ASEGURAMIENTO DE RECURSOS INFORMÁTICOS DE UNA NUBE HIBRIDA

YOBANY ANDREY BENITEZ HENAO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
MEDELLIN
2023

ASEGURAMIENTO DE RECURSOS INFORMÁTICOS DE UNA NUBE HIBRIDA

YOBANY ANDREY BENITEZ HENAO

Proyecto de Grado – Monografía presentado para optar por el título de

ESPECIALISTA EN SEGURIDAD INFORMÁTICA

EDGAR ROBERTO DULCE VILLARREAL

Tutor de Curso

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
MEDELLIN
2023

NOTA DE ACEPTACIÓN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Medellin., Fecha sustentación

DEDICATORIA

Dedico cada parte de este trabajo a las personas que me han apoyado en el proceso de aprendizaje, familia, profesores y amigos, cada aporte me ayudo a lograrlo.

AGRADECIMIENTOS

Agradezco a los profesores que estuvieron acompañándome en mi etapa de aprendizaje y sobre todo aquellos que reconocen que el conocimiento va más allá de reglas establecidas.

CONTENIDO

Pág.

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

GLOSARIO

API: "Application Programming Interface", es un grupo de funcionalidades o procedimientos expuestos que se desarrollan en un entorno web para que puedan ser utilizados por muchas aplicaciones.

AWS: "Amazon Web Services", proveedor de servicios de cómputo de nube liderado por la empresa Amazon.

BIG DATA: Hace referencia a un conjunto de datos que tiene un gran tamaño y no es posible procesarlo con software convencional, por lo que requiere de sistemas muy robustos para ello.

Bug: Es un error de software que genera un funcionamiento de manera inesperada.

Data Center: Traduce “centro de datos”, lugar donde se consolida la infraestructura tecnológica de una organización y se almacenan datos y aplicaciones[1].

DNS: Es un sistema de nombres de dominio, permite traducir un nombre en la red por una dirección IP para poder acceder a un servicio informático.

Firewall: Son sistemas físicos o virtuales que permiten el transito seguro entre dos sistemas o redes informáticas, permite controlar si el origen puede llegar al destino basado en reglas configurables[2].

Framework: Traduce “Marco de Trabajo”, conjunto de prácticas, conceptos y criterios para enfocar un tipo de problema y estandarizarlo para que sirva como referencia para otros temas similares.

Hardware: Elementos físicos que componen la estructura de los elementos tecnológicos o sistemas informáticos.

IDS: “Intrusion Detection System”, traduce “Sistema de detección de intrusos”, es un sistema de software o hardware que tiene como objetivo detectar actividades sospechosas en una red de computadores.

ISP: "Internet Service Provider", hace referencia al proveedor de servicios de internet que instala y asigna los medios físicos para que haya interconexión hacia las redes del mundo.

---

[1] CHECKPOINT. [Sitio Web]. ¿Qué es un data center (centro de datos)?. [Consultado el 10 de abril de 2022]. Disponible en: https://www.checkpoint.com/es/cyber-hub/what-is-a-data-center/

[2] CISCO. [Sitio Web]. ¿Qué es un firewall?. [Consultado el 10 de abril de 2022]. Disponible en: https://www.cisco.com/c/es_mx/products/security/firewalls/what-is-a-firewall.html

LDAP: "Lightweight Directory Access Protocol", es un protocolo y estándar informático que se utiliza para el intercambio de datos con base a un directorio, permite el manejo de autenticación y de atributos en aplicaciones.

Logs: En informática es un archivo de texto que almacena cronológicamente los eventos que van afectando a un sistema informático, con el fin de tener un rastro de auditoría.

Malware: En informática es un término para identificar cualquier tipo de programa malicioso o dañino que pueda comprometer un equipo tecnológico o un sistema de información.

MPLS: "Multiprotocol Label Switching", es un sistema de etiquetado que se utiliza en las redes informáticas para permitir que la información viaje de un lado a otro a través de enrutamiento y con niveles de prioridad[3].

Onpremise: Traduce “en local”, se refiere a un tipo de solución tecnológica que se encuentra en servidores dentro de la infraestructura de una empresa.

Query: Es una consulta que se realiza en un lenguaje de programación para extraer datos de determinado origen.

RoadMap: Hace referencia a la línea que recorre un proceso o un producto para la entrega de un servicio, como su alcance en el tiempo**.**

SLA: “Service Level Agreement”, traduce “Acuerdo de niveles de servicio”, tratado legal entre una compañía prestadora de servicios y un cliente para definir términos y condiciones del servicio.

Software: conjunto de programas informáticos permites realizar determinadas tareas en los equipos de cómputo.

Tier: En informática se refiere al nivel de fiabilidad en que se puede categorizar un centro de datos según sus capacidades de disponibilidad[4].

---

[3] CLOUDFLARE. [Sitio Web]. ¿Qué es MPLS (conmutación de etiquetas de protocolos múltiples?. [Consultado el 10 de abril de 2022]. Disponible en: https://www.cloudflare.com/es-es/learning/network-layer/what-is-mpls/

[4] INTERNETYA. [Sitio Web]. ¿Qué son TIER de los datacenter y cómo afectan mi hosting?. [Consultado el 10 de abril de 2022]. Disponible en: https://www.internetya.co/que-son-los-niveles-tier-de-los-data-centers-y-esto-como-afecta-mi-sitio-web/

UPS: "Uninterruptible Power Supply", es un dispositivo físico que aloja baterías u otros elementos encargados de almacenar energía con la finalidad de suplir corriente eléctrica frente a una interrupción.

VPN: “Virtual Private Network”, traduce “Red Privada Virtual”, configuración de redes de datos que permiten establecer una conexión segura entre dos puntos a través de internet[5]**.**

VNET: "Virtual Network", es un término informático que se utiliza para identificar las redes de datos en un ambiente de virtualización.

WAF: "Web Application Firewall", Es un sistema físico o virtual que ofrece servicios de protección informática para aplicaciones que se encuentran expuestas a internet.

WAN: “Wide Área Network”, Traduce “Red de Área Amplia” es una red de comunicaciones que permite interconexiones entre equipos geográficamente distantes.

[5] KASPERSKY. [Sitio Web]. ¿Qué es una VPN y cómo funciona?. [Consultado el 10 de abril de 2022]. Disponible en: https://latam.kaspersky.com/resource-center/definitions/what-is-a-vpn

RESUMEN

Los centros de datos han tenido una evolución constante con el fin de mejorar la disposición y la optimización de los recursos informáticos, desde la época de los años 60 se comenzaron a ver los diferentes enfoques que comenzaba a tener la infraestructura en cuanto a temas de virtualización, cada uno de estos nuevos avances comenzaban a generar nuevos retos para las organizaciones con el fin de mejorar su seguridad a la misma velocidad en la que evolucionaban los sistemas de información. A partir de ello se comenzaron a mejorar los data center tradicionales para protegerlos con mecanismos robustos como firewalls, Intrusion Detection System (IDS) o Web Application Firewall (WAF), además de sistemas de seguridad física que mantuviesen asegurados los recursos y los datos.

Las empresas se han tenido que adaptar a las nuevas exigencias del mercado lo cual ha hecho que su evolución deba ser rápida y organizada, el crecimiento de la infraestructura tecnológica y el acceso a los sistemas de información son grandes necesidades a las cuales han tenido que hacer frente, sin embargo la aceleración tecnológica trajo consigo tecnologías novedosas que rompen el paradigma de los data center locales y nace un concepto de computación en la nube, esta nueva modalidad de servicio permite a un proveedor de servicios poner a disposición su infraestructura tecnológica para el consumo de clientes, así podrán alojar allí sus sistemas de información, se comienza entonces a hablar de nuevos conceptos como la elasticidad, que permite reorganizar los recursos de la manera que se requiera y generar un costo solo por el uso. Siendo un servicio tan novedoso comienza a generar inquietudes frente a la seguridad de los datos, al estar alojados en ubicaciones geográficamente dispersas y solo ser accedidos a través de internet, incrementa su exposición ante un ataque informático, comienzan a derivarse nuevos tipos de nube entre las cuales se encuentra la nube hibrida, que converge lo mejor de esta nueva tecnología con los data center locales, permitiendo que haya una interconexión por medio de la cual la información pueda ser accedida de forma segura.

Pero son muchos los puntos a evaluar al momento de tomar la decisión de realizar esta transición, la confidencialidad, la integridad y la disponibilidad de la información y los recursos son algunos de los temas que se deben abordar, saber qué tipo de nube se va a implementar también genera peso en esta decisión, los ambientes públicos, privados o híbridos generan diferentes arquitecturas y diferentes riesgos lo que generará un esfuerzo en la creación de nuevas formas de gobernar la información y la infraestructura, se deben diseñar nuevos mecanismos para proteger la información, políticas de acceso, entre otros.

Una nube hibrida se convierte en una extensión de los Data Center tradicionales por lo que el gobierno de TI (tecnologías de la información) debe entender y adaptarse a esta nueva forma de operar, las organizaciones comienzan entonces a preguntarse cuál es la mejor manera de adoptar la tecnología en la nube sin afectar la seguridad de los datos, que elementos se deben tener en cuenta para ayudar a tomar las decisiones, que componentes pueden utilizar, como realizar un diseño y que políticas se pueden implementar, un buen gobierno ayuda enormemente a establecer pautas en la administración y adopción de la nube, apoyándose en lineamientos que evalúen los costos, la seguridad, la identidad, los nuevos recursos y los despliegues de manera efectiva.

ABSTRACT

The data centers have had a constant evolution in order to improve the provision and optimization of computing resources, since the time of the 60s the different approaches that the infrastructure began to have in terms of virtualization issues began to be seen. , each of these new advances began to generate new challenges for organizations in order to improve their security at the same speed at which information systems evolved. From this, traditional data centers began to be improved to protect them with robust mechanisms such as firewalls, IDS or WAF, in addition to physical security systems that kept resources and data secure.

Companies have had to adapt to the new demands of the market which has meant that their evolution must be fast and organized, the growth of technological infrastructure and access to information systems are great needs to which they have had to deal. front, however, the technological acceleration brought with it new technologies that break the paradigm of local data centers and a concept of cloud computing is born, this new service modality allows a service provider to make its technological infrastructure available for consumption of clients, so they can host their information systems there, then they begin to talk about new concepts such as elasticity, which allows resources to be reorganized as required and generate a cost only for use. Being such a novel service, it begins to generate concerns about data security, being hosted in geographically dispersed locations and only being accessed through the internet, increases its exposure to a computer attack, new types of cloud begin to arise among the which is the hybrid cloud, which converges the best of this new technology with local data centers, allowing an interconnection through which information can be accessed safely.

But there are many points to evaluate when making the decision to make this transition, confidentiality, integrity and availability of information and resources are some of the issues that must be addressed, knowing what type of cloud is going to implementing also generates weight in this decision, public, private or hybrid environments generate different architectures and different risks, which will generate an effort in the creation of new ways of governing information and infrastructure, new mechanisms must be designed to protect information, access policies, among others.

A hybrid cloud becomes an extension of the traditional Data Center, so the IT government must understand and adapt to this new way of operating, organizations then begin to ask themselves what is the best way to adopt cloud technology without affect data security, what elements must be taken into account to help make decisions, what components can be used, how to design and what policies can be implemented, good governance helps enormously to establish guidelines in

administration and adoption of the cloud, supported by guidelines that evaluate costs, security, identity, new resources and deployments effectively.

1 INTRODUCCION

La computación en la nube tiene diferentes modalidades que se pueden adaptar a los diferentes tipos de organizaciones, nube publica, privada e hibrida aparecen para apoyar la evolución tecnológica a la que deben enfrentarse las empresas[6], sin embargo, dada la preocupación que envuelve los temas de seguridad de la información alojados en ellas se opta como una buena opción la nube hibrida, es capaz combinar diferentes características para proveer servicios de calidad y seguros.

Ahora se presentan nuevos retos para las áreas de TI, consisten en definir como es el proceso de implementación y aseguramiento de esta nueva modalidad, diseñar nuevos esquemas de gobierno, administración y responsabilidades, también definir arquitecturas de conectividad que permitan comunicaciones seguras entre los sitios remotos de nube publica y nube privada, todo esto sin perder de vista la seguridad de los datos[7].

Durante el proceso de la adopción de esta tecnología se deben conocer cuáles son las ventajas y desventajas que puede ofrecer la nube, además cada una de sus derivaciones tiene propiedades diferentes que se adaptan a organizaciones con necesidades diferentes, es por eso por lo que se debe conocer sobre ellas y tener un concepto claro de lo que ofrecen. En el momento de pensar en estas tecnologías hay una falsa percepción de que toda la infraestructura debe estar en algún momento alojada en la nube del proveedor, pero hay muchos mecanismos y razones para convivir aun con el data center local, la seguridad de los datos se muestra como una de las preocupaciones más importantes al momento de hablar de nube, pero realmente se deben evaluar varios componentes que influyen en esa transición, ¿es posible tener lo mejor de ambos servicios?, una nube hibrida permite maximizar la infraestructura y las soluciones frente a los nuevos requerimientos de las organizaciones, al comparar ambas tecnologías se pueden tomar mejores decisiones y comenzar a tener una visión diferente del gobierno que se debe establecer, sin gobierno no hay seguridad, al tener controles establecidos y mejoras

[6] BAEZA, TADEO ROBERTO. [en línea]. El cómputo en la nube como factor de competitividad en las empresas. Tesis Ingeniera de Sistemas. Universidad Juárez Autónoma de Tabasco,2019. [Consultado el 25 de septiembre de 2022]. Disponible en: https://www.academia.edu/31073353/Ensayo_de_C%C3%B3mputo_en_la_Nube_como_factor_de_competitividad_empresarial

[7] DÍAZ ARIZA, WILSON DANIEL. [en línea]. computación en la nube y su seguridad. [Consultado el 03 de abril de 2022]. Disponible en: http://repository.unipiloto.edu.co/handle/20.500.12277/2785

continuas en el proceso de adopción, se puede llegar a un nivel de madurez optimo que permita crear arquitecturas seguras que sean coherentes con las necesidades de la organización.

