observar en la gráfica de la ilustración siguiente.

El gasto en infraestructura de nube compartida (pública) representará el 70,5% del gasto total en la nube en 2027, creciendo a una CAGR del 11,1% hasta alcanzar los 107.100 millones de dólares. Por otra parte, el gasto en infraestructura de nube dedicada (privada) crecerá a una CAGR del 9,7% hasta los 44.900 millones de dólares, representando el 29,5% del gasto en la nube total para 2027. En cambio, los gastos en la infraestructura no relacionada con la nube se mantendrán relativamente estables, creciendo a una CAGR del 1,6% hasta alcanzar los 68.900 millones de dólares en 2027.

IDC además predice que el gasto de los proveedores de servicios en infraestructura informática y de almacenamiento crezca a una CAGR del 10,4% hasta alcanzar los 148.900 millones de dólares en 2027.

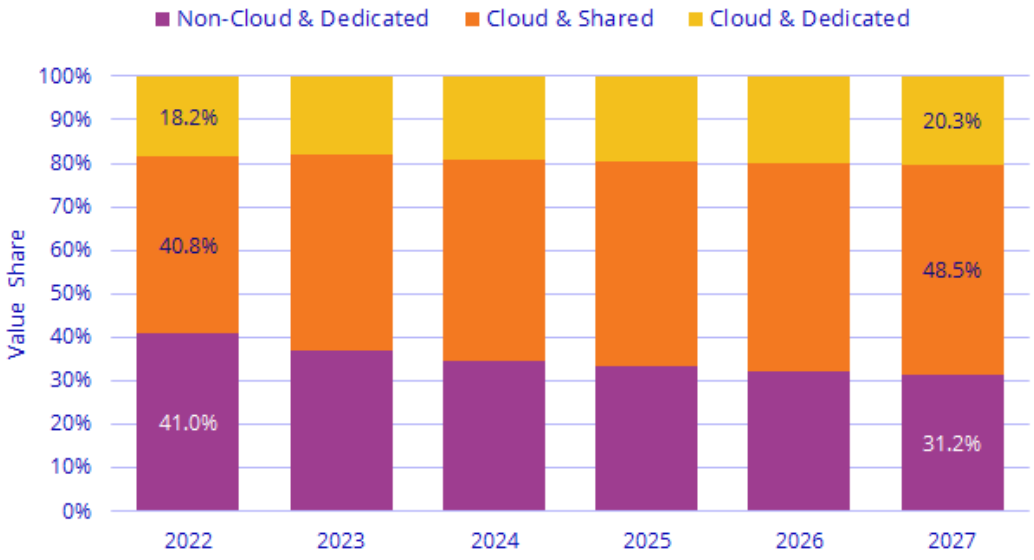

Ilustración 8. Gasto mundial en infraestructura de nube. Fuente: IDC

[18] A los efectos de este trabajo, se utilizan los términos sector e industria como sinónimos

[19] International Data Corporation, principal proveedor mundial de inteligencia de mercado, servicios de asesoramiento y eventos

El mercado de la computación en la nube crece en todas las regiones del mundo. Estados Unidos posee el mercado más grande, pero regiones como Asia-Pacífico se encuentran ante su mayor tasa de crecimiento anual adoptando nuevas tecnologías vanguardistas en la nube.

En 2023, el 45,2% de las empresas de la Unión Europea adquirieron servicios de computación en la nube. Se trata de un aumento de 4,2 puntos porcentuales (pp) en comparación con 2021. En el siguiente gráfico de Eurostat se puede apreciar dicha comparación.

Finlandia fue el país con mayor porcentaje de servicios adquiridos en 2023 con un 78,3%, seguido de Suecia con un 71,6%. España se encuentra casi al final de la gráfica rondando un 30%.

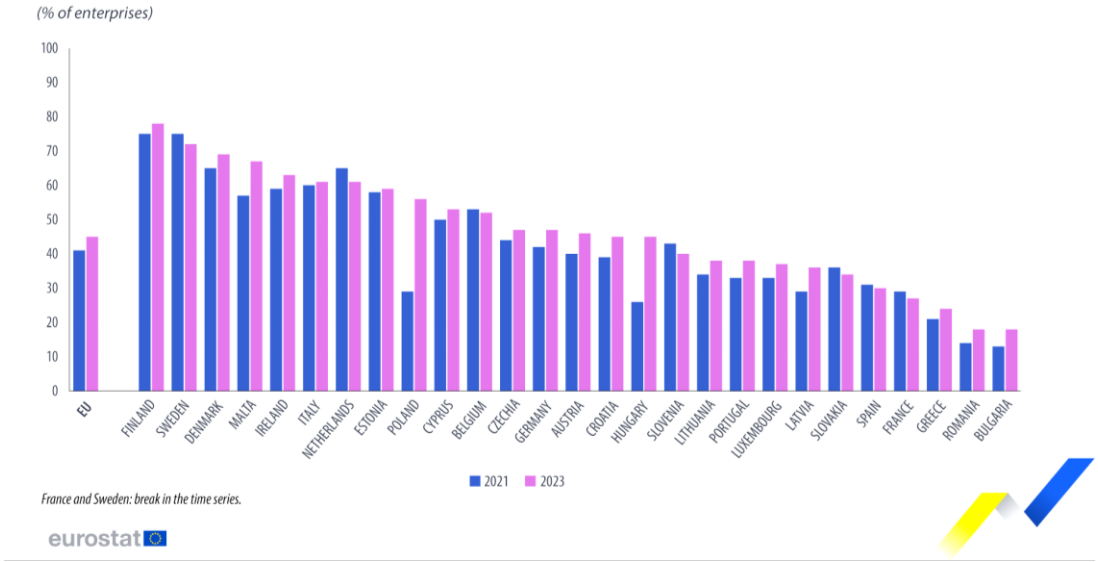

Ilustración 9. Compra de servicios en la nube en 2021 frente a 2023, por empresas de la UE. Fuente: Eurostat

De entre dichos servicios demandados en 2023, se encuentra en primer lugar el servicio de correo electrónico con un 82,7%, y en último lugar casi empatados se encuentran el software propietario con un 25,4% y el software de relación con el cliente con un 25%.

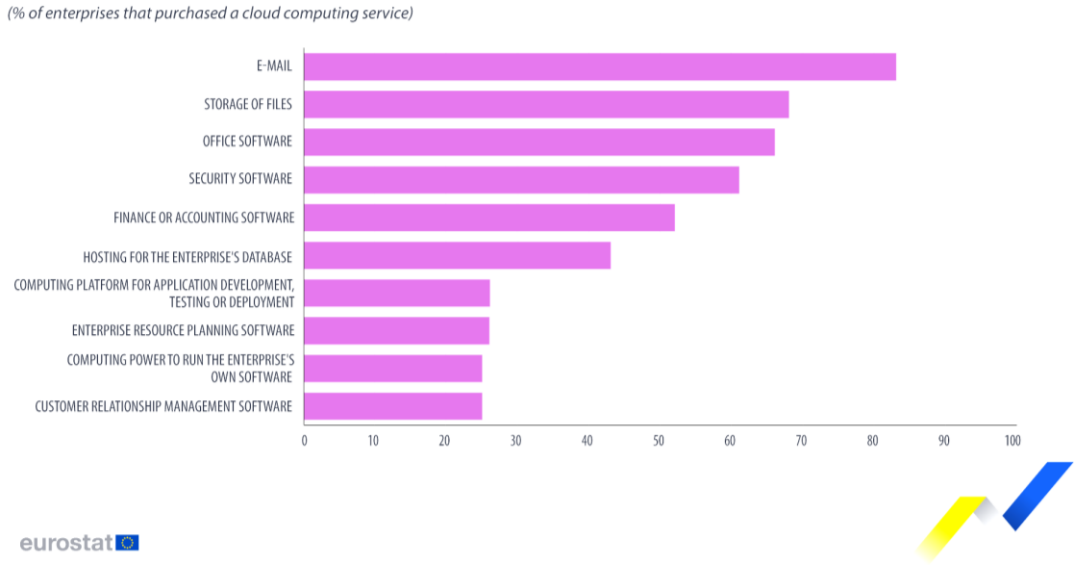

Ilustración 10. Servicios en la nube más comprados por la UE en 2023. Fuente: Eurostat

Una vez delimitado el sector, en las siguientes secciones se presentará a los principales competidores y se realizará un análisis externo del mismo, comenzando por un análisis PESTEL seguido por un análisis de la industria según el modelo de Porter que nos facilitará identificar oportunidades y amenazas que pueden facilitar o dificultar las posibilidades de alcanzar una ventaja competitiva sostenible.

Proveedores líderes del sector

Los tres proveedores líderes del mercado de servicios en la nube son, en primer lugar, Amazon Web Services, seguido de Microsoft Azure y Google Cloud Platform. Datos de Synergy Research Group muestran que, en conjunto, los tres líderes representaron el 67% del mercado mundial para el periodo de tiempo mostrado en el gráfico de la ilustración siguiente.

En términos de posicionamiento competitivo entre los principales proveedores de nube, Google y Microsoft consiguieron las cifras de crecimiento anual más fuertes, con Microsoft aumentando su cuota de mercado global en casi dos puntos porcentuales desde el cuarto trimestre del año pasado, obteniendo un 24% de participación global. La participación de Google también creció, sus cuotas de mercado mundiales en el cuarto trimestre fueron del 11%. Por su parte, Amazon vio caer su cuota mundial hasta el 31%, aunque mantuvo un fuerte crecimiento.

Entre los proveedores de segunda categoría[20], los que registraron las mayores tasas de crecimiento anual fueron Huawei, China Telecom, Snowflake, MongoDB, Oracle y VMware. En cambio, por cuota de mercado, destacaron Alibaba, Salesforce, IBM y Oracle, aunque con participaciones entre un 2% y un 5%.

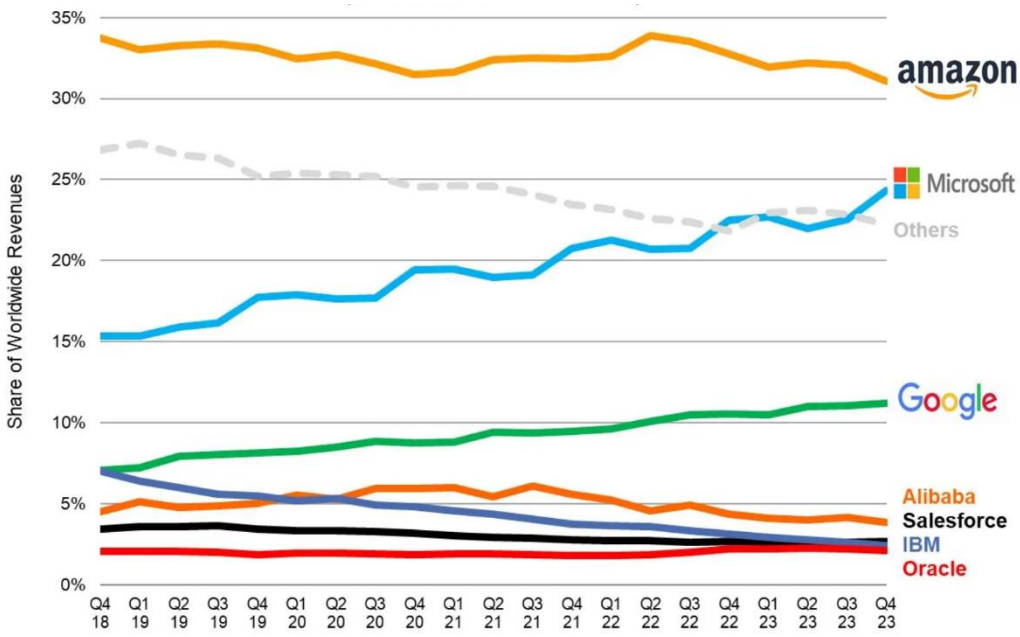

Ilustración 11. Proveedores cloud líderes. Fuente: Synergy Research Group

[20] Aquellos que están creciendo y cada vez son más importantes, pero no alcanzan las cuotas de mercado de los líderes del sector.

A medida que la adopción de la computación en la nube sigue creciendo, es esencial comprender las fortalezas y diferencias entre los principales proveedores del mercado: Amazon Web Services (AWS), Microsoft Azure y Google Cloud. La siguiente tabla comparativa destaca las características clave y servicios ofrecidos por cada uno de estos líderes, proporcionando una visión clara de sus capacidades y cómo se posicionan en el sector.

Servicios/Proveedores	AWS	Azure	Google Cloud
Modelo de servicio	IaaS, PaaS, SaaS	IaaS, PaaS, SaaS	IaaS, PaaS, SaaS
Computo	Amazon EC2 Instance	Azure Virtual Machines	Compute Engine
Contenedores	Amazon Elastic Kubernetes Service	Azure Kubernetes Service	Google Kubernetes Engine
Almacenamiento	AWS Simple Storage Service	Azure Blob Storage	Cloud Storage
Base de datos relacional	Amazon Relational Database Service (RDS)	SQL Database	Cloud SQL
Base de datos no relacional	DynamoDB	Azure Cosmos DB	Bigtable
Red	Virtual Private Cloud	Virtual Network	Virtual Private Cloud
Servicios	+200	+200	+120
Países	+200	+200	+200
AI y ML	SageMaker	Azure ML	TensorFlow
Seguridad	Identity and Access Management (IAM)	Azure Active Directory (AD)	Identity and Access Management (IAM)
Cuota de mercado	31	24	11
Precio	Modelo de pago por uso, basado en el consumo de recursos	Modelo de pago por uso, basado en el consumo de recursos	Modelo de pago por uso, basado en el consumo de recursos

Ilustración 12. Comparación AWS vs Azure vs Google Cloud. Fuente: Elaboración propia

Amazon Web Services (AWS)

Fundada en 2006, es el proveedor que domina el mercado de la computación en la nube. Ofrece una amplia gama de servicios de computación en la nube, posee una infraestructura global, precios competitivos, innovación continua y seguridad robusta. Netflix es un ejemplo de empresa que ya está en AWS.

Microsoft Azure

Lanzada en 2010, es el segundo proveedor de servicios en la nube a nivel mundial. Ofrece una amplia gama de servicios de computación en la nube, posee integración completa con productos de Microsoft, infraestructura global, y un enfoque de seguridad robusto y confiable. Un ejemplo de empresa que ya se encuentra en Azure es Siemens.

Google Cloud Platform (GCP)

Lanzada en 2011, es la oferta de Google en el mercado de la computación en la nube y se encuentra en la tercera posición a nivel mundial en este mercado. Ofrece una amplia gama de servicios de computación en la nube, aunque menor que la que ofrecen AWS y Azure. Destaca por su innovación y tecnología puntera, ya que aprovecha la experiencia de Google en IA, aprendizaje automático, big data y análisis de datos. También destaca por su soporte nativo para Kubernetes y por su cultura de código abierto que hace posible la integración de tecnologías y herramientas open source en GCP.

Spotify migró su infraestructura a Google Cloud Platform en 2016.

Entorno Genérico

El entorno genérico de un sector se refiere a las condiciones externas que afectan a todas las empresas que operan dentro de ese sector.

La dinámica y en constante evolución industria de la computación en la nube posee un entorno genérico en muy cambiante, influenciado por factores externos que abarcan desde regulaciones gubernamentales y políticas económicas hasta tendencias sociales y avances tecnológicos. Por ello, las empresas del sector deben estar atentas a los cambios en el entorno genérico y adaptar sus estrategias en consecuencia.

Para poder comprender este entorno se presenta a continuación un análisis PESTEL del sector de la computación en la nube.

Análisis PESTEL

Se trata de un análisis de factores políticos, económicos, sociales, tecnológicos, ambientales y legales que, en este caso, se centra en el sector de computación en la nube. Es un acrónimo en inglés de Political, Economic, Social, Technological, Environment and Legal.

Por medio de este análisis del sector se obtiene información relevante del entorno externo de una empresa, proporcionándole una comprensión clara de las oportunidades y riesgos potenciales que podrían tener impacto en su negocio.

Factores políticos

Los factores políticos desempeñan un papel fundamental en el entorno de la industria de la computación en la nube y afectan tanto las operaciones diarias como las estrategias a largo plazo de las empresas de este sector.

Regulaciones de protección y privacidad de datos como el RGPD[21] o CCPA[22] imponen medidas y requisitos de seguridad sobre los proveedores cloud. Estas regulaciones impactan en cómo los CSP procesan, almacenan y transfieren los datos de sus clientes, así como en la medida en qué dichos clientes confían en ellos.

Los gobiernos y sus políticas gubernamentales relacionadas con la ciberseguridad también influyen en las prácticas adoptadas por los CSP y la confianza de los clientes. También la inestabilidad política en un país o tensiones políticas comerciales pueden afectar, por ejemplo, a las cadenas de suministro aumentando costos o limitar la capacidad para operar o adquirir el material tecnológico necesario para una empresa.

Por otra parte, el apoyo gubernamental a la innovación tecnológica puede impulsar al crecimiento del sector de la computación en la nube, por ejemplo, fomentando inversiones en infraestructura digital o brindando oportunidades de expansión para proveedores de servicios en esta industria.

Por estos motivos, las empresas del sector de la computación en la nube deben monitorizar los factores políticos para garantizar su cumplimiento y aprovecharse de las oportunidades del mercado.

Factores económicos

Estos afectan a la demanda de servicios en la nube, así como a la expansión del sector. Uno de los factores económicos más influyentes es el crecimiento de la economía global, ya que en periodos de crecimiento económico las empresas tienden a aumentar su inversión en tecnología y servicios en la nube,

[21] Reglamento General de Protección de Datos, Reglamento 2016/679 del Parlamento Europeo y del Consejo
[22] Ley de Privacidad del Consumidor de California en los EEUU

incrementando así su eficiencia e innovación. Por el contrario, en periodos de recesión económica las empresas tienden a recortar gastos en tecnología, lo que afecta al sector de computación en la nube.

Los costos asociados al hardware y tecnología juegan un papel importante. Si estos se reducen permiten a los CSP ofrecer precios más competitivos. Sin embargo, las fluctuaciones de precios de componentes clave pueden afectar los márgenes de beneficio y las estrategias de precios de las empresas del sector.

Factores sociales

La aceptación y adopción de la tecnología por parte de la sociedad impulsa la proliferación de dispositivos conectados y el acceso generalizado a la red, lo que provoca la demanda de servicios en la nube que faciliten el procesamiento y almacenamiento de datos y la ejecución de aplicaciones complejas.

La pandemia global de COVID-19 ha acelerado la tendencia del teletrabajo y también la demanda de servicios que permitan la colaboración en línea. Otra tendencia como el cambio hacia el consumo bajo demanda está aumentando la necesidad de soluciones en la nube.

Factores tecnológicos

Los avances en tecnologías como la Inteligencia Artificial, el Machine Learning, el Big Data o el IoT están impulsando la evolución del sector y el crecimiento de la demanda de sus servicios. Sin embargo, la falta de estandarización puede afectar la interoperabilidad de entre diferentes proveedores de la nube y, por tanto, influir en el crecimiento del sector.

Factores ecológicos

En la actualidad, las preocupaciones medioambientales y la sostenibilidad están convirtiéndose en una de las prioridades de las empresas y los consumidores.

Factores como el consumo de energía, el uso de energías renovables, la reducción de la huella de carbono, la eficiencia de los recursos o la innovación en sostenibilidad se encuentra en auge en la industria de computación en la nube. Siendo esta una industria que se caracteriza por una alta demanda energética y de recursos materiales, por lo que se enfrenta a grandes desafíos.

Factores legales

Las leyes y regulaciones en torno a la privacidad y protección de datos, regulaciones de seguridad o leyes de propiedad intelectual, entre otras, afectan al sector de la computación en la nube.

Los proveedores de servicios en la nube han de navegar en un entorno regulatorio complejo, por ello deben conocer y cumplir estas leyes.

En resumen, al analizar los factores externos que influyen en el sector de la computación en la nube se puede apreciar como el sector es complejo y dinámico, y como se ve influenciado por diversos factores políticos, económicos, sociales, tecnológicos, ecológicos y legales que las empresas del sector han de tener en cuenta para operar de manera eficiente y seguir siendo competitivas en el mercado.