2 DEFINICIÓN DEL PROBLEMA

Los servicios tecnológicos en nube han comenzado a ganar potencial a medida que las exigencias de disponibilidad y aprovisionamiento se vuelven una prioridad, sin embargo, hay factores que generan preocupación entre las organizaciones al momento de tomar la decisión y una de ellas en la seguridad de sus datos y la confidencialidad de su información, se ven entonces en la necesidad de ser conservadores al momento de tomar la decisión de migrar servicios a la nube.

2.1 ANTECEDENTES DEL PROBLEMA

Aunque la empresas ven la computación en la nube como una opción, también determinar que puede ser un riesgo tener su información almacenada en una infraestructura que no controlan, una infraestructura que no solo es administrada por terceros sino que además es compartida con muchos otros clientes, entre las principales preocupaciones de las organizaciones para adoptar estas tecnologías se encuentra la seguridad, según una encuesta realizada por Coalfire una empresa enfocada en la ciberseguridad, el 93 por ciento de las empresas encuestadas tienen moderada o extremadamente preocupaciones por la seguridad y esto siempre representara que haya una adopción más fuerte de este tipo de tecnologías; la encuesta también arroja otros datos interesantes como que el 64 por ciento de los profesionales encuestados sienten inquietudes por la posible pérdida de información y/o confidencialidad de los datos [8]. Esto se debe a que las organizaciones tienen una falsa percepción de que los Data Center que pueden ver y tocar son más seguros aun cuando los eventos de seguridad normalmente no ocurren en gran medida con el acceso físico.

La nube hibrida contiene lo mejor de ambos mundos, pero muchas empresas no saben cómo comenzar esta transición, que deberían tener en cuenta en el proceso o como diseñar o gobernar esta nueva infraestructura.

2.2 FORMULACIÓN DEL PROBLEMA

Teniendo en cuenta lo antes mencionado se origina la inquietud:

¿Cuáles son los elementos para tener en cuenta en el proceso de asegurar los recursos informáticos en una nube publica para un ambiente hibrido?

[8] COALFIRE. [Sitio Web]. Security Concerns Still a Barrier to Cloud Adoption. [Consultado el 05 de abril de 2022]. Disponible en: https://www.coalfire.com/insights/news-and-events/press-releases/coalfire-cloud-study

3 JUSTIFICACION

La evolución tecnológica se está encaminando hacia la computación en la nube, año tras año ha crecido el consumo de los servicios Cloud y es relevante conocer lo que implica este proceso en cuanto a la seguridad de los datos y la forma en la que se acceden, dado que la disponibilidad y confidencialidad de la información hace parte de las preocupaciones de muchas empresas y, según Gartner, la nube es un punto neurálgico que impulsa a todas las organizaciones que quieran digitalizarse el día de hoy y prevé que en el trascurso del año 2022 se incremente su uso y consumo, por parte de los usuarios, en un 30% solo en infraestructura como servicio[9], el presente trabajo pretende aportar a los interesados en incursionar en la transición hacia una nube, una forma controlada de convertir su fuerza de cómputo en un ambiente hibrido, dando a conocer los temas más relevantes en cuanto a la seguridad de la información e infraestructura, con esto las empresas se podrán plantear si es conveniente o no dar el salto hacia estas nuevas tecnologías y cuáles son los riesgos y beneficios que conlleva, así, se podrá aportar un punto de vista que permita dilucidar muchas de las inquietudes respecto a esa transición.

[9] GARTNER. [Sitio Web]. IaaS, DaaS and PaaS to Witness Highest Spending Growth This Year. [Consultado el 25 de octubre de 2022]. Disponible en: https://www.gartner.com/en/newsroom/press-releases/2022-04-19-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-reach-nearly-500-billion-in-2022

4 OBJETIVOS

4.1 OBJETIVO GENERAL

Evaluar los principales componentes que se deben tener en cuenta para iniciar la transición y aseguramiento de la información hacia una nube hibrida.

4.2 OBJETIVOS ESPECÍFICOS

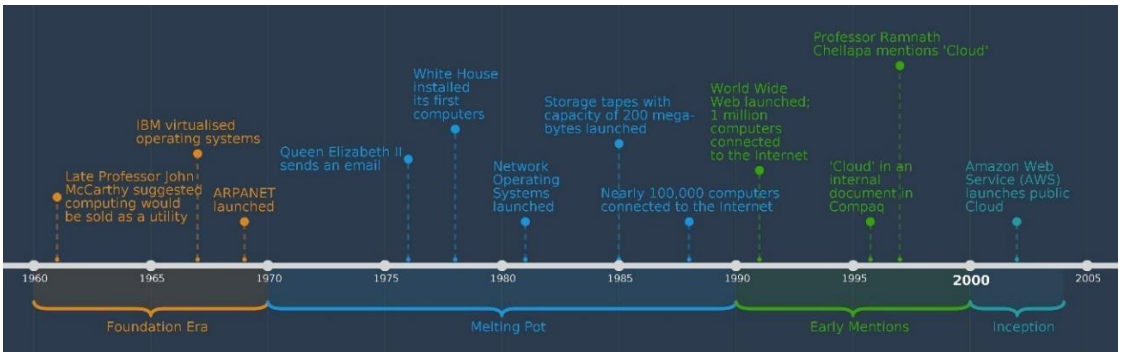
- Explicar las diferentes tecnologías de nube, publica, privada e hibrida definiendo cada una de ellas con sus ventajas y desventajas.
- Comparar los elementos de infraestructura y seguridad que componen un esquema tradicional de cómputo frente a las nuevas tecnologías de nube, describiendo los pilares que los relacionan como centros de datos.
- Justificar la construcción de un gobierno para la administración de recursos tecnológicos en una nube hibrida, explicando las disciplinas que se deben tener en cuenta para su adopción.

5 MARCO REFERENCIAL

5.1 MARCO TEÓRICO

La computación en la nube es un término, que, aunque es nuevo como nombre, ha existido desde hace décadas y ha ido evolucionando hasta lo que se tiene hoy. Durante la década de los años 60 se comenzaron a formar las bases para lo que sería la nube, el profesor John McCarthy un gran científico informático y creador del término “Inteligencia Artificial” fue quien en 1961 sugirió que la infraestructura tecnológica se comercializaría como un servicio en algún momento [10]. más tarde en 1967 IBM (International Business Machines) comienza a virtualizar sistemas operativos y esto permite que se pueda reutilizar hardware y tener varias aplicaciones siendo accedidas por diferentes usuarios en un solo punto de virtualización. Entre los años 70 y 80 nacen las redes TCP/IP (Transmission Control Protocol/Internet Protocol), todas las tecnologías que posteriormente sentarían las bases de la computación en la nube tomaron cierta madurez en la década de los 90, ya había más de 1 millón de máquinas conectadas a la red de internet, aplicaciones web y otros servicios que ya estaban siendo consumidos por diferentes usuarios. En 2002 aproximadamente Amazon lanza su primera versión de una nube publica donde presenta todos los beneficios que puede traer esta tecnología [11]. A continuación, se muestra una gráfica representando la línea de tiempo de todos los sucesos representativos del nacimiento de la computación en la nube.

Figura 1. Linea de tiempo del nacimiento de la computación en la nube



Fuente: BCS. [Sitio Web]. History of the cloud. [Consultado el 06 de abril de 2022]. Disponible en: https://www.bcs.org/articles-opinion-and-research/history-of-the-cloud/

[10] VARGHESE,BLESSON . [en línea]. History of the cloud. [Consultado el 06 de abril de 2022]. Disponible en: https://www.bcs.org/articles-opinion-and-research/history-of-the-cloud/
[11] Ibid

Tradicionalmente las organizaciones que manejan recursos informáticos han esquematizado la infraestructura tecnológica como elementos que deben encontrarse de manera local y persistente en establecimientos custodiados por la misma empresa, esta ha sido la manera en que las compañías protegen sus activos de información de manera física. Con el crecimiento exponencial de la tecnología, las áreas de TI (Tecnologías de la información) han comenzado a volverse costosas en cuanto al mantenimiento, renovación y escalamiento de los recursos, una empresa cuyo Core de negocio no es la tecnología hoy está considerando grandes aportes económicos para sostener su infraestructura tecnológica.

Con la evolución comenzaron a surgir nuevas tecnologías como la virtualización, que permitió ahorrar espacio físico y aprovechar mejor las capacidades de los recursos, aunque TI se vuelve un poco más costo-eficiente se continua operando con el método tradicional de tener un Data Center local con toda la operación y administración que conlleva, aunque la infraestructura se ha vuelto cambiante, la importancia de la confidencialidad e integridad de la información sigue siendo igual de importante en todos los ámbitos, tener los servicios de manera local generalmente le provee a los dueños de la información un parte de tranquilidad ya que consideran que es más fácil restringir el acceso a personal no autorizado o que se encuentre fuera de la organización, no obstante la misma evolución ha comenzado a obligar a los usuarios a compartir más y más información con usuarios externos a la compañía, proveedores, socios, aliados, clientes y entidades gubernamentales o públicas, estos cambios han generado en el área de TI nuevos retos para proteger la información y el acceso a los sistemas.

El surgimiento de la computación en la nube atravesó muchos paradigmas relacionados a los métodos tradicionales de gestionar infraestructura de TI, se comenzó a hablar de nuevos términos como infraestructura como servicio (IaaS), Software como servicio (SaaS) y plataforma como servicio (PaaS), que prometen elasticidad y escalamiento dinámico en la medida que la organización lo requiera, unos costos por uso que se convirtieron en una excelente opción si se aprovechan de manera sensata, comienza a crear un amplio catálogo de herramientas, motores de bases de datos, aplicaciones web, frameworks de desarrollo entre otros, todo esto con un aprovisionamiento casi inmediato por lo que los proyectos que requieren de tecnología pueden ser implementados con rapidez.

Aunque parece que todo son bondades surge un nuevo temor para las empresas, ¿Dónde están alojados mis datos? ¿Quién puede acceder a ellos? ¿Cómo los protejo? ¿Toda la infraestructura e información debe estar en la nube? Estos interrogantes han detenido muchos procesos de adopción de las tecnologías de nube, como indica Katie Costello en un artículo expuesto en el sitio oficial de Gartner

[12], "*El rápido ritmo de innovación en los servicios de infraestructura y plataformas en*

la nube (Cloud Infrastructure and Platform Services, CIPS) convierte a la nube en la plataforma de facto para nuevos servicios digitales y cargas de trabajo tradicionales existentes por igual, razón por la cual el 40 % o todas las cargas de trabajo empresariales se implementarán en CIPS para 2023, frente a solo el 20 % en 2020". El estudio se basa en el incremento sustancial del uso de las tecnologías en la nube debido a la pandemia por COVID-19 que sacudió al mundo en 2020.

Las empresas, en su afán por mantenerse firmes en el mercado, comenzaron a evaluar los aspectos que debían tener en cuenta para empezar llevar su información a la nube y que pueda ser accedida de manera segura, sin embargo, muchas de los que han adoptado tecnología en la nube solo lo han hecho para experimentar o considerar temas de contingencia de su infra local, debido a esta preocupación nace un nuevo concepto conocido como nube hibrida, surge como un nuevo concepto que incorpora la ubicación física de los elementos cuando generalmente en el concepto de nube no importaba, para permitir a la organización elegir que quiere operar de manera local y que desea migrar a la nube, todo esto ofreciendo una intercomunicación entre ambos mundos lo que convierte a la nube en una extensión del mundo en premisa y viceversa.

Aunque se presenta un esquema nuevo, las dudas sobre el acceso a la información sigue latente, la nube hibrida depende de la nube publica, la cual está expuesta a internet y puede representar aún más peligro si está conectada directamente con el entorno local, podría convertirse en una brecha de seguridad y de acceso a toda la organización. Grandes empresas prestadoras de servicios tecnológicos le están apostando a la computación en la nube y los ambientes híbridos hacen parte de su roadmap, IBM, RedHat, Microsoft, Amazon, Google, entre otros, poseen toda una infraestructura virtual que permite llevar a cabo la transición de manera segura, un buen diseño y gobierno de la infraestructura permitirán operar de manera segura.

[12] Costello,Katie. (2021). [en línea]. Gartner predice el futuro de las infraestructuras de Cloud y Edge Computing. [Consultado el 04 de abril de 2022]. Disponible en: https://www.gartner.es/es/articulos/gartner-predice-el-futuro-de-las-infraestructuras-de-cloud-y-edge-computing

5.2 MARCO CONCEPTUAL

Las tecnologías de nube están compuestas por diferentes tipos de recursos que tienden a ser transversales sin importar el tipo de nube que se elija, publica, privada o hibrida se deben entender algunos conceptos tanto en infraestructura como en seguridad.

Hay tres grandes tipos de servicios que son prestados por los proveedores de nube, IaaS, SaaS y PaaS, cada uno de estos elementos tienen sus propias capaz de seguridad y aunque cada proveedor ofrece herramientas diferentes para ello, se podrían consolidar en: Identity and Access Management (IAM), Directory Service, Administracion y almacenamiento de claves (KMS o KeyVault), firewalls o auditorias con control y automatización de eventos, las nubes hibridas contienen elementos adicionales de red como las VPN (Virtual Private Network).