Como empresa del sector, entender estos factores es crucial para anticipar oportunidades y amenazas, y para formular estrategias empresariales efectivas en este sector en constante evolución.

Entorno Específico

Hace referencia a aquellos factores que influyen sobre un determinado grupo de empresas que comparten características comunes y que se encuentran en la misma industria. En este caso, a las interacciones directas entre las empresas competidoras del sector de la computación en la nube, como también a sus relaciones con los proveedores, clientes u otros actores de interés.

Este entorno se ve influenciado por una competencia feroz entre gigantes tecnológicos. Los proveedores hardware y software rigen las capacidades de las plataformas en la nube, las alianzas estratégicas o colaboraciones entre empresas repercuten en el sector, y este también es sensible a las normativas de protección de datos y ciberseguridad.

En el siguiente apartado, se analiza este entorno utilizando el marco de las cinco fuerzas de Porter.

Fuerzas de Porter

El análisis de las cinco fuerzas de Porter, llamado así por su creador Michael E. Porter, permite comprender la dinámica competitiva del sector de la computación en la nube por medio del análisis de los siguientes cinco elementos:

Poder de negociación de los clientes

Es moderadamente alto. Los clientes tienen una amplia gama de opciones entre varios proveedores de servicios en la nube que ofrecen servicios relativamente similares, lo que les otorga cierto poder para negociar precios, condiciones y características de los servicios contratados. Además, aunque existe un coste asociado al cambio de proveedor o “switching costs”, este ha disminuido con la adopción de estándares abiertos y el desarrollo de herramientas que facilitan la migración de datos y aplicaciones entre diferentes plataformas en la nube. No existe por ello el bloqueo o “lock-in” de una empresa a un servicio o proveedor de servicios en la nube concreto.

Poder de negociación de los proveedores

Es moderado. Generalmente los proveedores de Hardware, Software u otros servicios de interés en el sector pueden tener un poder negociador significativo, aunque este puede verse reducido por las estrategias llevadas a cabo por las empresas para mantener el control sobre sus operaciones y costos.

Proveedores Hardware: Fabricantes de servidores, dispositivos de almacenamiento, componentes de red… La compra al por mayor de hardware es la opción elegida por los grandes proveedores de servicios cloud como AWS, ya que les permite negociar precios más bajos y condiciones favorables.

Proveedores Software: Plataformas de gestión de datos, Sistemas Operativos, soluciones de ciberseguridad… Poseen un poder negociador mayor para los casos en los que son productos esenciales y no tienen sustitutivos cercanos. Para reducir esta dependencia los proveedores cloud tienden a desarrollar sus propias soluciones o diversificar sus fuentes.

La electricidad es un recurso muy importante y altamente demandado por los proveedores cloud, por ello los proveedores de energía pueden tener un poder significativo sobre estos. Los CSP ubican por este motivo sus centros de datos en zonas con precios de electricidad más bajos e invierten en energías renovables para reducir este consumo energético.

Otro proveedor con poder negociador sobre los CSP son las empresas de telecomunicaciones que les brindan conexiones a Internet, ya que todo proveedor de servicios cloud depende de una conexión a Internet rápida y confiable. Una estrategia usada por proveedores cloud es la de crear redundancia en múltiples redes para reducir la dependencia de un solo proveedor de Internet.

Amenaza de productos o servicios sustitutivos

La existencia de las soluciones on-premise[23] representa una amenaza moderada-baja en el sector, ya que estas opciones tienden a ser menos flexibles y conllevan altos costes iniciales de capital y continuos de mantenimiento en comparación con las soluciones ofrecidas por los proveedores de servicios en la nube, aunque les proporcionen un control total sobre sus datos y sistemas. Una alternativa sería la nube híbrida, aunque no se trata de un sustitutivo directo.

Otra opción sería el servicio de Hosting tradicional, se contrata un servicio de alojamiento en un servidor físico o virtual. Reducen costes de hardware y mantenimiento, pero no poseen la flexibilidad ni escalabilidad de la computación en la nube.

Las tecnologías emergentes como Edge Computing o IoT representan más un complemento a la computación en la nube que un producto o servicio sustitutivo, aunque su evolución podría cambiar este panorama.

En definitiva, aunque existen productos y servicios sustitutivos a la computación en la nube ninguno proporciona la flexibilidad, escalabilidad, variedad de servicios, innovación y reducción de costos que la nube ofrece.

Amenaza de entrada de nuevos competidores

Es moderada-alta debido a la elevada escalabilidad de la computación en la nube que permite a nuevos competidores crecer rápidamente. No obstante, estos nuevos competidores han de enfrentarse a grandes empresas del sector en términos de escala, infraestructura, experiencia y confianza del cliente. Además, los costos de capital iniciales actúan como factor disuasorio de acceso al sector.

Rivalidad entre competidores existentes

La competencia entre proveedores de la nube es alta e intensa. Compiten tanto a nivel de precios, funcionalidades, rendimiento, seguridad, innovación, lealtad de clientes o nichos de mercado. Esta rivalidad puede verse apaciguada en cierta medida gracias a las colaboraciones entre proveedores o al alto crecimiento del mercado, que ofrece oportunidades a todos los competidores. Por ello, los proveedores han de mantenerse ágiles e invertir en innovación para tratar de asegurar su posicionamiento en el sector.

En resumen, este análisis indica que el sector es altamente competitivo, con un moderado grado de poder por parte tanto de los clientes como proveedores, una amenaza de productos sustitutivos moderada-baja y una alta e intensa rivalidad entre los competidores existentes.

Tendencias

El futuro del sector de la computación en la nube trae consigo infinitas oportunidades de crecimiento e innovación. Entre las tendencias actuales del sector cloud se encuentran algunas de las comentadas con anterioridad, como la migración a la Nube Híbrida y la Multinube.

[23] La organización se encarga de mantener sus propios servidores y hardware (infraestructura de TI interna)

Otras de las tendencias más destacadas para este 2024 son:

Big Data

Se refiere al conjunto de datos masivos y complejos que son difíciles de procesar con las herramientas tradicionales. Esos datos se caracterizan por su variedad, velocidad y volumen. Debido a esto se espera que el mercado del Big Data en la nube siga creciendo exponencialmente.

IA Generativa

La Inteligencia Artificial, y especialmente la IA Generativa, posee un enorme potencial para transformar diversos sectores y generar nuevas oportunidades. Se trata de una IA para crear contenido (texto, imágenes, vídeos…) que permite incrementar la productividad de los clientes, crear experiencias diferenciadas, generar ideas, automatizar procesos, optimizar operaciones, analizar datos o tomar decisiones de forma cada vez más eficiente, entre otras aplicaciones.

La infraestructura de la nube le permite estar disponible de forma masiva y asequible para empresas de todos los tamaños.

El Magic Quadrant o Cuadrante Mágico de Gartner (2024) reconoce a Microsoft como líder en servicios de desarrollador de IA en la nube. Más del 65% de las empresas que figuran en la lista Fortune 500[24] ya utilizan Azure OpenAI Service, y decenas de miles de otras organizaciones de diferentes sectores y de distintas partes del mundo están innovando con Azure AI.

Ilustración 13. Magic Quadrant 2024 for Cloud AI Developer Services. Fuente: Gartner

[24] Lista de la revista Fortune que presenta el ranking anual de las 500 empresas más grandes de EEUU según sus ingresos

Edge Computing

Es español Computación Perimetral, es clave para solucionar las situaciones donde la latencia es un tema crítico. Actualmente está ganando terreno, llevando la computación y el almacenamiento de datos más cerca de los dispositivos y usuarios finales, permitiendo procesar datos más cerca de donde se generan, así como mejorando la velocidad y la eficiencia en aplicaciones críticas para el tiempo de respuesta. Para ello emplea dispositivos Edge o de borde que pueden ser routers, gateways, u otros dispositivos inteligentes. Esto reduce la latencia y mejora el rendimiento para aplicaciones como IoT[25], vehículos autónomos y realidad aumentada.

Al contrario del modelo tradicional de computación en la nube, donde toda la información sale de los dispositivos finales para transitar por internet hasta los centros de datos centralizados y remotos, el modelo Edge presenta varias capas intermedias donde se descentraliza ese poder de cómputo.

Sin embargo, como ya hemos visto, el Cloud Computing posee numerosas ventajas, es escalable, costo-eficiente y accesible a nivel global.

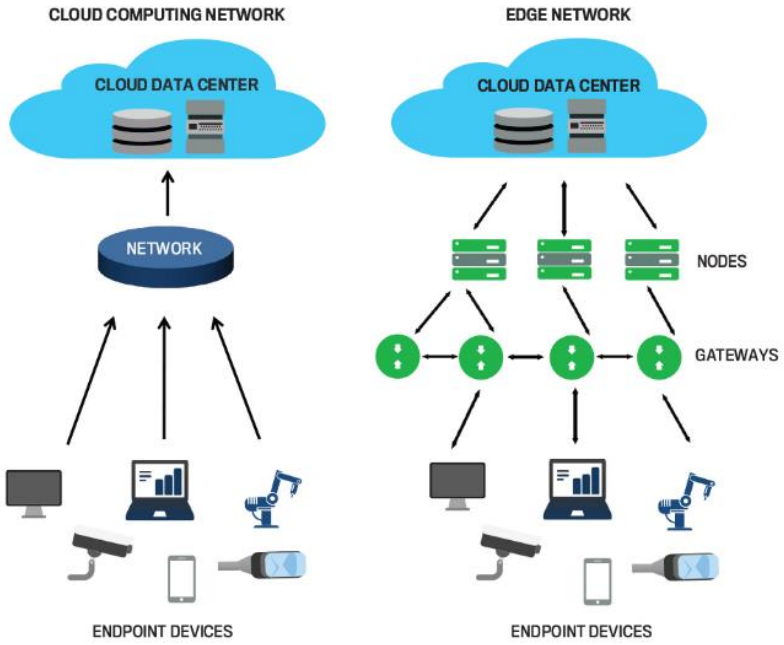

Ilustración 14. Computación en la Nube vs Computación Perimetral. Fuente: SFMagazine

Seguridad y resiliencia en la nube

Las empresas se preocupan cada vez más por la seguridad y el cumplimiento normativo a medida que más datos sensibles se trasladan a la nube, al mismo tiempo que aumenta el número de ciberataques. Por ello, los proveedores de servicios en la nube están invirtiendo en tecnologías y soluciones de seguridad avanzadas para garantizar la protección de los datos y el cumplimiento normativo.

Además, la resiliencia en la nube es clave para garantizar que las empresas puedan recuperarse eficazmente seguir funcionando ante desastres o fallos inesperados.

[25] Internet of Things o Internet de las Cosas

Algunas tendencias relacionadas con la ciberseguridad son: la arquitectura Zero Trust (Confianza Cero)[26], SASE[27] o el uso de ML[28] para la toma de decisiones basadas en conclusiones anteriores.

Cultura FinOps

Es el acrónimo de Finanzas y DevOps[29]. Esta cultura se basa en la colaboración entre los equipos de finanzas y los equipos de TI para optimizar el uso de la nube tomando decisiones informadas y basadas en datos, maximizando así su valor comercial y minimizando costes.

IDC predice que el 70% de las 1000 empresas globales cloud[30] aumentarán la madurez de FinOps a finales de 2024.

[26] Estrategia de seguridad en la que se asume que no se puede confiar en ningún usuario ni software
[27] Secure Access Service Edge, marco de seguridad que fusiona servicios de red con servicios de seguridad y permite adoptar un sistema de seguridad basado en la nube
[28] Matching Learning o Aprendizaje Automático. Rama de la IA que permite a las máquinas aprender y mejorar su rendimiento sin ser programadas explícitamente
[29] Development and Operations, Desarrollo de Software y Operaciones TI
[30] Lista de las empresas más grandes del mundo según diferentes criterios, consideradas líderes en sus respectivos sectores

Capítulo 4. Estudio de caso: Amazon Web Services (AWS)

Aparición

La empresa Amazon comenzó a utilizar la computación en la nube para mejorar su propia infraestructura interna a principios de la década de los 2000, y fue en 2006 cuando decidió lanzar AWS, su división de computación en la nube, compartiendo así los beneficios de la nube con otras empresas. AWS fue un gran éxito y destaca por ser el proveedor líder de ese sector en el mundo.

Antes de AWS, la computación en la nube era costosa y compleja, solo accesible para grandes empresas con recursos para invertir en su propia infraestructura. Tras su llegada, cualquier empresa sin importar su tamaño o presupuesto puede tener acceso a la nube. Es por esto por lo que ha sido reconocida por "democratizar la nube", es decir, por impulsar que los servicios en la nube sean accesibles y factibles para una amplia gama de empresas y usuarios.

Crecimiento

En sus inicios, AWS proporcionaba servicios principalmente enfocados en IaaS como su infraestructura de cómputo en la nube, Amazon Elastic Compute Cloud (EC2), el almacenamiento en la nube, conocido como Amazon Simple Storage Service (S3), y el almacenamiento persistente para las instancias EC2, Amazon Elastic Block Store (EBS).

Con el tiempo, fue creciendo exponencialmente, ampliando y diversificando su oferta de soluciones y servicios en la nube a más de 200, que abarcan tanto IaaS, PaaS y SaaS.

En cuanto a clientes, también experimentó un crecimiento exponencial desde su lanzamiento. En concreto, se vio impulsado por su adopción por parte de empresas líderes, clientes gubernamentales y del sector público, y diversos segmentos de clientes que van desde startups hasta grandes empresas.

Aunque no se puede saber con certeza el número de clientes de AWS, al no divulgar la empresa dicha información, los siguientes datos son orientativos. Según un estudio de Gartner, se estima que en la actualidad AWS posee más de 100 millones de clientes activos en todo el mundo.

AWS cuenta actualmente con más de 130 mil socios de diferentes países y más del 75% de las empresas que cotizan en el IBEX 35 utilizan su tecnología en la nube.

Regiones

Para AWS una *región* engloba una ubicación física en el mundo donde agrupa varios centros de datos, y a cada grupo de centros de datos lógicos la denomina *zona de disponibilidad*. Esta compañía se caracteriza por poseer un diseño de múltiples zonas de disponibilidad por cada región, lo cual ofrece numerosas ventajas a los clientes como mayor tolerancia a fallos, ya que dichas zonas se encuentran aisladas y físicamente separadas entre sí de modo que, si una experimenta una interrupción, las otras en la misma región no se verán afectadas. AWS consigue de este modo una mayor disponibilidad, rendimiento y seguridad.

La empresa mantiene las regiones de América del Norte, América del Sur, Europa, China, Asia-Pacífico, Sudáfrica y Medio Oriente. En concreto, posee presencia en 245 países y territorios, y dispone de infraestructura cloud en 33 regiones lanzadas cada una con varias zonas de disponibilidad, formando un total de 105 en todo el mundo.

Además, posee más de 600 puntos de presencia (POP[31]) de CloudFront y 13 cachés periféricas regionales. Lo que quiere decir que su red de entrega de contenido (CDN[32]), que utiliza para distribuir contenido de forma rápida y segura a los usuarios de todo el mundo, emplea POP o servidores que se encuentran en ubicaciones estratégicas en todo el mundo. De este modo, puede almacenar contenido en caché cerca de los usuarios y reducir así la latencia y mejorar el rendimiento.

En resumen, AWS ha experimentado un crecimiento significativo debido a su amplia gama de servicios, su escalabilidad y confiabilidad, su tolerancia a fallos, sus precios competitivos, su facilidad de uso y su comunidad activa.

Amazon CloudFront en Europa

El servicio de red de entrega de contenido de AWS ha experimentado una significativa expansión y crecimiento. En concreto centrándonos en Europa, como se puede ver en el mapa de la ilustración siguiente, AWS ha ampliado su presencia por medio de infraestructuras y centros de datos en numerosas ubicaciones europeas, mejorando así la latencia y rendimiento en dichas áreas.

CloudFront se encuentra presente en las principales ciudades europeas como Londres, Berlín, París y Madrid, entre otros, mejorando así la experiencia de los usuarios con su alta disponibilidad y rendimiento óptimo. AWS CloudFront muestra así su compromiso por el soporte a sus clientes.

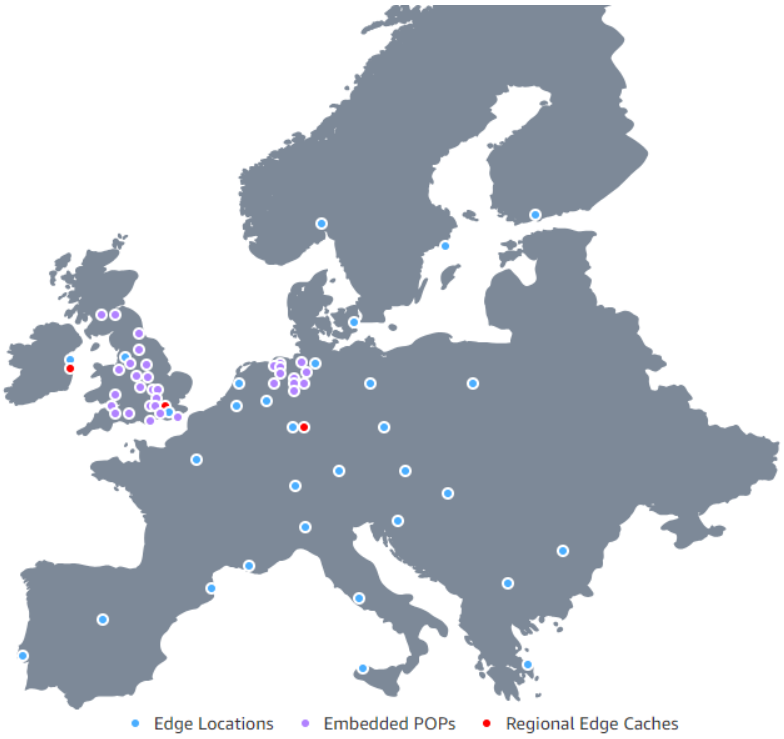

Ilustración 15. Amazon CloudFront en Europa. Fuente: AWS

[31] Points Of Presence
[32] Content Delivery Network

AWS en España

La inversión de AWS en España para el periodo 2024 a 2033, según un informe de AWS, será de 16.900 millones de dólares estadounidenses (15.700 millones de euros). La estimación de la contribución prevista de la región española de AWS al Producto Interior Bruto (PIB) en España será de unos 21.600 millones de euros, de los cuales, 12.900 millones de euros en Aragón. Además, estiman que formarán más de 17.500 puestos de trabajo, de los que 6.800 serán en Aragón.

La empresa trabaja con variedad de organizaciones en España de diferentes tamaños e incluso con agencias gubernamentales y empresas públicas, tales como BBVA, Telefónica, Cepsa, Glovo, Renfe o el Ayuntamiento de Madrid, entre otras.

AWS en Aragón

AWS ha establecido su presencia en Aragón, España, en noviembre de 2022. Se trata de la octava región de infraestructura conformada en Europa, compuesta por tres zonas de disponibilidad en Zaragoza.

La presencia de AWS en Aragón no solo mejora la capacidad tecnológica de la región, sino que también promueve el crecimiento económico y la innovación local, al tiempo que apoya la sostenibilidad y el cumplimiento regulatorio. Esta inversión estratégica subraya el compromiso de AWS con el desarrollo y el éxito de sus clientes en España y en toda Europa. Además, la empresa ofrece una variedad de certificados y programas de formación para capacitar a nuevo personal.

Análisis DAFO

Se trata de un análisis que permite identificar las Debilidades, Amenazas, Fortalezas y Oportunidades de un negocio o proyecto específico para ayudarle a realizar planes estratégicos y mantenerse a la vanguardia de las tendencias del sector.

En este caso, se realiza el análisis DAFO de AWS:

Debilidades

Amazon Web Services depende en cierta medida de proveedores externos para componentes de hardware y otras infraestructuras, lo que puede afectar su cadena de suministro y costos operativos relacionados con la subida de precios de hardware o la escasez de componentes.

Otra debilidad de AWS es su estructura de precios. Al disponer de una alta variedad de servicios y distintas opciones de configuración, los clientes pueden tener dificultades a la hora de prever el coste de su facturación. Es por ello, que AWS ofrece herramientas como AWS Cost Explorer para que las empresas controlen sus gatos, aunque para su uso se requiere un aprendizaje previo.