5.2.1 IaaS.

La sigla significa Infraestructure as a Service, este modelo de servicio permite que las empresas puedan aprovisionar recursos de hardware virtual con el fin de aprovisionar servicios de manera muy inmediata, una de las ventajas de este tipo de servicio es que los recursos son flexibles y de aprovisionamiento inmediato, al estar alojado en la nube no existen preocupaciones por elementos como la energía, la disponibilidad y todos los elementos de tiempo que costaría adquirir equipos físicos en un Data Center tradicional, sin embargo el usuario final debe continuar custodiando temas como el sistema operativo y todas las aplicaciones relacionadas a él. [13]

5.2.2 PaaS.

Platform as a Service, en la plataforma como servicio se avanza un poco más en la desagregación de servicios que debe operar el usuario, ya que se ofrece acceso a la administración de la aplicación y los datos, pero ya no se permite acceder a partes del cómo el sistema operativo, plugin, instalación de nuevas herramientas, controles de versión, temas de licenciamiento, todo esto hace parte de la administración del proveedor de la nube. [14]

[13] GOOGLE CLOUD. [Sitio Web]. ¿Qué es IaaS?. [Consultado el 06 de abril de 2022]. Disponible en: https://cloud.google.com/learn/what-is-iaas?hl=es

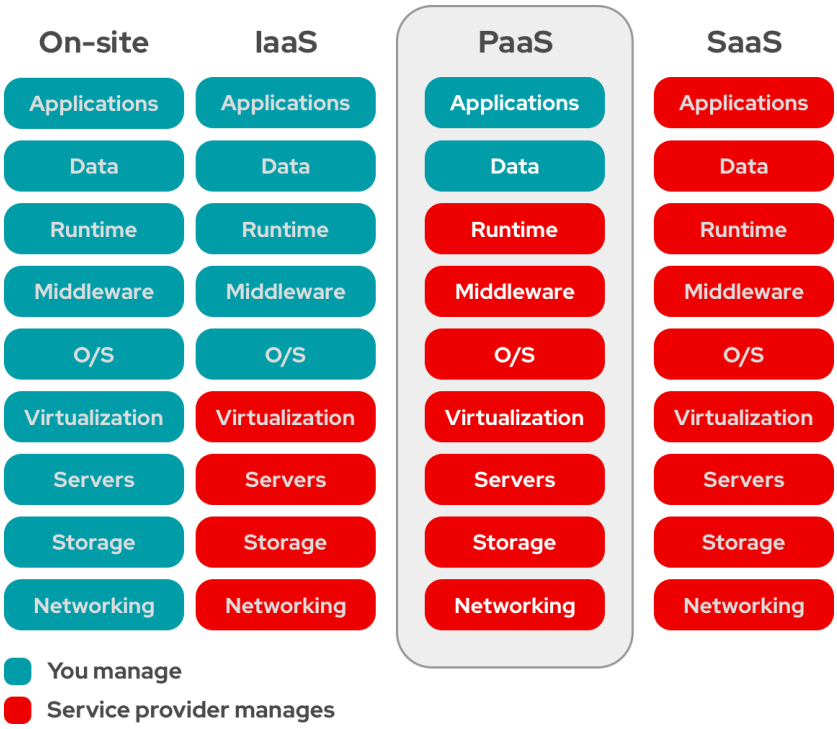
[14] MICROSOFT AZURE. [Sitio Web]. Plataforma como servicio. [Consultado el 06 de abril de 2022]. Disponible en: https://azure.microsoft.com/es-es/overview/what-is-paas/

5.2.3 SaaS.

El software como servicio es la última capa de servicios en la nube, este representa la prestación de un servicio sin ningún tipo de administración por parte del usuario final, más allá de las parametrizaciones que requiera, el proveedor de nube mantiene y actualiza todo lo referente al software, hardware y seguridad, esto genera un despliegue rápido a un muy bajo costo.

A continuación, se muestra de manera grafica los tipos de recursos y el nivel de administración que tiene en cada uno, por parte del proveedor de nube y del usuario.

Figura 2. Diferencias de administración entre los servicios de nube



Fuente: RED HAT. [Sitio Web]. Diferencias entre PaaS, IaaS y SaaS. [Consultado el 06 de abril de 2022]. Disponible en: https://www.redhat.com/es/topics/cloud-computing/what-is-paas

Frente a los conceptos de seguridad normalmente la computación en la nube maneja controles de acceso cuyo tipo de servicio SaaS permite al usuario parametrizarlo y configurarlo.

5.2.4 IAM

según Gartner, la administración e identidad de acceso es una disciplina que habilita y permite los derechos individuales de acceso, en el momento correcto y por las razones correctas, [15]. Este módulo tiene como fin asegurar el acceso a los servicios de cómputo, aplicaciones y datos que se encuentran almacenados en los proveedores de nube, permite monitorear cada evento y controlar quien puede ver y/o acceder que recurso, se obtiene entonces un modelo de seguridad centralizado que permite trabajar desde cualquier ubicación.

5.2.5 Directory Service

Es muy común encontrarse con que las organizaciones ya cuentan con un sistema propio de autenticación de usuarios como lo es Microsoft Active Directory, la nube provee mecanismos para reutilizar estos servicios que ya están operando de manera eficaz en las organizaciones y los conecta con su sistema de autenticación propio, esto permite garantizar que los usuarios puedan continuar utilizando sus credenciales habituales para el tema de autenticación y dejarle al IAM el tema de autorización.

5.2.6 Administracion y almacenamiento de claves

La preocupación de salvaguardar los secretos como claves, llaves, certificados entre otros, lleva a los proveedores de nube a crear un almacén dedicado a esta labor, los almacenes de llaves permiten alojar información sensible que puede ser consultada por aplicaciones, esto evita que en el código fuente de ellas permanezcan grabadas en al guna variable, el proceso consiste en consumir un servicio web a través de HTTPS (Hyper Text Transfer Protocol Secure) que, una vez verificada la identidad de la aplicación o del usuario, le permitirá acceder solo al secreto que tiene autorización de leer.

[15] GARTNER. [Sitio Web]. Identity and Access Management (IAM). [Consultado el 06 de abril de 2022]. Disponible en: https://www.gartner.com/en/information-technology/glossary/identity-and-access-management-iam

6 EXPLICAR LAS DIFERENTES TECNOLOGÍAS DE NUBE, PUBLICA, PRIVADA E HIBRIDA DEFINIENDO CADA UNA DE ELLAS CON SUS VENTAJAS Y DESVENTAJAS

Las tecnologías de nube han sido el resultado del desarrollo tecnológico en cuanto a infraestructura de TI, aunque la virtualización se conoce hace muchos años, nunca se había integrado de tal manera que se empezara a ofrecer como servicio, servidores, redes, seguridad, aplicaciones y bases de datos. Existen tres tipos conocidos de nube, nube publica, nube privada y nube hibrida, todas ellas con características diferentes que resuelven problemas diferentes.

6.1 Nube pública

Se puede definir que una nube publica se caracteriza porque su infraestructura es completamente ajena al usuario que está haciendo uso de ella, o sea, todo lo relacionado a servidores, red, almacenamiento y demás servicios tecnológicos son soportados por un tercero, además de esto se debe tener en cuenta que todos los recursos son compartidos a través de todos los clientes y/o empresas que estén utilizando esos servicios, como parte de los acuerdos con el proveedor, esta infraestructura debe tener una segmentación lógica para evitar que una empresa pueda acceder a los recursos de otra.

La nube publica se basa en un esquema de virtualización que tiene la capacidad de extender las capacidades de las infraestructuras tradicionales de una organización, esto le permite aprovisionar e implementar recursos en un sitio físicamente remoto. En esta opción de nube se tienen actualmente unas preocupaciones en el tema de seguridad por parte de los responsables de las áreas de tecnología, se debe invertir mucho tiempo en analizar temas como el cifrado de la información y los mecanismos de transporte seguro ya que todo el tráfico viaja a través de internet[16].

Otros aspectos importantes son los temas de conectividad que deben ser evaluado, ya que la ubicación geográfica de un proveedor de servicios de nube publica puede inferir directamente en la latencia del servicio.

La nube publica ofrece servicios como PaaS, IaaS y SaaS, estos servicios permiten adecuar muchos tipos de soluciones y acomodarse a las necesidades de los usuarios, cada una de ellas tiene un manejo diferente de la seguridad y se deben evaluar cada uno de los riesgos asociados a ellas.

[16] VMWARE. [Sitio Web]. ¿Qué es una nube pública? [Consultado el 13 de abril de 2022]. Disponible en: https://www.vmware.com/es/topics/glossary/content/public-cloud.html

A continuación, en la tabla 1 se relacionan algunos aspectos positivos y negativos de esta modalidad de nube:

Tabla 1. Pros y Contras de Nube Publica

Pros	Contras
Alta escalabilidad que permite crecer en recursos de manera casi ilimitada y muy rápido	Preocupación por la seguridad de los datos y el acceso no autorizado a la infraestructura, esto se relaciona más por malas prácticas de las organizaciones que por las implementaciones del proveedor de nube
Los costos asociados a hardware y software se reducen y se implementa una modalidad de pago por uso	El pago por uso puede incrementarse de manera desmesurada y elevar los costos si no se aprovisiona lo que realmente se requiere y en los tiempos que se necesita
Riesgo mínimo de perdida de datos debido a redundancia por parte de los proveedores de nube	Tiempos de respuesta altos frente a una necesidad de soporte si no se contratan o revisan adecuadamente los niveles de SLA ofrecidos por el proveedor
Flexibilidad que permite aumentar o disminuir recursos en la medida que los altos volúmenes de trabajo lo requieran	La personalización es limitada dado que la administración de la infraestructura corre por cuenta del proveedor
Se reduce el tiempo de aprovisionamiento para ambientes de desarrollo, pruebas o producción	Se debe contar con conexiones estables de internet y buenos anchos de banda

Fuente: Propia

6.2 Nube privada

El concepto de nube privada nace de la necesidad de cubrir las preocupaciones de seguridad que se encuentran en las nubes públicas, muchos proveedores de infraestructura comenzaron a ofrecer servicios de “nube local” y se implementan dentro de los Data Centers internos de cada compañía, como lo comenta Peter Mell y Timothy Grance del instituto nacional de estándares y tecnología (NIST), “*La infraestructura de la nube está aprovisionada para uso exclusivo de una organización que comprende múltiples consumidores. Puede ser propiedad de la organización, un tercero o una combinación de ellos, administrarlo y operarlo, y puede existir dentro o fuera de las instalaciones*.”[17].

Esta modalidad de nube conserva características similares de una publica como lo es el tema del autoservicio y la escalabilidad pero también tiene un conjunto de limitaciones que se deben tener en cuenta, por ejemplo, la arquitectura es poco flexible dado que seguramente deberá adaptarse a las necesidades de aplicaciones propias de la compañía, el almacenamiento de datos puede volverse complejo dado que una organización puede hacer del uso de almacenamiento local y requerir capacidades de almacenamiento en la nube publica, puede atraer costos adicionales, también a pesar que se tiene un control de la infraestructura, una mala administración puede generar brechas de seguridad que permitan generación de vulnerabilidades con las que antes no contaba la organización.

Los motivos frecuentes para elegir este tipo de nube radican básicamente en:

- Los requerimientos de seguridad y control de la información dictados por la organización sean tan estrictos que no faculten a la nube publica como una opción.
- La empresa tiene un gran tamaño y musculo financiero que le permita ser costo eficiente con este tipo de modalidad privada.
- La organización tiene unos requisitos muy específicos en cuanto a los niveles de servicio que no encuentra personalizables en una nube pública.

[17] GRANCE, TIMOTHY Y MELL, PETER.[en linea]. The NIST Definition of Cloud Computing. [Consultado el 13 de abril de 2022]. Disponible en: https://csrc.nist.gov/glossary/term/private_cloud

A continuación, en la tabla 2 se muestra un cuadro comparativo de características en favor y en contra de este tipo de nube:

Tabla 2. Pros y Contras de Nube Privada

Pros	Contras
La seguridad ofrece control de los datos ya que están almacenados en servidores de la empresa	una mala administración puede dejar expuestas vulnerabilidades
Para medianas y grandes empresas puede ser más costo eficiente en el tiempo adquirir la infraestructura	se requiere de una inversión económica inicial significativa
Permite personalizar el servicio tanto como la organización lo requiera	un exceso de modificaciones puede convertir el servicio en inflexible
el acceso y la administración son de manejo total de la organización	se requiere de personal capacitado en seguridad e infraestructura para administrarla

Fuente: Propia

la diferencia más notoria entre una nube privada y una nube publica, es que la nube privada va enfocada a un solo cliente, mientras que una nube publica es inherentemente multiusuario y puede tener N clientes al mismo tiempo, las nubes privadas son accedidas de las redes internas de la organización mientras que las nubes públicas por lo general lo hacen desde internet, ambas requieren diferentes enfoques de seguridad. [18]

[18] CHECKPOINT. [Sitio Web]. What is Private Cloud Security?. [Consultado el 13 de abril de 2022]. Disponible en: https://www.checkpoint.com/cyber-hub/cloud-security/what-is-private-cloud-security/

6.3 Nube hibrida

Conociendo las bondades y dificultades de nube publica y nube privada, nace un concepto transversal conocido como nube hibrida que permite tomar lo mejor de ambos mundos y combinarlos en una nueva modalidad de infraestructura, este tipo de nube realiza una correlación de los recursos Onpremise de forma que permite que se puedan compartir datos, servicios y aplicaciones de una forma segura, así las organizaciones pueden controlar la información que debe estar en la nube y la que no, datos críticos y aplicaciones privadas pueden mantenerse en el entorno local con los procesos de seguridad que se tengan dispuestos para ellas y pueden usar la nube publica para flexibilizar otros procesos de la compañía que lo requieran.

Las nubes hibridas permiten desligar las aplicaciones de lugares geográficos y aun así continuar comunicándose con el mundo local y acceder a los recursos corporativos, obviamente se deben tener unos controles de comunicación privada que puede darse por sistemas de VPN implementados entre la nube publica y el mundo onpremise[19].

Con esta modalidad se pueden continuar utilizando los servicios de nube publica como lo son IaaS, PaaS y SaaS, favoreciéndose con la flexibilidad y el poder de cómputo para cargas básicas o no sensibles para la organización y permitiendo solo la comunicación con los servicios locales, de elementos o recursos específicos que requieran de ella, se puede optar por alojar allí también servicios críticos no expuestos, con la debida administración, se puede denegar cualquier tipo de acceso público y solo permitir acceso vía VPN o WAN.