Aunque la empresa es conocida por su robustez y su continua innovación e inversión en seguridad, es un objetivo de ciberataques debido a su influencia en el mercado global, lo cual podría dañar su reputación y erosionar la confianza de sus clientes.

Amenazas

Los fuertes competidores del sector, Microsoft Azure y Google Cloud Platform, suponen una amenaza a la empresa. Ambas empresas invierten en su infraestructura continuamente e intentan atraer a los mismos clientes que AWS. Las tres compiten tanto a nivel de precios, servicios e innovación en el sector.

Cambios en las regulaciones gubernamentales de diferentes países en torno a la privacidad de los datos, la ciberseguridad y otros aspectos pueden suponer una amenaza y afectar la operación de AWS, así como generar preocupaciones de cumplimiento para sus clientes.

Fortalezas

La empresa ofrece una amplia variedad de servicios en la nube que abarcan desde cómputo, almacenamiento, análisis, seguridad, inteligencia artificial y más. Esta amplia gama de servicios permite a los clientes encontrar soluciones a medida para suplir sus necesidades específicas. Sin olvidar la capacidad de escalabilidad y flexibilidad que ofrece a los clientes para escalar sus recursos de manera rápida y eficiente según las demandas de sus aplicaciones y cargas de trabajo.

Cabe destacar también su robusta infraestructura alrededor del mundo, lo cual asegura que sus servicios estén disponibles globalmente. Además, dicha infraestructura es diseñada para ser resiliente a fallos, haciéndola muy fiable para empresas que dependen de AWS para operaciones críticas.

Esto le ha llevado a disponer de una posición dominante en el sector cloud que le otorga una ventaja competitiva y le permite influir en las tendencias del mercado. Así como, la continua expansión de su infraestructura refuerza su compromiso para atender a un mercado global en constante crecimiento.

Oportunidades

AWS expande su presencia internacional, abriendo nuevas regiones y centros de datos en todo el mundo, para satisfacer la creciente demanda de servicios en la nube y para establecer su fuerte presencia en mercados emergentes.

También la adopción y desarrollo de nuevas tecnologías, como la inteligencia artificial o el aprendizaje automático, suponen una gran oportunidad para AWS atrayendo consigo nuevos clientes.

En resumen, AWS posee grandes fortalezas, pero también enfrenta desafíos y amenazas. Identificar y abordar estas debilidades, amenazas, fortalezas y oportunidades es fundamental para mantener y fortalecer su posición como el proveedor líder de servicios en la nube.

Capítulo 5. Seguridad en la nube

La seguridad en entornos de computación en la nube es un campo dinámico que evoluciona continuamente. Debido a la amplia aceptación de la computación en la nube, sus opciones de implementación populares y su diseño personalizado, ha sido necesario agregar y ajustar muchos parámetros ya establecidos en la disciplina de la seguridad informática.

En este campo podemos encontrar amenazas tradicionales como ataques de denegación de servicios distribuidos (DDoS) o brechas de datos, así como nuevos desafíos tal que los ataques a las interfaces y APIs como puntos de entrada al sistema y la falta de supervisión de los recursos en la nube.

Para mitigar dichas amenazas se emplean diversas tecnologías como el cifrado, firewalls de protección, estrategias de Confianza Cero (Zero Trust), sistemas de gestión de accesos e identidades (IAM), sistemas de prevención y detección de intrusos (IDPS), entre otras.

En este capítulo se explorarán las normativas vigentes relacionadas con la seguridad en la nube, y posteriormente, se comparará la seguridad informática tradicional frente a las nuevas exigencias de seguridad en entornos cloud. Se abordará el impacto del Reglamento General de Protección de Datos (RGPD) europeo en la protección de datos en la nube, se presentarán diversas estrategias de seguridad específicas para entornos de computación en la nube y se analizarán una serie de noticas actuales relativas a este campo.

Marco Legal

Las normativas, leyes y estándares de seguridad vigentes tienen como objetivo proteger la integridad, confidencialidad y disponibilidad de los datos y servicios en entornos de computación en la nube. Algunos de los más relevantes son:

Reglamento General de Protección de Datos (RGPD)

Se aplica a toda empresa que procese datos de ciudadanos de la Unión Europea (UE), independientemente de su ubicación geográfica. Estableciendo requisitos para garantizar la seguridad de los datos de carácter personal de ciudadanos de la UE. Entró en vigor en mayo de 2016.

Ley Orgánica de Protección de Datos de Carácter Personal y Garantía de los Derechos Digitales (LOPD-GDD)

Se trata de la ley española aprobada tras derogar en 2018 la Ley Orgánica de Protección de Datos (LOPD) de 1999. Esta nueva LOPD se centra en la protección de datos de carácter personal de forma alineada y acorde al comercio electrónico, la computación en la nube y la digitalización en general que vivimos hoy en día.

ISO[33] 27017:2015

Se trata de un código de buenas prácticas que proporciona directrices específicas para los controles de seguridad aplicables a los servicios en la nube. Este estándar se basa en el ISO 27001 y 27002, y ofrece controles adicionales para la implementación y administración de la seguridad de la información en la nube.

[33] Organización Internacional de Normalización, o en inglés, International Organization for Standardization

ISO 27018:2019

Conjunto de buenas prácticas que se centra en la protección de datos personales en la nube. Este estándar establece controles de privacidad y seguridad para los proveedores de servicios en la nube que manejan datos de identificación personal (PII).

Ley de Privacidad del Consumidor de California (CCPA[34])

Esta ley de privacidad de alcance estatal entró en vigor en 2020, siendo la ley de protección de datos más completa de los EE. UU. hasta la fecha marcando así un precedente en el país. Regula cómo las organizaciones gestionan los datos personales de los residentes en California.

FedRAMP[35]

Se trata de un programa que evalúa y asegura la autorización de servicios en la nube utilizados por agencias federales, es decir, asegura que cumplan con los requisitos de seguridad del gobierno federal de los Estados Unidos. Se basa en el estándar de la publicación especial 800-53 rev. 4 del Instituto Nacional de Estándares y Tecnología de EE. UU. (NIST).

NIST SP800-144

Documento publicado por el NIST que proporciona directrices para la seguridad en la nube. Aborda los riesgos específicos de la nube, y describe directrices y recomendaciones prácticas para organizaciones que buscan implementar o mejorar sus prácticas de seguridad y privacidad en este entorno. Este marco es ampliamente respetado y referenciado en el ámbito de la ciberseguridad.

COBIT 5

Control Objectives for Information and Related Technologies (COBIT). Marco de gobierno y gestión de TI desarrollado por ISACA[36]. Proporciona orientación para definir las funciones, responsabilidades y controles necesarios para garantizar la adopción segura de la nube al tiempo que se cumplen los objetivos empresariales.

AWS Well-Architected Framework

Conjunto de prácticas para diseñar infraestructuras seguras, resilientes, eficientes y optimizadas en Amazon Web Services (AWS). Abarca cinco pilares para evaluar y mejorar las arquitecturas en la nube, esots son: excelencia operativa, seguridad, fiabilidad, eficiencia del rendimiento y optimización de costes. Siguiendo este marco, las organizaciones pueden garantizar que sus arquitecturas de nube se ejecuten de manera óptima y cumplan con los requisitos comerciales y técnicos.

CSA STAR

Security, Trust & Assurance Registry, se trata de un programa de certificación de seguridad en la nube gestionado por la Cloud Security Alliance (CSA). Proporciona un marco completo para evaluar y comparar la seguridad de los CSP de cara a que las organizaciones tomen decisiones informadas.

Cloud Controls Matrix (CCM)

La Matriz de Controles en la Nube de Cloud Security Alliance (CSA) es una herramienta de seguridad para evaluar la seguridad de los servicios en la nube. Incluye controles mapeados a estándares o regulaciones y buenas prácticas que sirven como referencia para evaluar la seguridad de los proveedores de servicios en nube.

[34] California Consumer Privacy Act
[35] Federal Risk and Authorization Management Program
[36] Information Systems Audit and Control Association. Asociación internacional que da apoyo a metodologías y certificaciones para actividades de auditoría y control en sistemas de información

CSA Security Guidance

Guía de seguridad proporcionada por CSA que ofrece recomendaciones y buenas prácticas para proteger los entornos en la nube. La guía cubre una amplia gama áreas, desde la gobernanza y el cumplimiento hasta la gestión de identidades y accesos, entre otras. Es un recurso valioso para organizaciones ya que les ayuda a construir una base sólida de seguridad en la nube.

CIS Controls

El Centro para la Seguridad en Internet (CIS) proporciona controles de ciberseguridad con el objetivo de proteger los entornos en la nube. Se centra en acciones de seguridad críticas que las organizaciones deben implementar para proteger sus recursos en la nube. Estos controles cubren áreas como la gestión protección de datos, de accesos o la gestión de vulnerabilidades.

Estas normativas y marcos regulatorios brindan una guía clara sobre cómo proteger los datos y los servicios en la nube de diversas amenazas y vulnerabilidades, permitiendo establecer un entorno seguro y confiable para la computación en la nube.

Seguridad informática vs seguridad en la nube

La seguridad informática tradicional y la seguridad en la nube tienen como objetivo proteger los datos y sistemas ante amenazas y ciberataques. La principal diferencia entre ambas es la ubicación de los datos y recursos. En la seguridad informática tradicional estos se almacenan y administran en centros de datos locales dentro del perímetro de red de la organización, mientras que cuando se emplea la nube estos se encuentran almacenados en los centros de datos de los CSP.

Esto quiere decir que, ante cualquier ataque o amenaza, en el caso de la seguridad informática tradicional el responsable de la protección de los datos y recursos, así como de la seguridad de la infraestructura cloud, es la organización. Frente al caso de la seguridad en la nube, en el cual el CSP posee la responsabilidad de proteger la infraestructura física y la capa de virtualización ante ataques, pero el cliente u organización que contrata el servicio posee la responsabilidad de asegurar la seguridad de sus datos y recursos, es decir, de todos sus activos ubicados en la nube. A esto se le denomina Modelo de Responsabilidad Compartida entre el proveedor de la nube y el cliente.

Por ejemplo, el CSP se encarga de facilitar y proveer accesos seguros a los dispositivos de almacenamiento y redes, así como de saber responder ante desastres. Mientras que el cliente es el responsable de configurar los servicios que controlen los accesos, gestión de logs[37], etc.

El cliente tendrá la responsabilidad en los modelos IaaS, SaaS y PaaS de asegurar y gestionar la seguridad de sus datos, aplicaciones y APIs, y si se trata de un modelo IaaS deberá también hacerse cargo del sistema operativo y máquinas virtuales. El CSP es responsable de los servidores, el almacenamiento, las redes e instalaciones, así como, para el modelo PaaS, de gestionar la seguridad en las aplicaciones instaladas.

[37] Gestión de inicios de sesión en el sistema

Responsabilidad compartida en AWS

Por parte del CSP, en este caso AWS, se requiere que se encargue de la disponibilidad del servicio, mantenimiento de la base de datos, la protección y respuesta ante ataques externos a la infraestructura y a los servicios en la nube, así como la configuración y seguridad de la red.

Por parte del cliente se espera que proteja la cuenta AWS, lleve un control y registro de los usuarios y sus permisos incluyendo el control de accesos, realice una configuración correcta de los servicios de AWS y actualice los sistemas.

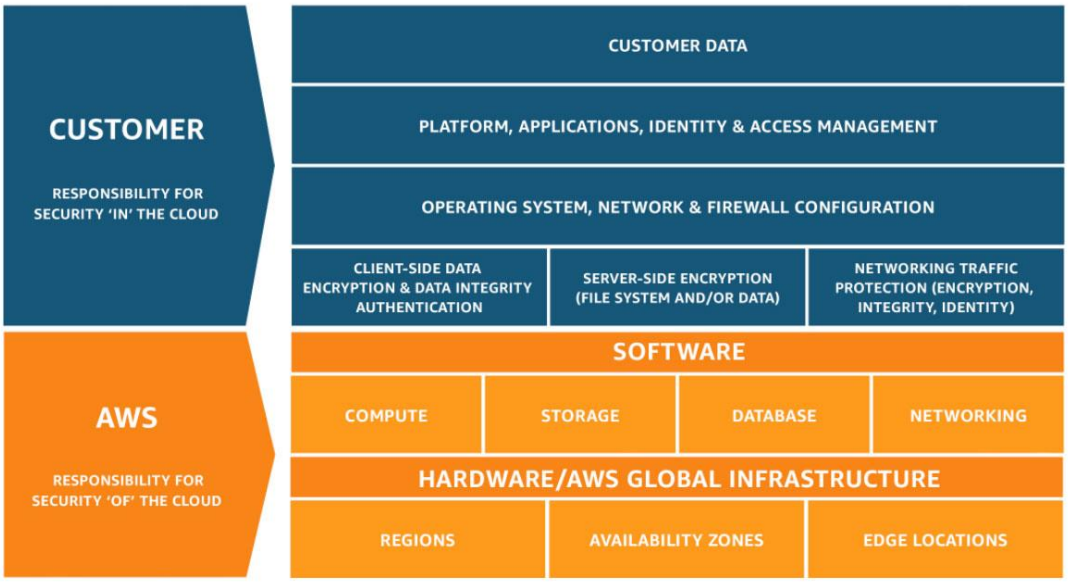

Ilustración 16. Modelo de responsabilidad compartida. Fuente: AWS

Escenario

Una organización almacena su sitio web de comercio electrónico en la nube. Un atacante lanza un ataque DDoS contra el sitio web, con el objetivo de inundarlo con tráfico falso y hacerlo inaccesible para los clientes legítimos.

Responsabilidad del CSP:

- ✓ Proporcionar protección contra DDoS a nivel de infraestructura: El CSP debe tener implementadas medidas de seguridad para mitigar ataques DDoS a gran escala, como firewalls de red, sistemas de detección de intrusiones y servicios de balanceo de carga.
- ✓ Aislar a cada cliente: El CSP debe garantizar el aislamiento de cada cliente por medio de la segmentación lógica de la red.
- ✓ Mantener la infraestructura de la nube segura: El CSP debe aplicar parches de seguridad y actualizaciones de software de manera regular para corregir vulnerabilidades que podrían ser explotadas por los atacantes.

Responsabilidad del cliente:

- ✓ Proteger las aplicaciones y los datos: El cliente debe implementar medidas de seguridad para proteger sus aplicaciones y datos que se ejecutan en la nube, como firewalls de aplicaciones web, sistemas de detección de intrusos y controles de acceso (cifrados).
- ✓ Configurar correctamente la seguridad en la nube: El cliente debe configurar correctamente las opciones de seguridad de la nube, como las reglas de firewall y las listas de control de acceso, para restringir el acceso a sus recursos.
- ✓ Monitorizar la seguridad de las aplicaciones y los datos: El cliente debe monitorizar de forma continua la seguridad de sus aplicaciones y datos en la nube para detectar y responder ante posibles amenazas.

En cualquier caso, la colaboración entre el CSP y el cliente es esencial para mantener un entorno de nube seguro.

Impacto del RGPD en la nube

El Reglamento General de Protección de Datos de la Unión Europea se aplica desde el 25 de mayo de 2018. Este garantiza la privacidad de los datos personales en la nube, y para ello impone una serie de requisitos. Estos requisitos afectan tanto a los CSP como a los clientes que utilizan estos servicios.

Además, este reglamento pretende unificar todas las leyes actuales que afectan a la privacidad que tenían el resto de los países. En general, actualiza las normas sobre cómo se tiene que usar la información personal digital de los usuarios.

Algunos principios fundamentales del RGPD son la licitud, la integridad, la confidencialidad, la lealtad y la transparencia, la limitación de la finalidad y la limitación del plazo de conservación.

Algunos de los principales requerimientos de este reglamento que afectan a los CSP:

- El CSP debe adoptar medidas de seguridad suficientes para proteger los datos personales contra el acceso no autorizado, la alteración, la divulgación o la destrucción accidental o ilícita. Esto incluye medidas físicas, técnicas y organizativas, como controles de acceso, cifrado, auditoría y registro de actividades.
- Se deberá nombrar un Delegado de Protección de Datos (DPO) si se procesan datos personales a gran escala o si la actividad de dicho tratamiento implican riesgos elevados para los derechos de las personas físicas. El DPO actuará como punto de contacto con las autoridades y los interesados del tratamiento de sus datos cuando ocurra cualquier violación que implique un riesgo sobre los datos personales, en menos de 72 horas tras haber ocurrido.
- El CSP deberá facilitar el ejercicio de los derechos de los interesados, como el acceso, el borrado, la rectificación, la limitación u oposición al tratamiento.

Requerimientos sobre el cliente:

- El cliente debe asegurarse de que el CSP en el que contrata los servicios cumple lo establecido en el RGPD.
- El cliente debe adquirir el consentimiento de toda aquella persona interesada para realizar el tratamiento de sus datos personales.

– EL contrato entre el CSP y el cliente deberá contener los requerimientos necesarios para asegurar el correcto tratamiento de los datos personales. Entre estos aspectos se encontraría el derecho o no a la transferencia de estos datos a terceros, la finalidad del tratamiento, las medidas de seguridad a emplear, etc.

El RGPD ha tenido un impacto significativo en la gestión de datos en la nube, estableciendo normas estrictas para proteger la privacidad de los usuarios en la Unión Europea. Las empresas que manejan grandes volúmenes de datos deben asegurarse de cumplir con estas regulaciones para evitar sanciones severas.

Un ejemplo reciente de la aplicación rigurosa del RGPD es la imposición de multas a gigantes tecnológicos como Meta, Google y Amazon por un total de 3.440 millones de euros por infringir el RGPD. Siendo Meta la más sancionada con 2.545 millones de euros.

Como se puede apreciar, el cumplimiento del RGPD en el sector de la computación en la nube es un compromiso compartido entre el CSP y el cliente. La colaboración entre ambos es imprescindible para poder garantizar el control y la gestión adecuada de la seguridad en la nube, con todo lo que ello implica. Las empresas, sin importar su tamaño, que manejan datos deben asegurarse de cumplir con estas regulaciones para evitar sanciones severas y no perder la confianza de sus clientes.

Estrategias de seguridad

Algunas de las estrategias clave para reforzar la seguridad en la nube son:

Cifrado de datos

Lo que se conoce como cifrado en tránsito y en reposo, ya que se trata de cifrar los datos tanto en su transferencia como en su almacenamiento en la nube.

Google Cloud, por ejemplo, realiza ambos cifrados para garantizar que solo las personas autorizadas tengan acceso a los datos por medio de las claves encriptadas. Para la encriptación en tránsito, los datos se encriptan antes de ser enviados, los extremos de la comunicación se autentican, y los datos se desencriptan y verifican al llegar al receptor de la comunicación. De la encriptación en reposo se encarga Cloud Storage.

Además, Google emplea una tercera encriptación llamada Encriptación en Uso para encriptar los datos que se encuentran en un momento dado en uso por algún servidor, para ello emplea Confidential VMs y Confidential Google Kubernetes Engine Nodes.

Seguridad perimetral

Se trata de un modelo de seguridad de red en el que ningún usuario que se encuentre fuera de la red puede acceder a los datos que se encuentren en el interior de esa red. Una vez que un usuario se conecta a la red, puede acceder a todas las aplicaciones y datos de esta.

Las organizaciones que utilizan este modelo invierten importantes recursos en defender el perímetro de su red, y para ello implementan firewalls, gateways, sistemas de detección de intrusos (IDS) o sistemas de prevención de intrusos (IPS), entre otros.

Sistemas de Gestión de Accesos e Identidades (IAM[38])

Sistemas encargados de la gestión de las identidades[39] y accesos de los usuarios a los recursos del CSP. Para ello, implementa políticas robustas de gestión de identidades en la nube y proporciona accesos a los recursos pertinentes, siempre en función de los derechos de cada identidad (quién puede acceder a qué recursos en la nube). Un ejemplo es AWS IAM.

Otra estrategia relacionada es la de Confianza Cero o Zero Trust en la que de manera predeterminada no se confía en ningún sistema o usuario. El proceso implica validar siempre las identidades de los usuarios y sus derechos de acceso a un sistema concreto, salvo que se determine lo contrario explícitamente.