La nube hibrida, aunque tiene muchas bondades, presenta un nuevo dilema en el tema de seguridad de la información, aunque puedo controlar en donde alojo mis datos, no exime a las redes de estar plenamente comunicadas de alguna manera, el mundo de nube publica es capaz de alcanzar el mundo onpremise y viceversa, el nuevo reto consiste en diseñar de manera precisa la arquitectura que pueda garantizar la confidencialidad, integridad y disponibilidad de los datos.

[19] DELOITTE. [Sitio Web]. La nube híbrida. [Consultado el 13 de abril de 2022]. Disponible en: https://www2.deloitte.com/es/es/pages/technology/articles/nube-hibrida.html

A continuación, en la tabla 3 se aprecian algunos aspectos positivos y negativos de la nube hibrida:

Tabla 3. Pros y Contras de Nube Hibrida

Pros	Contras
Permite un mayor control de seguridad en la información crítica de la organización	Puede ser complejo el diseño de la seguridad a implementar entre ambos mundos
Temas como Big Data pueden ser ejecutados en la nube publica y no afectar infraestructura local ni adquirir nuevo hardware para ello	Se puede generar una dependencia de los servicios del proveedor para poder expandirse y ejecutar nuevos procesos
La conectividad a través de canales seguros permite el acceso a los recursos alojados en nube publica de manera segura	se debe adquirir dispositivos que permitan esta comunicación y contratar anchos de banda que permiten mover los volúmenes de información que se requieran
Es adaptable y flexible porque permite a la organización decidir que, como y donde alojar sus servicios	Se debe tener información constante sobre las actualizaciones que el proveedor de nube publica hace sobre su infraestructura para evitar problemas de compatibilidad
Genera reducción de costos en adquisición de infraestructura nueva para ambientes de desarrollo y pruebas	Una mala planificación puede aumentar los costos de uso de nube publica afectando la costo eficiencia de la operación
Se puede integrar un sistema de identidades para poder acceder a los recursos desde ambos mundos	Es complejo elegir qué elementos deben encontrarse en nube publica y cuales onpremise y como se deben dar los accesos de autenticación y autorización

Fuente: Propia

Los tres tipos de nube presentan características y comportamientos diferentes de acuerdo con las necesidades de cada organización, no se tiene una fórmula que indique cuales es la mejor y cual no lo es, todo depende del diseño y de las arquitecturas que se requieran para brindar solución a un determinado proyecto. Sin embargo, tienen en común que todos los proveedores de nube prestan estos servicios y son garantes de su sostenibilidad y soporte, además de la disponibilidad para los usuarios que usarán el servicio, pero se debe considerar siempre el papel de cada organización al momento de compartir responsabilidades una vez se tome la decisión de cuál es la modalidad que adoptará.

7 COMPARAR LOS ELEMENTOS DE INFRAESTRUCTURA Y SEGURIDAD QUE COMPONEN UN ESQUEMA TRADICIONAL DE CÓMPUTO FRENTE A LAS NUEVAS TECNOLOGÍAS DE NUBE, DESCRIBIENDO LOS PILARES QUE LOS RELACIONAN COMO CENTROS DE DATOS

Al pensar en incursionar en los temas de nube es imposible evitar comparar los diferentes puntos que conforman una tecnología y otra para ayudar a tomar la decisión correcta, la infraestructura on premise vs la infraestructura Cloud es una cuestión por regla en la que todos los administradores de sistemas deben pensar. Para poder lograr una adecuada transformación digital en las compañías, no se pueden obviar ninguno de los temas que conforman esta comparativa. Además, dado que la nube se ha convertido en un factor estratégico se deben analizar y entender todas las casuísticas que rodean están tecnologías[20].

Se puede decir entonces que hay pilares determinantes para permitir la comparación entre ambos ambientes, ubicación, disponibilidad, seguridad, escalabilidad y costos.

7.1 Ubicación

Los centros de datos tradicionales cuentan con toda la infraestructura de cómputo ubicada en las sedes físicas de la organización, todos sus dispositivos tecnológicos como los son servidores, switches, firewalls, IDS, entre otros, se encuentran alojados bajo la supervisión del personal de tecnología de la empresa y de agentes de seguridad que lo custodian.

Un sistema de nube considera que la ubicación de su infraestructura se encuentra geográfica distribuida a nivel mundial, cuenta con gran número de dispositivos tecnológicos para poder prestar sus servicios en los diferentes modelos, o sea, aunque eventualmente existe físicamente en algún lado, para el cliente es indiferente ya que solo está consumiendo un servicio.

Para una nube hibrida convergen estas dos casuísticas, ya que se apoya de la ubicación física de los centros de datos del cliente y debe existir una intercomunicación con los servicios de la nube, se puede decir entonces, que aumenta el punto de fallo, dependiendo de cómo este construida la nube hibrida, ya que para que funcione al 100% la nube hibrida depende de factores entre ambos mundos.

[20] MARQUES. [Sitio Web]. Comparativa Cloud vs On-premise. [Consultado el 01 de mayo de 2022]. Disponible en: https://www.marquesme.com/comparativa-servidor-cloud-vs-on-premise

Aunque existan diferencias entre ellas, cada infraestructura requieren de mantenimiento constante y muy exhaustivo, para así poder brindar un buen funcionamiento a los sistemas a lo largo del tiempo, en los Data Center tradicionales esta tarea se encuentra a cargo del equipo propio de tecnología quien debe estar capacitado para ello, la tecnología en nube por otro lado ya cuenta con equipos expertos dedicados a esta tarea por lo que no es necesario pensar en ello, sin embargo para el tema de nube hibrida igualmente se requiere de la intervención de los equipos locales para asegurar la conectividad y correcta prestación del servicio con la nube.

7.2 Disponibilidad

Es indispensable poder disponer de los servicios de información en cualquier momento, hay varios fatores que influyen en la disponibilidad de los Data Center tradicionales y de nube que se deben tener en cuenta, la fiabilidad y mantenimiento de cada uno de sus componentes, diseño de las redes de comunicación, comportamiento del sistema y su operación. Los Data Center on premise cuentan con una clasificación creada por Uptime Institute[21] llama Tier Classification donde básicamente se refieren a la clasificación de un Data Center de acuerdo con sus condiciones físicas y características, dándole un valor porcentual en cuanto a la disponibilidad que manejan de acuerdo con ello.

Tier I: es un nivel básico de infraestructura para respaldar los recursos informáticos, normalmente debe contener UPS (Uninterruptable Power Supply), áreas específicas para los dispositivos tecnológicos, equipos de refrigeración y generadores para cortes de energía, este tipo de Tier debería prestar un 99.671 % de disponibilidad.

Tier II: En este nivel, los componentes de infraestructura cubren necesidades de redundancia en temas de energía y refrigeración lo que permite realizar mantenimientos con más frecuencia y hay seguridad frente a interrupciones, se incluyen componentes como, unidades de refrigeración, módulos de UPS, equipos extractores de calor, generadores de energía, este tipo de Tier se comienza a enfocar en entornos más críticos donde la disponibilidad de la información toma fuerza, debido a la redundancia pueden haber desconexiones de tipo físicas y poder continuar operando, este nivel presta una disponibilidad de 99.741 %. [22]

[21] UPTIMEINSTITUTE. [Sitio Web]. About Uptime Institute. [Consultado el 01 de mayo de 2022]. Disponible en: https://uptimeinstitute.com/about-ui

[22] UPTIMEINSTITUTE. [Sitio Web]. Sistema de clasificación Tier. [Consultado el 01 de mayo de 2022]. Disponible en: https://es.uptimeinstitute.com/tiers

Tier III: se centra en la redundancia en todos los factores, evitando así el cierre de un centro de datos por labores de mantenimiento, toma factores de los Tier II y los maximiza para poder apoyar entornos de infraestructura critica, la disponibilidad prestada equivale al 99.982. %

Tier IV: Cuenta con sistemas distribuidos y geográficamente aislados, donde actúan como redundancia ante cualquier desastre, esta separación es requerida para evitar puntos de falla centralizados en ubicaciones específicas y así se evita que se comprometan los sistemas redundantes, básicamente se añaden componentes de tolerancia a fallos a los sistemas de Tier III donde las operaciones y la información estará disponible aunque se vea afectado todo un sitio, la disponibilidad prestada es del 99.995 %.[23] En la tabla 4 se pueden observar los niveles de disponibilidad de cada nivel de Tier y la indisponibilidad permitida para que pueda situarse en ese rango.

Tabla 4. Disponibilidad Data Center

Tier	% disponibilidad	% de indisponibilidad	Tiempo de indisponibilidad al año.
Tier I	99.671%	0.329 %	28.82 horas
Tier II	99.741%	0.251 %	22.68 horas
Tier III	99.982%	0.018 %	1.57 horas
Tier IV	99.995%	0.005 %	52.56 minutos

Fuente: CLIATEC. [Sitio Web]. Diseño Data Center y Grados de disponibilidad (Tier). [Consultado el 01 de mayo de 2022]. Disponible en: https://cliatec.com/diseno-data-center/

En la tecnología en la nube provee altos niveles de disponibilidad y muchos de ellos están asociados a los diferentes servicios que prestan, de hecho es muy normal encontrar diferente niveles de acuerdo de servicio dependiendo de que recurso va a consumir la organización, dado que hay opciones donde el cliente determina la disponibilidad de sus recursos ya sea por redundancia local, de zonas , regiones o

[23] CLIATEC. [Sitio Web]. Diseño Data Center y Grados de disponibilidad (Tier). [Consultado el 01 de mayo de 2022]. Disponible en: https://cliatec.com/diseno-data-center/

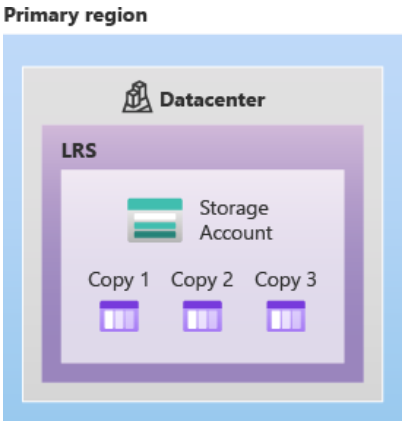
geografía mundial, todos estos factores ofrecerán un factor de disponibilidad diferente para el acceso a la información.

Almacenar por ejemplo información en un disco virtual trae las siguientes opciones.

Redundancia local: genera una réplica de hasta tres veces dentro de un mismo centro de datos de la nube, esto indica que se puede tener un nivel de disponibilidad de 99,999999999 % (once nueves) durante un año.

En la figura 3 se puede observar el comportamiento de réplica de un almacenamiento en la nube en su zona primaria.

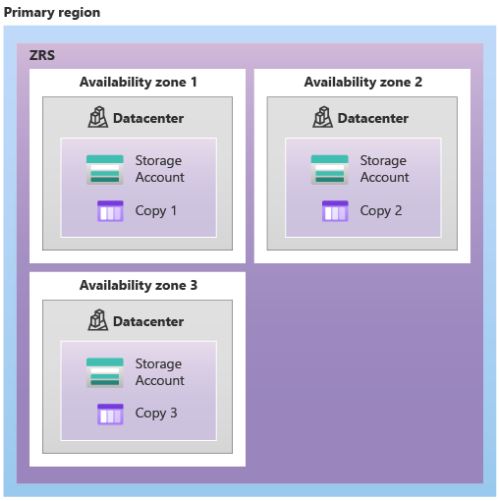
Figura 3. Disponibilidad nube redundancia local



Fuente: MICROSOFT. [Sitio Web]. Redundancia de Azure. [Consultado el 01 de mayo de 2022]. Disponible en: https://docs.microsoft.com/es-es/azure/storage/common/storage-redundancy

Redundancia por zona: este método de redundancia genera una réplica sincrónica de la información hasta en tres zonas dentro de la misma región donde se encuentre el Data Center primario del proveedor de nube, si una de las zonas falla el proveedor de nube redirecciona el trafica y modifica cualquier tema de DNS (Domain Name System) para no generar impacto con el acceso a la información, la disponibilidad prestada es del 99,9999999999 % (doce nueves) durante un año. En la figura 4 se ejemplifica la manera en que el almacenamiento realiza replicas por sus zonas de redundancia en una misma región del proveedor de nube.