En conclusión, adoptar la nube ofrece numerosas ventajas a las organizaciones, como la escalabilidad, la agilidad y la reducción de costes. Sin embargo, este entorno también presenta nuevos desafíos en materia de seguridad. Implementar estrategias robustas de seguridad en la nube es crucial para proteger los datos confidenciales, prevenir ciberataques y garantizar el cumplimiento de las regulaciones internacionales. Estas estrategias no solo logran proporcionar una mayor seguridad, sino que también aumentan la resiliencia, permiten formar un entorno seguro y confiable, mejorando de este modo la confianza en las soluciones en la nube.

Al ser un sector en constante evolución, se requieren constantes esfuerzos para asegurar un buen control y gestión de la seguridad, pero con las herramientas y prácticas de seguridad adecuadas, las organizaciones y CSP lograrán adelantarse a los actores maliciosos.

Actualidad

El informe anual de Cloud and Threat de Netskope Threat Labs (2024) afirma que más del 50% de las descargas de malware provenían de aplicaciones SaaS líderes, como Microsoft OneDrive. En la siguiente ilustración se desglosan algunas de las aplicaciones, con una comparación interanual, en las que los adversarios tienen más éxito a la hora de engañar a sus víctimas para que descarguen troyanos.

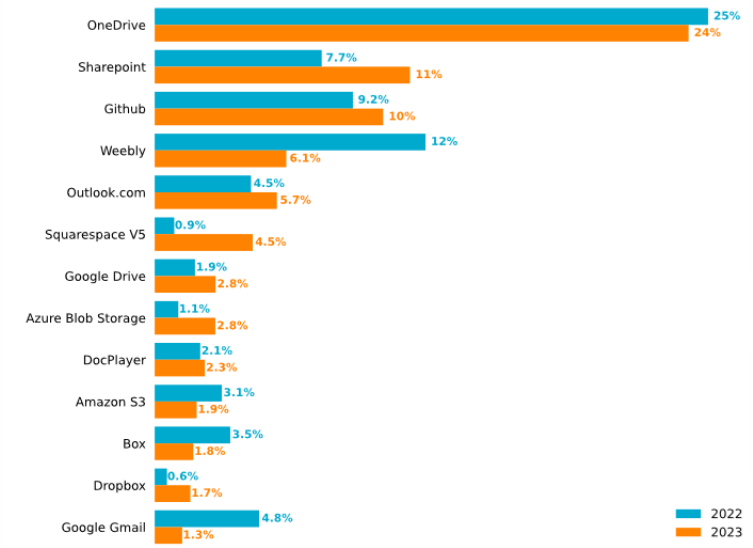

Ilustración 17. Porcentaje total de malware descargado. Fuente: Netskope

[38] Identity and Access Management

[39] La identidad, en el contexto informático, indica un conjunto de propiedades que se pueden medir y registrar digitalmente

Entre las aplicaciones en la nube y SaaS objetivo de los adversarios en las campañas de phishing en 2023, un ecosistema de aplicaciones destaca por encima de todos los demás: Microsoft. La popularidad de esta empresa entre los usuarios empresariales hace que sus credenciales sean un objetivo lucrativo para los atacantes.

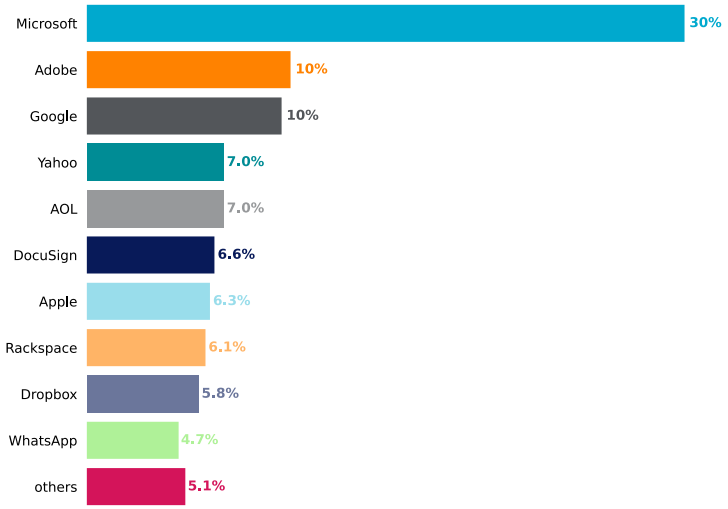

Ilustración 18. Top objetivos cloud de phishing. Fuente: Netskope

El informe además distingue entre dos tipos de ataques, geopolíticos y criminales. Entre los actores criminales más activos se encuentran grupos rusos, alrededor de un 70% de los ciberataques provienen de Rusia, mientras que los ataques geopolíticos son liderados por adversarios chinos. En Europa, como se puede apreciar en la ilustración siguiente, un 97% de los ciberataques fueron criminales frente a un 3.2% geopolíticos.

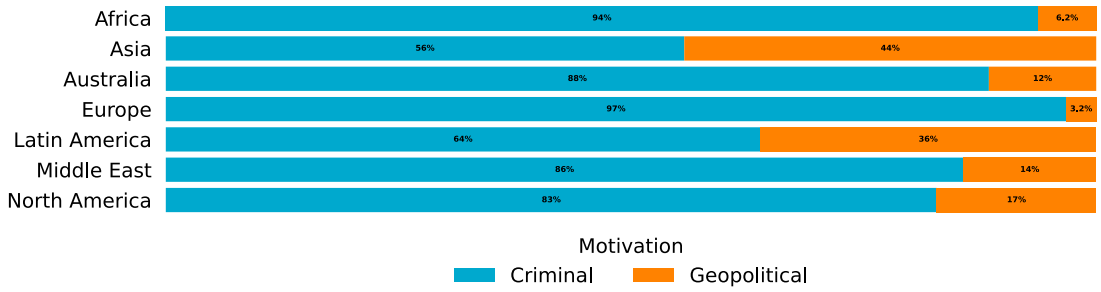

Ilustración 19. Motivación de ciberataques según la región. Fuente: Netskope

Esta información se vincula estrechamente con recientes incidentes de ciberseguridad, como por ejemplo el hackeo que sufrieron el Santander y Ticketmaster. Una noticia (2024) sobre el informe realizado tras el ciberataque describe cómo el robo de credenciales a un empleado de Snowflake habría permitido acceder a los datos de TicketMaster y el Santander. Snowflake por su parte asegura no haber sufrido ningún tipo de brecha de seguridad recientemente, sino que se debió a malas prácticas de las víctimas.

Estos incidentes subrayan la crucial importancia de implementar medidas robustas de ciberseguridad. La computación en la nube ofrece soluciones avanzadas, como monitoreo constante, actualizaciones automáticas y herramientas de mitigación de ataques. Sin embargo, la falta de precauciones adecuadas puede llevar a brechas de seguridad significativas, exponiendo datos sensibles y causando daños

reputacionales y financieros. Por tanto, es crucial adoptar prácticas de seguridad rigurosas para proteger la información en la nube y priorizar la adopción segura de aplicaciones y continuar invirtiendo en la reducción del riesgo de ingeniería social mediante la formación en seguridad y la implementación de tecnologías, como las tecnologías anti-phishing.

Capítulo 6. Conclusiones

A la vista de los objetivos planeados al inicio del estudio y los resultados obtenidos, puede concluirse que el sector de computación en la nube se ha convertido en un pilar fundamental de la economía digital global.

La computación en la nube ha cambiado la forma en que las empresas administran los recursos técnicos con características como escalabilidad, flexibilidad, pago por uso y autoservicio bajo demanda. La investigación teórica en este campo contribuye a esta transformación, permitiéndonos comprender diferentes modelos de servicios e implementaciones, así como tecnologías clave.

El análisis externo de la industria utilizando el análisis PESTEL y el modelo de las cinco fuerzas de Porter revela un entorno altamente dinámico y competitivo. Los factores políticos, económicos, sociales, tecnológicos, ambientales y legales son críticos para el desarrollo de la industria, mientras que las fuerzas competitivas como la amenaza de nuevos participantes y la competencia entre competidores existentes resaltan la necesidad de innovación continua y optimización de costos para sostener la industria.

El estudio de caso de Amazon Web Services (AWS) brinda información sobre cómo la empresa se está moviendo hacia el mercado a través de una estrategia de innovación continua, diversificación de servicios e infraestructura sólida. AWS ha demostrado cómo aprovechar las economías de escala y seguir siendo competitivo, pero también enfrenta desafíos, particularmente en materia de seguridad y cumplimiento normativo.

La seguridad en la nube sigue siendo una preocupación importante para los usuarios y proveedores de servicios. La protección de datos, la privacidad, la gestión de identidades y el cumplimiento normativo son áreas que requieren atención constante. Las estrategias de seguridad son fundamentales para reducir el riesgo y garantizar la confianza de los usuarios en los servicios en la nube.

En resumen, la industria de la computación en la nube se encuentra en una etapa de rápido desarrollo y crecimiento, y su importancia en la infraestructura tecnológica global está aumentando. AWS destaca como líder del mercado por su innovación y capacidad para brindar servicios potentes. Sin embargo, la seguridad y el cumplimiento seguirán siendo desafíos clave que los proveedores deben abordar para garantizar un crecimiento sostenible continuo y la confianza de los usuarios. Este estudio destaca la necesidad de una vigilancia constante y adaptación a los cambios tecnológicos y regulatorios para seguir siendo competitivos en esta industria dinámica.

En el transcurso de este estudio, se han identificado varias áreas donde se pueden realizar aportaciones significativas. En primer lugar, destacar la importancia de fomentar una cultura de innovación en el sector para que las organizaciones puedan mantenerse al día de las rápidas evoluciones tecnológicas. En segundo lugar, enfatizar la necesidad de fortalecer y adaptar continuamente las alianzas estratégicas entre proveedores de servicios en la nube y entidades regulatorias para asegurar un entorno seguro y conforme a las normativas.