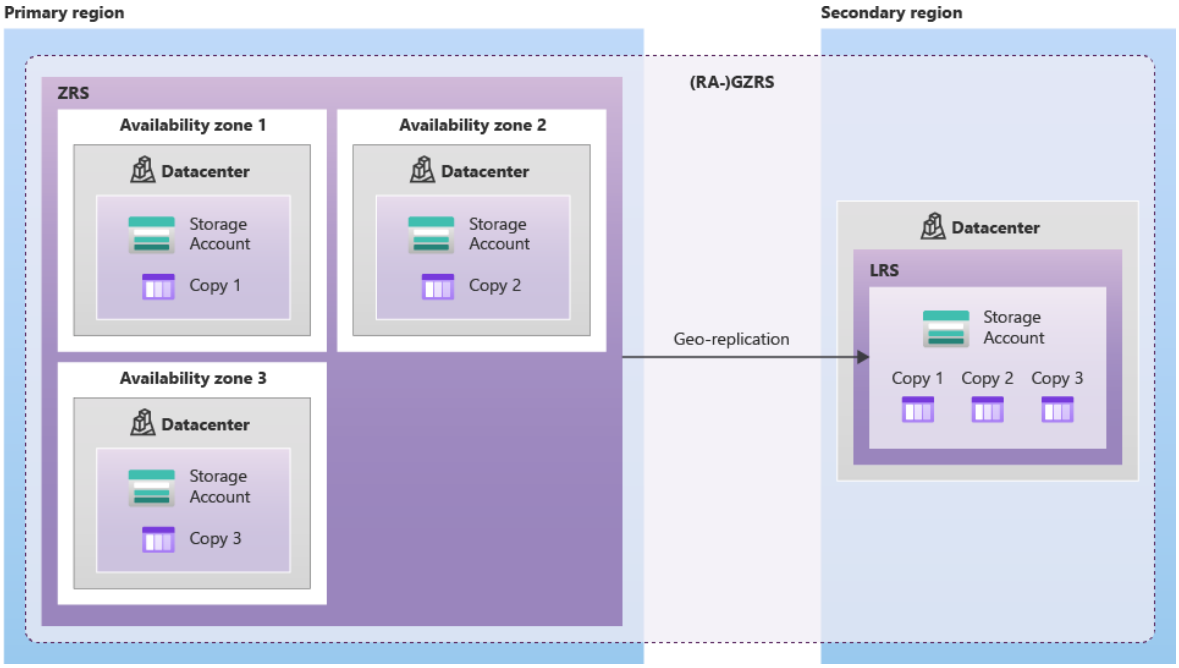
Figura 4. Disponibilidad nube redundancia por zonas



Fuente: MICROSOFT. [Sitio Web]. Redundancia de Azure. [Consultado el 01 de mayo de 2022]. Disponible en: https://docs.microsoft.com/es-es/azure/storage/common/storage-redundancy

Redundancia de regiones o geografía: este método de redundancia provista por la nube copia hasta tres veces los datos de forma sincrónica dentro de una misma ubicación física y luego copia de manera asincrónica los datos a ubicaciones que se encuentran a cientos y miles de kilómetros en otros centros de datos del proveedor de nube, esto permite una disponibilidad de 99,99999999999999 % (dieciséis nueves) durante un año. En la figura 5 se observa cómo es la réplica de almacenamiento entre diferentes regiones (Data Center) de un proveedor de nube.

Figura 5. Disponibilidad nube redundancia por región geográfica



Fuente: MICROSOFT. [Sitio Web]. Redundancia de Azure. [Consultado el 01 de mayo de 2022]. Disponible en: https://docs.microsoft.com/es-es/azure/storage/common/storage-redundancy

7.3 Seguridad

Sin duda uno de los aspectos más importantes para tener en cuenta en cualquier infraestructura es la seguridad de la información, hay aspectos importantes que se deben tener en cuenta al momento de analizar este apartado y es que la protección de datos a nivel de un centro de datos on premise se puede considerar en tres aspectos:

Sistemas informáticos: La información confidencial o sensible puede ser manipulada en un punto central como un servidor o un computador teniendo en cuenta los enlaces de comunicación o las terminales remotas que pueden acceder a él. Para todo el tema de la seguridad lógica en fundamental tener en cuenta dispositivos de seguridad y software que permitan controlar estos accesos, firewalls, enrutadores, herramientas de escaneo de vulnerabilidades y cumplimiento, todas estas herramientas deben considerarse al momento de asegurar infraestructura on premise, en cuanto a la seguridad física las consideraciones son a nivel de acceso a los Data Center, se requiere vigilancia 7x24 , cámaras de seguridad, personal de

vigilancia, controles biométricos, sistemas de detección y prevención de incendios y otros factores que puedan afectar la seguridad física de los elementos tecnológicos y por ende la información y los sistemas.

Cifrado: El personal de TI debe proponer estrategias y herramientas para asegurar la confidencialidad de la información, se deben implementar sistemas que permitan que la información sea almacenada de manera segura, en caso de ser interceptada de alguna manera se debe dar parte de tranquilidad que no puede ser leída por personal no autorizado.

Privacidad: Es un punto importante donde se requiere que los centros de datos cuenten con fuertes sistemas de autenticación y autorización, la identidad del usuario que requiere acceder a la información es fundamental para su protección, en el mundo on premise existe herramientas como la Microsoft Active Directory y OpenLDAP, que permiten lograr este objetivo en gran medida, centralizando los usuarios y contraseñas en un protocolo LDAP (Lightweight Directory Access Protocol) que es un estándar internacional y muchos sistemas de información se pueden integrar con ellos, también se puede reforzar adquiriendo plataformas que permitan un control de identidades que se apoyan en estas herramientas antes mencionadas pero adicionan una capa de autorización basada en roles que permiten definir quién puede acceder a que. Todas estas tecnologías son implementables en los Data Center tradicionales, pero requieren de personal con conocimiento para ello y para su administración, además de los costes que le genera a la compañía en temas de inversión de infraestructura y mantenimiento anual.

Además, para garantizar un centro de datos con altos estándares en calidad en seguridad de la información, se debe incursionar en temas de las normas internacionales ISO 27000 que también generara costos y administración adicional para la empresa mantener estos estándares.[24]

Para la seguridad en la nube hibrida se deben tener en cuenta muchos aspectos similares, pero se le deben sumar los propios de la tecnología de nube, dado que una nube hibrida cuenta con un mix del mundo on premise y nube publica, se debe tener muchos de los aspectos antes mencionados en el mundo local, sistemas de autenticación y autorización, seguridad en centro de datos y especial cuidado en los temas de aseguramiento de la conectividad. La nube hibrida permite integrar estas tecnologías de seguridad locales con las propias de la nube, esta combinación se convierte en un fuerte aliado para el evitar el acceso a los recursos de nube de

[24] ESCUNTAR ESCOBAR, CYNTHYA LISBETH. [en línea]. estudio comparativo de centro de procesamiento de datos orientado hacia la mediana empresa. Tesis Ingeniera de Sistemas. pontificia universidad católica del ecuador,2018. [Consultado el 03 de abril de 2022]. Disponible en: http://repositorio.puce.edu.ec/handle/22000/16131

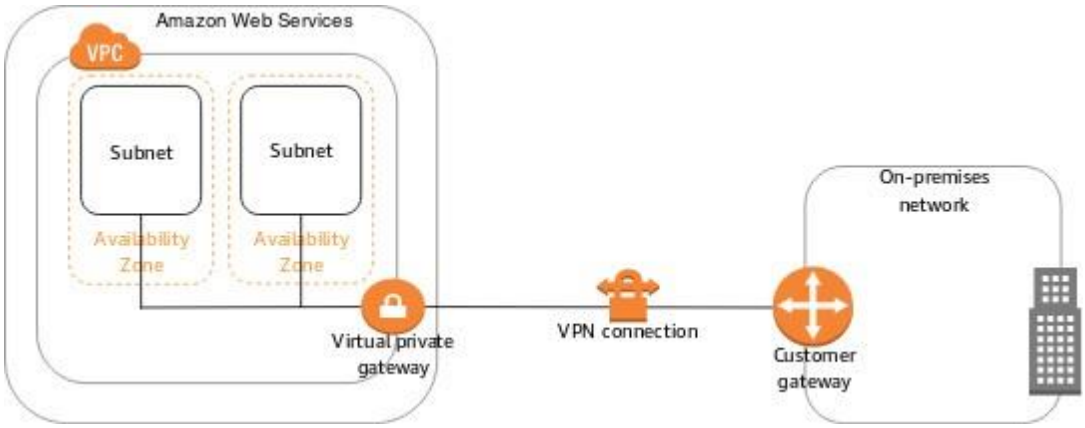
personal no autorizado y puede seguir siendo administrado desde las plataformas locales para una mayor tranquilidad por parte de las áreas de tecnología.

Los requisitos de seguridad en los que se debe pensar al momento de pensar en una nube ya sea hibrida o no, son: la identificación del usuario, la autorización para el acceso a los recursos, garantizar la integridad y confidencialidad de los datos, la disponibilidad y no repudio. En una nube cada servicio provee sus sistemas de autorización, ya sea PaaS, SaaS o IaaS y las nubes hibridas en particularmente son muy fuertes en este apartado, por ejemplo, Microsoft Active Directory es básicamente un centro de autenticación de usuarios y contraseñas, todos los proveedores de nube cuentan con un sistema de integración para este servicio, Azure hace uso de una característica llamada AzureAD Connect que lo que permite es sincronizar de forma continua los usuarios y contraseñas desde el mundo on premise hacia su nube, a través de un canal seguro por HTTPS, con esta información alimenta su propio almacén de usuarios llamado Azure Active Directory, así cuando se requiere brindar acceso a un usuario a cualquier recurso de la nube, en su módulo de identidades (IAM) permitirá buscar usuarios dentro del dominio de la organización y asignarles el permiso respectivo, igualmente se podría dar acceso a alguien externo a la compañía pero ya son temas de gobierno, con estos métodos se garantiza la confidencialidad de la información y la empresa puede tener parte de tranquilidad ya que los usuarios tienen un único punto de administración que sería on premise y eliminar o deshabilitar un usuario allí automáticamente lo hará en la nube.

Los canales de comunicación juegan un papel importante en las nubes hibridas, ya que se debe pensar en una capa adicional para el transporte de la información, muchos recursos de la nube van a interactuar con el mundo on premise y hacerlo a través de internet no es una opción recomendada para la seguridad de la información, nativamente los servicios que se crean en la nube tienen accesos públicos, no quiere decir que cualquiera puede ver los datos, solo que teniendo las URL (Uniform Resource Locator) y los permisos adecuados podría accederse a través del internet, para una nube hibrida esto no es concebible, por ello los proveedores de nube ofrecen métodos de comunicación entre ambos mundos por medio de 2 servicios, VPN o MPLS privadas (Multiprotocol Label Switching), las VPN se forman desde los dispositivos locales como los firewall de las compañías creando una puerta de entrada, desde el proveedor de nube se pueden crear diferentes recursos de red que permiten crear otra puerta de acceso, VNET que es una red virtual que puede tener un segmento definido por el cliente, y luego crear un VPN Gateway ligado a esa VNET, cuando esta integración está dada, el proveedor de nube entrega información como la IP publica para registrarla en el firewall on premise y una key o llave para verificar que la comunicación se está realizando el cliente correcto, cuando se establece esta comunicación entre ambos

mundos, ya hay un canal cifrado que permitirá el trasporte de la información a través de el con un direccionamiento de la red corporativa y se podrán acceder a los recursos on premise y viceversa de manera segura. Una canal de MPLS privado pretende utilizar un proveedor de red o ISP local (Internet Service Provider) para que por medio de él se cree una red extendida hasta los centros de datos de los proveedores de nube, este método es más costoso, pero ofrece una mayor confiabilidad y disponibilidad de la información ya que se obtiene una alta redundancia ofrecida por el ISP y la nube, además la información puede viajar por canales de información más amplios y rápidos, con una latencia menor.[25] En la figura 6 se puede observar un diagrama de conectividad a través de una VPN sitio a sitio desde el proveedor de nube hacia el entorno on premise.

Figura 6. VPN nube hibrida

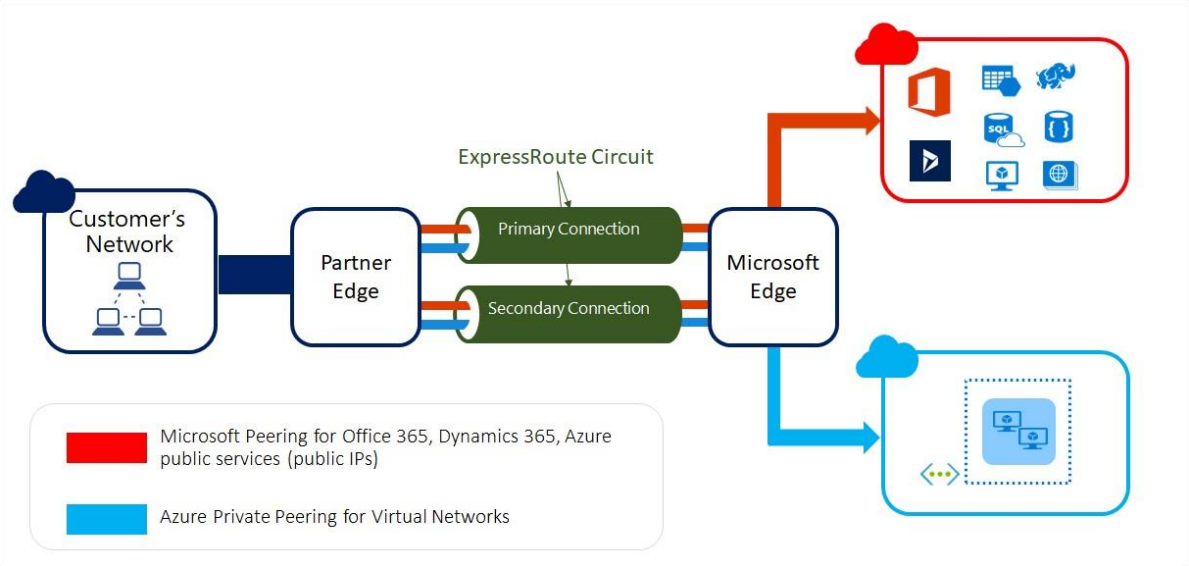


Fuente: AWS. [Sitio Web]. AWS Site-to-Site VPN. [Consultado el 01 de mayo de 2022]. Disponible en: https://docs.aws.amazon.com/vpn/latest/s2svpn/Examples.html

Igualmente, en la figura 7 se observa un esquema de alta disponibilidad por medio de dos canales MPLS desde un proveedor de nube hacia el proveedor de conectividad o ISP de los recursos on premise, a través de esta conexión se puede acceder a los recursos de manera rápida y segura, aun más que con la implementación de una VPN, esto debido a que se usan canales privados, aun así, el precio económico de este tipo de soluciones suele ser muy elevado.

[25] AWS. [Sitio Web]. AWS Site-to-Site VPN. [Consultado el 01 de mayo de 2022]. Disponible en: https://docs.aws.amazon.com/vpn/latest/s2svpn/Examples.html

Figura 7. MPLS nube hibrida.