Por otro lado, aunque ya existen programas de capacitación continua para profesionales de TI y marcos de evaluación para la seguridad y gestión de la nube, sería beneficioso mejorarlos y adaptarlos con un enfoque especifico en las últimas tendencias de seguridad y gestión de la nube de modo que sean más efectivos y respondan mejor a las necesidades dinámicas del sector. Con esto, se contribuiría significativamente a asegurar que se adapte la gestión de la nube a las necesidades cambiantes del mercado y las normativas vigentes.

Otro aspecto por incentivar es la colaboración entre la industria y las instituciones académicas para la investigación y el desarrollo de soluciones innovadoras en el ámbito de la computación en la nube, aun existiendo numerosas iniciativas hoy en día siempre hay espacio para mejorar y maximizar los beneficios no solo a los proveedores de servicios en la nube sino también a los usuarios de estos servicios.

Bibliografía

Alonso, M. (18 de Noviembre de 2022). *Asana*. Obtenido de https://asana.com/es/resources/porters-five-forces

Álvarez, D. (s.f.). Introducción al RGPD (ASLEPI). Escuela de Ingeniería Informática de Oviedo, Asturias, España.

Atlassian. (s.f.). Obtenido de https://www.atlassian.com/es/trust/compliance/resources/fedramp

AWS. (s.f.). Obtenido de https://aws.amazon.com/es/architecture/well-architected

AWS. (s.f.). Obtenido de https://aws.amazon.com/es/local/spain

AWS. (s.f.). Obtenido de https://aws.amazon.com/es/about-aws/global-infrastructure

AWS. (s.f.). Obtenido de https://aws.amazon.com/es/what-is/virtualization

AWS. (s.f.). Obtenido de https://aws.amazon.com/es/compliance/shared-responsibility-model

AWS. (s.f.). Obtenido de https://aws.amazon.com/es/what-is/iac

AWS. (s.f.). Obtenido de https://aws.amazon.com/es/what-is-cloud-computing

AWS. (2024). *Inversión de AWS en España.*

Bachiller, Trujillo, S., & Marcelino, P. (2020). *Estudio comparativo de plataformas Cloud Computing para arquitecturas SOA.* Pimentel, Perú.

Bécares, B. (3 de Febrero de 2021). *Genbeta*. Obtenido de https://www.genbeta.com/actualidad/amazon-web-services-esta-su-historia-asi-ha-ido-escribiendo-exito-andy-jassy-futuro-ceo-amazon

BOE. (5 de Diciembre de 2018). Obtenido de https://www.boe.es/buscar/pdf/2018/BOE-A-2018-16673-consolidado.pdf

Borra, P. (2024). Comparison and Analysis of Leading Cloud Service Providers (AWS, Azure and GCP). En *International Journal of Advanced Research in Engineering and Technology (IJARET)* (págs. 266-278). Boca Raton, USA: IAEME.

Chauhan, M., & Shiaeles, S. (2023). *An Analysis of Cloud Security Frameworks, Problems and Proposed Solutions.* Basel, Switzerland: Khaled Elleithy.

CIS. (s.f.). Obtenido de https://www.cisecurity.org/controls

Cisco. (s.f.). Obtenido de https://www.cisco.com/c/es_mx/solutions/software-defined-networking/overview.html

Cisco. (s.f.). Obtenido de https://www.cisco.com/c/en/us/about/case-studies-customer-success-stories/skanska.html

Cisco. (25 de Enero de 2023). Obtenido de https://www.cisco.com/c/es_mx/solutions/cloud/what-is-cloud-computing.html

CloudFlare. (s.f.). Obtenido de https://www.cloudflare.com/es-es/learning/access-management/castle-and-moat-network-security

Cotrino Benavides, Á. A. (2022). *Strategies to improve the industry 4.0.* UNED.

CSA. (s.f.). Obtenido de https://cloudsecurityalliance.org/research/guidance

CSA. (s.f.). Obtenido de https://cloudsecurityalliance.org/research/cloud-controls-matrix

CSA. (s.f.). Obtenido de https://cloudsecurityalliance.org/star

Delgado Martorell, S. (18 de Diciembre de 2023). *La Razón*. Obtenido de https://www.larazon.es/emergente/quien-domina-mercado-computacion-nube-mundo_20231218657febad29f31800017f70a9.html

Etherington, A. (2023). *Cloud Services (Managed and Professional) Forecast Update and Trends, Global.* Omdia.

EUR-Lex. (4 de Mayo de 2016). Obtenido de https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016R0679

Eurostat. (8 de Diciembre de 2023). Obtenido de https://ec.europa.eu/eurostat/web/products-eurostat-news/w/ddn-20231208-1

FedRAMP. (s.f.). Obtenido de https://www.fedramp.gov

GlobalData, T. I. (18 de Junio de 2020). *Verdict*. Obtenido de https://www.verdict.co.uk/cloud-computing-timeline/?cf-view

Google Cloud. (s.f.). Obtenido de https://cloud.google.com/learn/what-is-cloud-computing

Google Cloud. (s.f.). Obtenido de https://cloud.google.com/learn/what-are-containers

Google Cloud. (s.f.). Obtenido de https://cloud.google.com/learn/what-is-artificial-intelligence

Google Cloud. (s.f.). Obtenido de https://cloud.google.com/security/encryption

Grant, R. M. (2014). *Dirección estratégica: Conceptos, técnicas y aplicaciones.* Aranzadi.

Hasan, M. Z., Hussain, M. Z., Siddiqui, A., Mubarak, Z., & Qureshi, A. (2023). *Data security and Integrity in Cloud Computing.* Goa, India: ICONAT.

IBM. (16 de Noviembre de 2022). Obtenido de https://www.ibm.com/es-es/topics/cloud-computing

Juárez, M., & Romera, J. (27 de Mayo de 2023). *El Economista*. Obtenido de https://www.eleconomista.es/actualidad/noticias/12295028/05/23/meta-google-y-amazon-suman-multas-de-3440-millones-por-la-privacidad.html

Karczewska, J. (29 de Mayo de 2017). *ISACA*. Obtenido de https://www.isaca.org/es-es/resources/news-and-trends/industry-news/2017/cobit-5-and-the-gdpr

Kirsch, D., & Hurwitz, J. (2020). *Cloud Computing For Dummies.* Hoboken, New Jersey: John Wiley & Sons, Inc.

Mell, P., & Grance, T. (Diciembre de 2011). *NIST.* Obtenido de https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf

Mell, P., & Grance, T. (Septiembre de 2011). *NIST*. Obtenido de https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

Microsoft Azure. (28 de Septiembre de 2022). Obtenido de https://azure.microsoft.com/es-es/resources/cloud-computing-dictionary/what-is-cloud-computing

Microsoft Azure Blog. (s.f.). Obtenido de https://azure.microsoft.com/es-es/blog

NEEDHAM, M. (11 de Enero de 2024). *IDC*. Obtenido de https://www.idc.com/getdoc.jsp?containerId=prUS51763424

Netskope. (2024). Obtenido de https://www.netskope.com/netskope-threat-labs/cloud-threat-report/cloud-and-threat-report-2024

OpenStack. (2022). Obtenido de https://www.openstack.org/user-survey/2022-user-survey-report

Oracle. (s.f.). Obtenido de https://www.oracle.com/es/security/identity-management/what-is-iam

Oracle. (14 de Noviembre de 2022). Obtenido de https://www.oracle.com/es/cloud/what-is-cloud-computing

Organismo de Certificación Global (NQA). (2015). Obtenido de https://www.nqa.com/es-es/certification/standards/iso-27017

Organismo de Certificación Global (NQA). (2019). Obtenido de https://www.nqa.com/es-es/certification/standards/iso-27018

Pascual Estapé, J. A. (7 de Junio de 2024). *Computer Hoy*. Obtenido de https://computerhoy.com/ciberseguridad/descubren-como-fueron-hackeados-santander-tickermaster-1389240

Perri, L. (16 de Noviembre de 2023). *Gartner*. Obtenido de https://www.gartner.com/en/articles/what-are-industry-cloud-platforms

PowerData. (s.f.). Obtenido de https://www.powerdata.es/big-data

Raeburn, A. (1 de Julio de 2021). *Asana*. Obtenido de https://asana.com/es/resources/swot-analysis

RedHat. (20 de Enero de 2023). Obtenido de https://www.redhat.com/es/topics/internet-of-things/what-is-iot

RENO, N. (1 de Febrero de 2024). *Synergy Research Group*. Obtenido de https://www.srgresearch.com/articles/cloud-market-gets-its-mojo-back-q4-increase-in-cloud-spending-reaches-new-highs

Revista Cloud Computing. (22 de Enero de 2024). Obtenido de https://www.revistacloudcomputing.com/2024/01/6-tendencias-cloud-para-empresas-en-2024

Santos, D. (2 de Abril de 2024). *HubSpot*. Obtenido de https://blog.hubspot.es/marketing/crear-analisis-pestel

Schwartz, M. (29 de Diciembre de 2018). *AWS*. Obtenido de https://aws.amazon.com/es/blogs/enterprise-strategy/switching-costs-and-lock-in

Seda, D. (3 de Mayo de 2024). *Microsoft Azure*. Obtenido de https://azure.microsoft.com/en-us/blog/microsoft-is-a-leader-in-the-2024-gartner-magic-quadrant-for-cloud-ai-developer-services

Sinha, S., Bhatnagar, V., Agrawal, P., & Bali, V. (2024). *Integration of Cloud Computing with Emerging Technologies.* Boca Ratón, Florida: CRC Press; Taylor & Francis Group.

Stamford, C. (13 de Noviembre de 2023). *Gartner*. Obtenido de https://www.gartner.com/en/newsroom/press-releases/11-13-2023-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-reach-679-billion-in-20240

State of California Department of Justice. (13 de Marzo de 2024). Obtenido de https://oag.ca.gov/privacy/ccpa

Sunyaev, A. (2020). Internet Computing: Principles of Distributed Systems and Emerging Internet-Based Technologies. Springer.

Trevenque cloud. (s.f.). Obtenido de https://www.cloudcenterandalucia.es/blog/iaas-paas-y-saas-que-son-ejemplos-y-diferencias

Varusha, A. (7 de Febrero de 2024). *N-iX*. Obtenido de https://www.n-ix.com/cloud-computing-trends

VMWare. (s.f.). Obtenido de https://www.vmware.com/topics/glossary/content/software-defined-networking.html