Fuente: MICROSOFT AZURE. [Sitio Web]. What is Azure ExpressRoute?. [Consultado el 01 de mayo de 2022]. Disponible en: https://docs.microsoft.com/en-gb/azure/expressroute/expressroute-introduction

7.4 Escalabilidad

Los centros de datos tradicionales deben lidiar con los temas de crecimiento tecnológico y crecimiento vegetativo de los datos, para todas las empresas se convierte en un factor crítico la posibilidad de poder crecer y el tiempo que esto le puede tomar. Tradicionalmente las áreas de tecnología se deben apoyar en el proceso de compras para poder adquirir recursos, esto significa que deben planear con mucha antelación las actividades, migraciones o posibles requerimientos para así adquirir la infraestructura adecuada para suplir todas las necesidades posibles en todos los escenarios, sin embargo, ante eventualidades es muy difícil responder con aumentos de capacidad que el negocio requiera, para una correcta escalabilidad en un centro de datos on premise se deben tener lo factores:

- Planificar una capacidad inicial que permita cambios futuros a nivel de espacio físico, conectividad, almacenamiento y seguridad.
- El diseño implementado debe ser modular para que permita aumentar o disminuir de acuerdo con lo requerido, esto implica tiempos de adquisición y ventanas de mantenimiento.
- La tecnología adquirida debe permitir actualizaciones de hardware y software con un roadmap amplio en el tiempo.

El elemento de la escalabilidad es uno de los puntos más fuertes que tiene la nube hibrida , es prácticamente uno de los factores por la que tiene una razón de ser, dada la gran capacidad de cómputo que tiene la nube, permite crecer tanto horizontal como verticalmente en temas de tecnología, y lo hace de una manera muy rápida casi inmediata por lo que le puede proveer a una organización maximizar los límites de su infraestructura de cómputo on premise entregándole a la nube los temas más fuertes en cuanto a procesamiento y almacenamiento. La escalabilidad horizontal consiste en el crecimiento que puede tener una infraestructura a nivel de fuerza de cómputo como los son los servidores, la nube hibrida permite ir adicionando nodos en la medida que el sistema de información lo requiera y todo administrado por el cliente en tiempo real, también se puede automatizar de acuerdo a métricas configurables que determinen un estado actual de la plataforma y con base a esa información realice los incrementos, también se puede programar de acuerdo a tiempos establecidos, un banco por ejemplo podría ampliar su capacidad de cómputo programándolo solo para los días de pago de nómina. Igualmente sucede con el crecimiento vertical, este consiste en la capacidad que puede tener un nodo actual y su aumento de manera personalizada en cualquier momento que sea requerido.

Los temas de seguridad se benefician de este tipo de escalabilidad ofrecida por la nube, en un ambiente tradicional al tener servicios expuestos se debe considerar fuertemente la adquisición de equipos de protección contra amenazas que puedan mitigar o evitar ataques de ciberseguridad, si la organización se convierte en un blanco de ataque para algún grupo organizado ciber terrorista puede ocasionar eventos como la denegación de servicio. En 2020 Nokia dio a conocer algunas observaciones referentes a tendencias en DDoS (Denegación de Servicio Distribuido), como lo comenta Alberto Rios Osorio director comercial de Latinoamérica para Nokia, en el informe *Deepfield Network Intelligence Report: Networks in 2020 (Deepfield – Informe de inteligencia de redes). Se observa un aumento del 40 % en el tráfico de DDoS y un aumento en la cantidad de sitios afectados. El problema DDoS es real, la intensidad, sofisticación y volumen de los ataques está aumentando, con picos en el tráfico diario de DDoS que pasaron de 1,5 Tb/s en enero de 2020 a más de 3 Tb/s en mayo de 2021"*[26].

Debido a esto las arquitecturas de software deben tener un respaldo en temas de seguridad que permitan escalar de manera rápida, fácil y flexible, los servicios SaaS en la nube proveen diferentes tipos de elementos como firewalls, WAF o IDS, que

[26] Rios Osorio, Alberto. [en línea]. Cumpliendo con los retos de seguridad, escalabilidad e interconexión de redes de los centros de datos en la Nube. [Consultado el 01 de mayo de 2022]. Disponible en: https://www.datacenterdynamics.com/es/opinion/cumpliendo-con-los-retos-de-seguridad-escalabilidad-e-interconexi%C3%B3n-de-redes-de-los-centros-de-datos-en-la-nube/

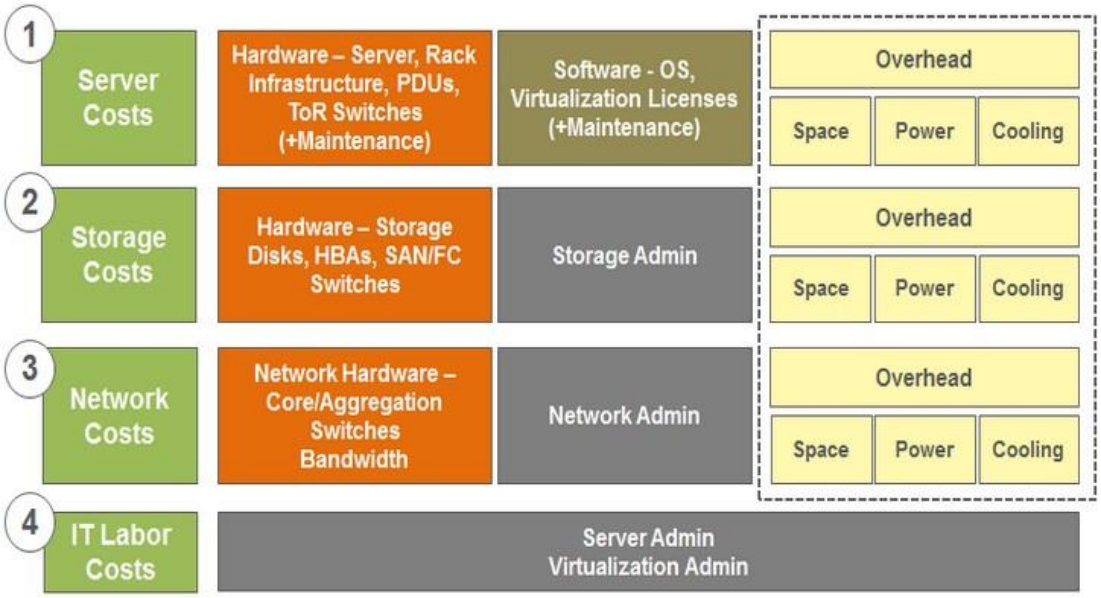
pueden implementarse para proteger los servicios expuestos ya sea en la nube o en on premise la nube hibrida permite lograr esto.

7.5 Costos

Un factor que puede determinar la viabilidad de un proyecto, implementación o adopción de una nueva tecnología son los costos, el precio debe estar acorde con las necesidades de la empresa y debe verse reflejado en algún tipo de retorno de inversión. En el mundo on premise adquirir un servidor genera muchos más costos que solo comprar un servidor, de hecho, se debe calcular minuciosamente el TCO (Total Cost of ownership), que equivaldría a la suma de Costos del Almacenamiento + Costos de los servicios de TI + los costos del elemento tecnológico adquirido + los costos de los servicios de red.

En la figura 8 se puede observar todos los servicios que se deben tener en cuenta al momento de realizar el análisis de costos para un nuevo servidor, donde se incluyen temas de almacenamiento, redes, energía, personal calificado, entre otros.

Figura 8. Elementos costeables on premise

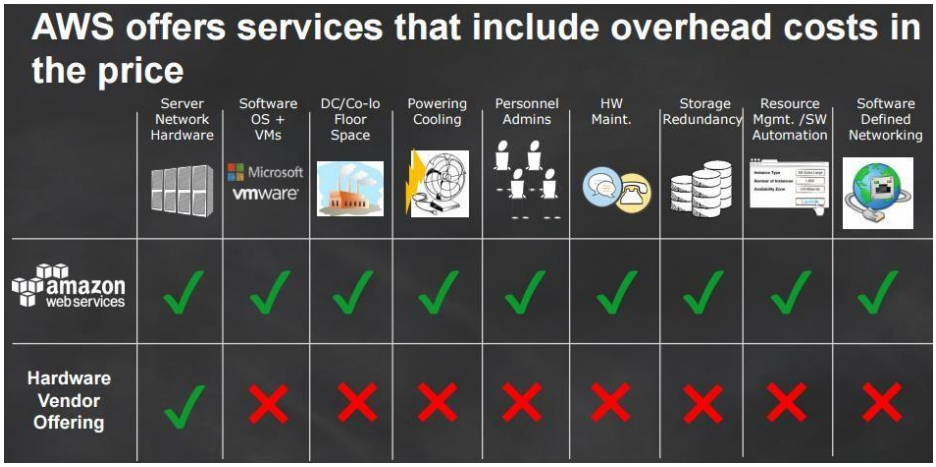


Fuente: ENGISOFT CLOUD SERVICES. [Sitio Web]. Roi En Cloud Y Total Cost Of Ownership. [Consultado el 01 de mayo de 2022]. Disponible en: https://www.engisoftcloud.com/roi-en-cloud-y-total-cost-of-ownership/

Se puede observar entonces que para la adquisición de un solo servidor se deben calcular temas de operación de TI, trafico generado en la red y uso de los dispositivos de networking (Switches, Patch Cord), almacenamiento (tipo de discos, cifrado, disponibilidad, SAN, fibras), energía UPS, refrigeración y licenciamiento.

Al tener esta información definida se puede, ahora sí, comparar los precios con la infraestructura de una nube, esto debido a que cuando se adquiere un elemento de la nube ya sea hibrida o publica, el valor cobrado por el proveedor ya tiene calculado todos esos elementos. En la figura 9 se pueden observar los elementos que se deben tener en cuenta al realizar una comparativa de costos entre servicios en nube y on premise, y como los proveedores de nube asumen muchos de estos.

Figura 9. Comparativa servicios incluidos en costos nube vs on premise



Fuente: ENGISOFT CLOUD SERVICES. [Sitio Web]. Roi En Cloud Y Total Cost Of Ownership. [Consultado el 01 de mayo de 2022]. Disponible en: https://www.engisoftcloud.com/roi-en-cloud-y-total-cost-of-ownership/

El pago por uso es la metodología usada por la nube hibrida, todos los servicios están disponibles para su uso , en el momento que se requiera acceder a ellos y usarlos se comienzan a generas los costosos asociados a ellos, no se requieren procesos de pagos complejos ni tiempos de espera, al aumentar la capacidad de los recursos o disminuirla, esto se verá reflejado en los costos mensuales generados por el proveedor de nube, se requiere entonces de un trabajo fuerte en el tema de gobierno para que tener una nube hibrida sea un método costo eficiente de evolución tecnológica, a continuación, en la tabla 5 se muestra una comparativa aproximada de un elemento de seguridad WAF en la nube vs un dispositivo F5 on premise.

Tabla 5. Comparativas características F5 - Application Gateway

Condición	F5 WAF Avanzado	Microsoft Azure Application Gateway
Pros	Las características varían de un cliente a otro. Algunos clientes están de acuerdo con las funciones básicas de WAF y otros usan WAF avanzado con algunas otras funciones.	Las características más valiosas de Microsoft Azure Application Gateway son las políticas, el almacén de datos que utilizan y la plataforma en la nube en la que opera.
	Se puede monitorear ubicaciones de IP, pero se tienen restricciones de cada país. Tiene una función de replicación. Las licencias se pueden compartir, turnándose con cada licencia.	Algunas de las características clave de esta solución son el mantenimiento de bajo nivel requerido, el servicio de proxy flotante y el equilibrio de carga.
	Muy fácil de implementar y funciona bien.	Las funciones de equilibrio de carga y firewall de aplicaciones web son las más valiosas
	Gran base de datos de firmas de ataque	la prueba de salud valida el backend para asegurarse que está comunicándose con el dispositivo correcto
	capacidades antivirus y de mitigación de DDoS	La función WAF replica el firewall y tiene características de mitigación DDoS
Cons	podría mejorar la precisión del escaneo. Hay muchos falsos positivos	Es un poco complicado de configurar. Mapear los certificados es un poco complejo
	La solución podría mejorar al tener un módulo de captura independiente. Tiene una función integrada que puede implementar la captura en su sitio web publicado. Sin embargo, no es muy fácil de usar.	la solución no admite ningún otro protocolo TCP además de HTTP y HTTPS.
	Difícil de escalar	Se debe mejorar la flexibilidad en opciones de configuración personalizadas

Continuación Tabla 5.

Condición	F5 WAF Avanzado	Microsoft Azure Application Gateway
Costos	Es más caro que otras soluciones y, dependiendo de los módulos, puede haber tarifas adicionales.	Es una solución económica de pago por uso
	F5 agrupa servicios y se paga un paquete completo en lugar de componentes individuales	No se requieren pagos de licenciamiento ni planes anuales
	Requiere pago por modelos de soporte anuales	subir la versión no requiere costos de implementación
		Hay incrementos de valor asociados con los niveles de soporte que se pueden adicionar al servicio

Fuente: Propia

Aunque los servicios en la nube siguen creciendo para intentar asumir los roles que prestan los dispositivos físicos de seguridad, aun se tienen limitantes al momento de la personalización que se puede requerir para cada organización, al intentar utilizar un servicio Cloud, se debe considerar cada una de las características que tiene a su disposición y realizar un cálculo de costo eficiencia para determinar cuál es la mejor solución.

8 JUSTIFICAR LA CONSTRUCCIÓN DE UN GOBIERNO PARA LA ADMINISTRACIÓN DE RECURSOS TECNOLÓGICOS EN UNA NUBE HIBRIDA, EXPLICANDO LAS DISCIPLINAS QUE SE DEBEN TENER EN CUENTA PARA SU ADOPCIÓN

A medida que las organizaciones deciden y comienzan a introducir componentes de tecnología nube en sus infraestructuras tecnológicas, se ven obligadas a extender sus marcos de referencia para poder adoptar los nuevos componentes que se empiezan a incluir en el gobierno de TI, las nuevas tecnologías de nube no solo traen nuevas oportunidades de crecimiento sino que también conllevan nuevos riesgos que tanto los proveedores de nube como las organizaciones deben tener presentes y evaluarlos estrechamente para poder maximizar el nivel de seguridad y compromiso que se tiene con la nuevas tecnologías.[27]

Para una organización que inicia el proceso de adopción de la tecnología de nube, es muy importante comenzar a gobernar y controlar todo lo que emerge allí, afortunadamente muchos de los procesos y marcos de referencia que aplican a los centros de datos on premise también tienen la capacidad de cubrir todos estos elementos nuevos, muchos de los principios de gobierno de TI encontrados en los marcos de ITIL y de NIST son aplicables a la nube y aún más cuando la nube elegida es hibrida y debe interactuar directamente con todos los recursos locales de la infraestructura de la organización. La gobernanza de la nube es un proceso continuo que requiere constantes revisiones y no se puede clasificar como un destino en el que solo se llega una vez y el proceso termina, al igual que en los procesos de TI locales, se debe tener una mejora continua y más aún dado que los proveedores de nube están en contante actualización de tecnología lo cual impacta directamente las aplicaciones, servicios, arquitecturas y diseños que se haya planteado una organización en las primeras fases de su inmersión hacia la nube. Tener una buena gobernanza permite crear barreras seguras que acompañan las organizaciones en todo su recorrido durante el proceso.[28]

Dado que la mejora continua es un elemento primordial de la gobernanza de TI en la nube, los requisitos de gobierno pueden cambiar continuamente, por lo cual se requiere de estrategias un poco diferentes a las tradicionales, tal vez esperar que un pequeño grupo de analistas de seguridad y continuidad establezcan unas

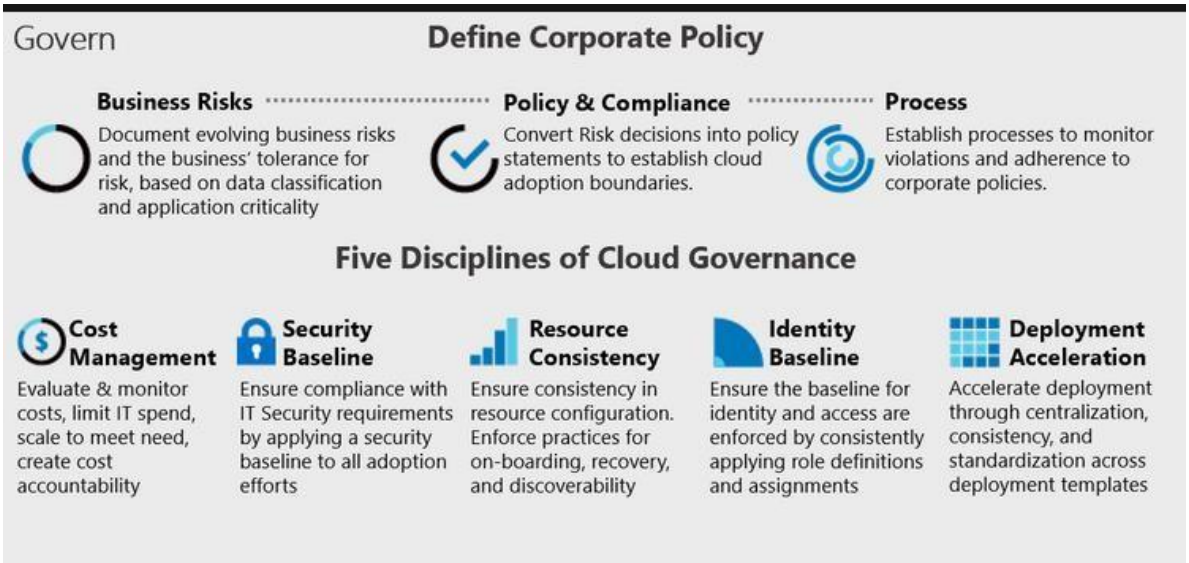
[27] BAEZA, TADEO ROBERTO. [en línea]. El cómputo en la nube como factor de competitividad en las empresas. Tesis Ingeniera de Sistemas. Universidad Juárez Autónoma de Tabasco,2019. [Consultado el 25 de septiembre de 2022]. Disponible en: https://www.academia.edu/31073353/Ensayo_de_C%C3%B3mputo_en_la_Nube_como_factor_de_competitividad_empresarial

[28] MICROSOFT IGNITE. [Sitio Web]. Gobernanza de la metodología para la nube. [Consultado el 25 de septiembre de 2022]. Disponible en: https://learn.microsoft.com/es-es/azure/cloud-adoption-framework/govern/methodology

políticas para el gobierno no sea la mejor opción ya que dada la velocidad de cambio de la nube, las empresas esperan que los resultados sean mucho más rápidos y dinámicos sin que se pierda en ningún momento la administración y seguridad de la nube.

Proveedores de tecnología en nube como Microsoft, Amazon y Google, trabajan a través de marcos de adopción conocidos como Cloud Adoption Framework en donde se manejan diferentes disciplinas para poder llegar a un término exitoso de su uso y gobierno, se proporcionan unas guías que permiten a las organizaciones a establecer rutas y procesos que generen valor y seguridad al momento de hacer la transición, la siguiente figura referencia como debería ser un resultado final del proceso.

Figura 10. Gobierno de TI en Nube



Fuente: MICROSOFT IGNITE. [Sitio Web]. Gobernanza de la metodología para la nube. [Consultado el 25 de septiembre de 2022]. Disponible en: https://learn.microsoft.com/es-es/azure/cloud-adoption-framework/govern/methodology

En este marco de referencia se muestra las diferentes líneas que se deben tener en cuenta al momento de evaluar los nuevos riesgos y oportunidades de mejora que permitirá una adopción y gobierno exitosas, todos los retos que presenten cada una de ellas deben ir resolviéndose, el gobierno de TI debe identificar las acciones

necesarias, con base al marco de referencia propuesto por los proveedores de Cloud, y así asegurar cada una de ellas.[29]

Con base en los framework de adopción de los proveedores de Cloud, se pueden generar un grupo de disciplinas que permiten a una organización poder determinar su estado de madurez frente a los nuevos retos que presenta un gobierno en la nube, todos ellos tienen asociados componentes que deben ser evaluados y que conllevan beneficios o riesgos de implementarlos o no.

La nube hibrida comienza a tener una gran acogida para muchas organizaciones, por lo que crear un buen gobierno genera madurez y aseguramiento en los recursos que se van a administrar, un ejemplo de ello serian las empresas de sector financiero, según Nutanix, que es una empresa marcada como líder en software de infraestructura por Gartner[30], las empresas prestadoras de servicios financieros deben de ser muy estrictas en el cumplimiento de estatutos gubernamentales y regulaciones con la protección de la información de sus bases de datos, es por eso que actualmente aproximadamente el 18% de estas compañías optaron por el modelo de nube hibridas y otro 51% esta en planes a mediano plazo para adoptar este tipo de nube[31], esto se debe a que muchas políticas de regulación obligan a estos sectores a no alojar la información crítica en ubicaciones de terceros, lo que supone un reto al momento de tomar decisiones, un buen gobierno debe permitir una gran flexibilidad de manipular o mover aplicaciones según su criticidad, unos muy buenos diseños de infraestructura que se adapten a la transformación digital y la seguridad como un elemento primordial para dar cumplimiento y regulación.

A continuación, se describen las disciplinas que se deben tener en cuenta para generar un buen gobierno.

8.1 ADMINISTRACION DE COSTOS

Aunque las nuevas tecnologías ofrecen resultados rápidos al menor costo posible, las opciones de pago por uso pueden ser un arma de doble filo al momento de administrar los costos de procesamiento y de datos, cada componente de la nube

[29] GOOGLE CLOUD. [Sitio Web]. The Google Cloud Adoption Framework. [Consultado el 25 de septiembre de 2022]. Disponible en: https://services.google.com/fh/files/misc/google_cloud_adoption_framework_whitepaper.pdf?hl=es

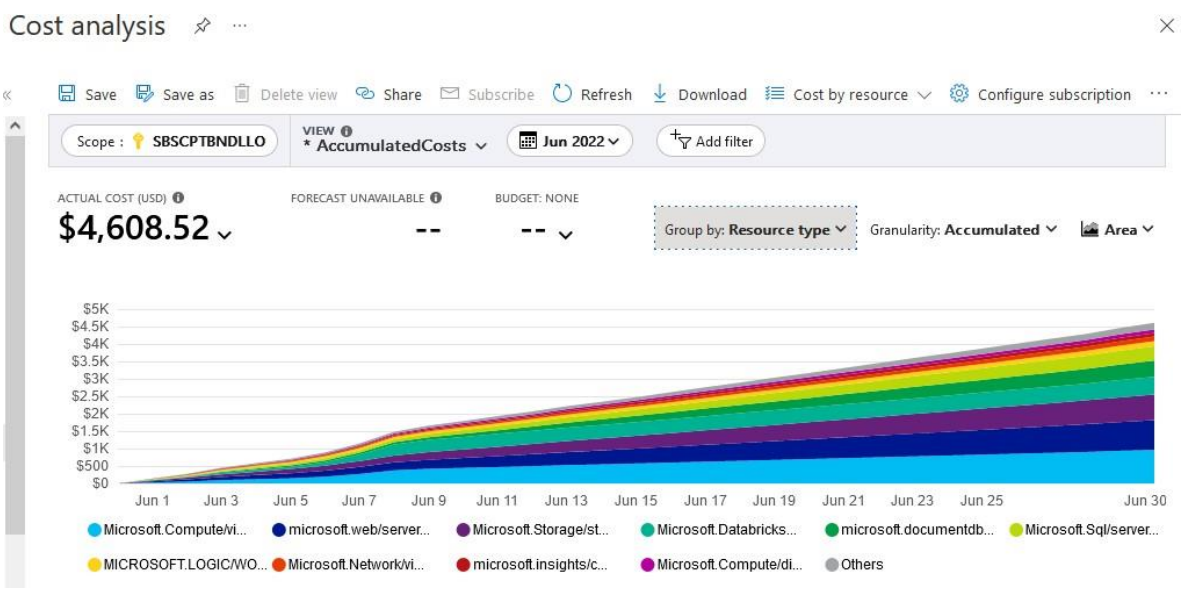
[30] GARTNER. [Sitio Web]. Nutanix Cloud Infrastructure Ratings. [Consultado el 25 de octubre de 2022]. Disponible en: https://www.gartner.com/reviews/market/hyperconverged-infrastructure-software/vendor/nutanix/product/nutanix-cloud-infrastructure

[31] NUTANIX. [Sitio Web]. Enterprise Cloud Index Nutanix. [Consultado el 25 de octubre de 2022]. Disponible en: https://www.nutanix.com/mx/viewer?type=pdf&lpurl=/mx/go/enterprise-cloud-index-for-financial-services&fromCampaign=true

tiene valores dependiendo del tipo de recurso y su funcionalidad, en muchas ocasiones las organizaciones caen en el error que el aprovisionamiento y el no uso de un elemento tendría un costo cero, pero dados los esfuerzos que el proveedor de nube debe realizar en ocasiones para reversar computo, puede comenzar a generar cobros por ello, la nube permite realzar cambios en los paradigmas tradicionales de costos fijos y comienza a reemplazarlos por gastos variables que deben ser cuidadosamente revisados antes de incursionar en algún proyecto, por ejemplo, si una empresa debe incursionar en un proyecto de analítica, debe estimar los costos de recursos como Databricks, este componente se basa en Apache Spark y se utiliza para todo lo relacionado con Big Data, al procesar allí modelos de información se comienzan a levantar capacidades de infraestructura virtual que apoyaran el tratado de esos modelos, se está hablando de memoria RAM y procesadores de alto rendimiento que comenzaran a convertir la información, al realizarse este proceso el proveedor de nube comienza a generar costos basados en estas capacidades y el tiempo en que tardan los modelos de datos en terminar su transformación, además de esto debe llevar los resultados a un DataLake o lago de datos que es el componente que se encarga de almacenarlos. Durante este recorrido se generaron muchos gastos asociados al cumplimiento del resultado final, cada proveedor de nube tiene una estimación de estos costos, pero se debe tener la capacidad de poder identificar cada uno de los elementos que intervienen en el flujo para poder calcular de manera asertiva el costo aproximado.

Tener un correcto gobierno y control de esta disciplina permitirá que la nube se convierta en un aliado costo eficiente, cada proveedor cuenta con un mecanismo fiable para determinar los costos generados por cada uno de los elementos, como se puede observar en la siguiente figura, Microsoft Azure puede determinar la métrica de consumo de cada componente por un periodo de tiempo determinado.

Figura 11. Resumen ejemplo de Costos Nube Microsoft

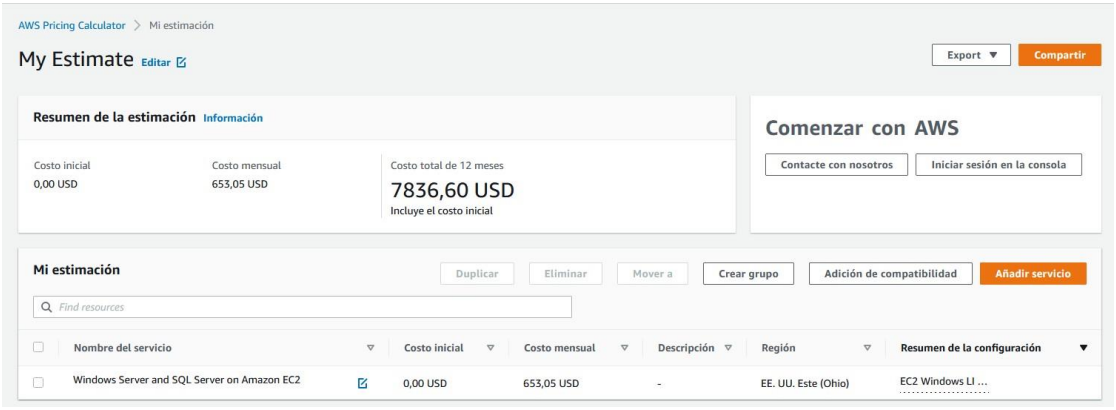


Fuente: Propia

Se puede inclusive llegar a un mejor detalle buscando un solo recurso en particular, una base de datos, un almacenamiento o una máquina virtual.

Al momento que la organización tiene una iniciativa, tiene a su alcance recursos que ofrecen los proveedores de nube para estimar estos costos, llamados calculadoras de precios, allí se puede acceder a todos los recursos que ofrece el proveedor de nube y generar un listado de componentes según la arquitectura diseñada para el nuevo proyecto, y así tener una valor aproximado de lo que costará alojarlo en la nube, la siguiente figura es un ejemplo de la plataforma de AWS (Amazon Web Services) donde puede observar el costo asociado a un servidor Windows Server con Microsoft SQL Server Instalado, el costo estimado contempla valores tanto de hardware como de software.

Figura 12. Calculadora Costos AWS



Fuente: AWS. [Sitio Web]. AWS Pricing Calculator. [Consultado el 25 de septiembre de 2022]. Disponible en: https://calculator.aws/#/estimate

El consumo de recursos en la nube debe regirse por lineamientos y políticas que se generen al interior de la compañía, en un ambiente hibrido se va a tener infraestructura local que debe reutilizarse para poder alcanzar el máximo beneficio, al crear estos diseños, se debe contemplar cuales son los recursos con los que cuenta la organización y definir en su estrategia cuales son los componentes que requieren estar en la nube.

Se comienza entonces a hablar de modelo operativo en donde se deben comenzar a gestionar tanto los recursos como las personas para que puedan estar en la capacidad de construir modelos económicos basados en la nube y que al conocer cada uno de los componentes que conforman una arquitectura hibrida puedan definir el mejor camino. Los ambientes híbridos permiten poder controlar, hoy en día, el estricto licenciamiento que pueden ofrecer algunos proveedores de software como IBM o SAP que son tan rigurosos con los temas de licencias por procesadores, memoria o disco, es por esto por lo que debe haber sinergias entre ambos ambientes y tener un correcto gobierno de cada uno de los recursos podrá permitir tomar mejores decisiones para manejo de los costos.

8.2 LINEA BASE DE SEGURIDAD

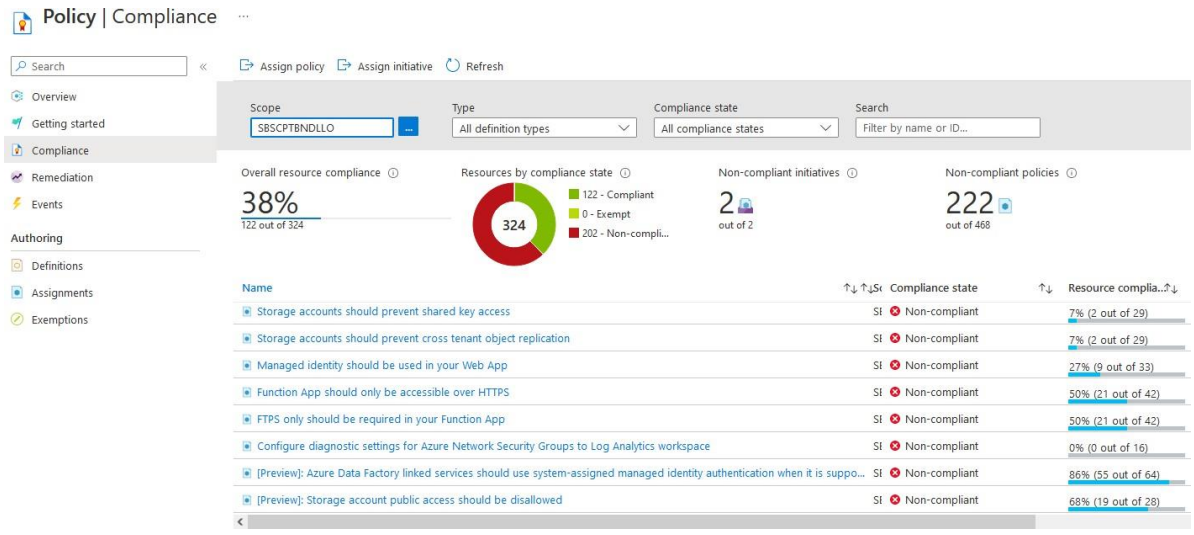
Uno de los temas más cruciales e importantes en el tema de Cloud es la seguridad, muchas de las organizaciones tienen como punto crítico esta categoría y de hecho es tal vez el principal motivo por el que tienden a crecer con cautela en los servicios de nube, definitivamente como parte de un buen gobierno de TI se encuentra la

aplicación de políticas de seguridad sobre todos los componentes, los modelos operativos de las empresas deben reforzar al personal para que asuma los nuevos retos, dado que muchos de los componentes que la nube ofrece se basan en tecnologías nuevas y su modo de operación también es nuevo. Una organización que ya tiene establecidas unas políticas de seguridad a nivel de plataformas on premise debe evolucionar y extender esas políticas para que puedan cubrir todo el entorno hibrido que ofrece la combinación de ambos ambientes.

Los proveedores de nube ofrecen varios mecanismos para tener un correcto control de la seguridad, tienen módulos de aplicación de políticas que ayudan a que sean aplicadas en el momento que se están creando los recursos, estas líneas base de seguridad facilitan el gobierno de TI sobre muchos elementos y permiten generar métricas de cumplimiento.

Proveedores como Amazon y Microsoft tienen mecanismos que permiten el cumplimiento de políticas para los recursos, entre ellas muchas relacionadas a temas de seguridad, AWS tiene el módulo llamado AWS Config y Microsoft tiene el suyo llamado Azure Policy cada uno de ellos permite llevar un control y monitoreo del cumplimiento de las políticas, como punto positivo de estos modulo es que se pueden configurar para que sean forzados y no solo para auditoria, lo que indica que al momento de crearse un recurso debe cumplir con las políticas dispuestas para él en caso contrario el sistema no permitirá su creación, en la siguiente figura se puede observar una lista de políticas que pueden implementarse del lado de la nube de Microsoft.

Figura 13. Azure Policy Compliance



Fuente: Propia

Allí se puede observar una métrica de cumplimiento en donde se puede realizar gestión a los recursos que cumplen o no con las políticas de seguridad, se encuentran entonces temas como forzar el protocolo HTTPS para todas las aplicaciones web, prevenir el uso público de cuentas de almacenamiento, tener un manejo de identidades para las aplicaciones web, entre muchas otras, generar una métrica de cumplimiento se puede basar en evaluar cuantos recursos se encuentran creados en la plataforma de nube y compararlos con la cantidad de ellos que están en cumplimiento de las políticas, además de estos recursos que proveen los proveedores, se deben tener políticas establecidas a nivel de organizaciones y documentarlas, también deben de realizarse auditorias periódicas para verificar el estricto cumplimiento de ellas.

El gobierno de TI debe visualizar la nube hibrida como una extensión de su Data Center local, y trasladar sus buenas prácticas y marco de trabajo a ese ambiente, por ejemplo, si la organización tiene como política interna que todas las bases de datos solo pueden ser accedidas a través de la red interna o VPN, crear bases de datos en la nube puede presentar un reto para el grupo de seguridad y de redes, nativamente los recursos de nube fueron diseñados para ser públicos, por lo que establecer políticas para ellos deben estar respaldadas por un equipo con conocimiento técnico que sea capaz de aplicarlas y dejar funcional el sistema, el concepto de VPC[32] (Virtual Private Cloud) o Virtual Private Endpoints, surge como opción a esas necesidades, donde muchos de los recursos de Cloud ya sea en modo IaaS, PaaS o SaaS, son capaces de tener una conexión directa hacia la red privada de nuestra organización y así poder acceder a ellas a través de la red interna así mismo esos recursos pueden acceder a los recursos on premise para compartir y transmitir información, ahí se va dando forma a la nube hibrida y va de la mano con las políticas de seguridad corporativas, para poder tener un buen gobierno y control se debe tener un inventario constante de los recursos que se tienen creados y realizarles un análisis de riesgos a cada uno para evaluar si están cumpliendo o no con las líneas de seguridad establecidas por el equipo de TI.

El área de TI puede apoyarse en cualquier marco de referencia como COBIT o la familia de normas ISO 27000 para apalancar sus líneas base de seguridad, inclusive los proveedores de Cloud se ven en la obligación de tener este tipo de certificaciones para poder prestar sus servicios, lo que indica que hay una estrecha relación entre la prestación de servicios, el gobierno y la seguridad, de hecho se pueden tomar varios controles de referencia que se pueden utilizar al momento de gestionar, analizar y evaluar la seguridad de los componentes que se tienen en la

[32] AWS. [Sitio Web]. AWS PrivateLink concepts. [Consultado el 25 de septiembre de 2022]. Disponible en: https://docs.aws.amazon.com/vpc/latest/privatelink/concepts.html

nube hibrida y que van de la mano con los estándares internacionales, inventario de hardware y software, administración continua de vulnerabilidades, uso de accesos con privilegios, análisis de logs de auditoría, defensa antimalware, administración de los puertos en los protocolos de red, procesos de recuperación de datos, a continuación, se puede observar algunos de los elementos que se pueden tener en cuenta para la correcta creación de una línea base de seguridad que abarque los elementos de nube y que son aplicables a un ambiente hibrido.

En la tabla 6 se puede observar el primer control a tener en cuenta, se debe administrar activamente que dispositivos o sistemas están autorizados por la organización para estar conectados a la red.

Tabla 6. Políticas de Seguridad y Control 1

Inventario Hardware y Software				**Aplicabilidad modelo de servicio**		
Tipo	**Función de Seguridad**	**Control**	**Descripción**	**IaaS**	**PaaS**	**SaaS**
Dispositivo/Aplicación	Identificar	Utilizar una herramienta de descubrimiento	Se debe realizar un escaneo de la red para identificar que componentes se encuentran dentro de la organización	X	X	
Dispositivo/Aplicación	Identificar	Mantener información de los dispositivos y aplicaciones	Asegurarse de que el inventario entregue información como el propietario, dirección IP y otros valores importantes	X	X	
Dispositivos	Responder	Remover dispositivos no autorizados	Cualquier dispositivo que no se encuentra autorizado debe ser bloqueado y removido de la red	X	X	
Dispositivos	Proteger	Utilizar certificados de cliente para autenticar dispositivos	Usar certificados de cliente para autenticar dispositivos de Hardware dentro de la organización	X		X
Aplicaciones	Proteger	Utilizar listas blancas de aplicaciones	Utilizar tecnologías que permitan definir qué tipo de aplicaciones son permitidas en la organización	X		

Fuente: CIS. (M2020). [Sitio Web]. CIS Controls Cloud Companion Guide. [Consultado el 03 de abril de 2022]. Disponible en: https://www.cisecurity.org/white-papers/cis-controls-cloud-companion-guide/

En la tabla 7 se observan políticas de control que están relacionadas a la gestión activa de vulnerabilidades, esto con el fin de poder minimizar y remediar cualquier acción de un atacante.

Tabla 7. Políticas de Seguridad y Control 2

Gestion de Vulnerabilidades				Aplicabilidad modelo de servicio		
Tipo	**Función de Seguridad**	**Control**	**Descripción**	**IaaS**	**PaaS**	**SaaS**
Aplicaciones	Detectar	Ejecutar escaneos programados de vulnerabilidades	se debe utilizar herramientas que permitan realizar automatización de análisis de vulnerabilidades y estén basadas en políticas de cumplimiento	X	X	
Aplicaciones	Proteger	Desplegar parches de seguridad de manera automática para sistemas operativos	Se debe contar con herramientas que permitan instalaciones periódicas de actualizaciones, además que permitan asegurar que los servicios prestados por el proveedor están al día en actualizaciones	X	X	
Aplicaciones	Proteger	Despliegue de actualizaciones para elementos de software	se debe tener un plan de actualización de parches y versiones para las aplicaciones en la organización, también que permitan identificar si la aplicación que entrega el proveedor está al día	X	X	
Aplicaciones	Responder	Comparar los resultados de los escaneos	Se debe realizar ocasionalmente una comparación de los resultados de los escaneos de vulnerabilidades con otros anteriores para determinar los cambios que ha habido	X	X	
Aplicaciones	Responder	Utilizar Rango de priorización	se debe tener una escala de priorización para la mitigación de los riesgos encontrados	X	X	

Fuente: CIS. (M2020). [Sitio Web]. CIS Controls Cloud Companion Guide. [Consultado el 03 de abril de 2022]. Disponible en: https://www.cisecurity.org/white-papers/cis-controls-cloud-companion-guide/

Se debe contar con procesos y herramientas que permitan identificar, prevenir o corregir el uso de cuentas con privilegios, tener este control en la línea base es indispensable, en la tabla 8 se observan algunos ejemplos.

Tabla 8. Políticas de Seguridad y Control 3

Usuarios de Accesos con Privilegios				Aplicabilidad modelo de servicio		
Tipo	**Función de Seguridad**	**Control**	**Descripción**	**IaaS**	**PaaS**	**SaaS**
Usuarios	Detectar	Mantener inventario de las cuentas administradoras	Se debe tener un sistema de inventario de usuarios con privilegios donde se almacenen sus claves de manera segura	X	X	X
Usuarios	Proteger	Cambiar contraseñas por defecto	Al momento de instalar una aplicación de terceros o cualquier sistema de información, se deben cambiar todas las contraseñas por defecto que traigan los usuarios	X	X	X
Usuarios	Proteger	Usar claves individuales	Si se tienen usuarios que no pueden tener múltiple factor de autenticación, se deben asignar claves únicas y complejas para cada uno	X	X	X
Usuarios	Proteger	Usar múltiple factor de autenticación para cuentas con privilegios	Todas las cuentas de usuarios administradores deben contar con un mecanismo de múltiple factor de autenticación para el acceso	X	X	X
Usuarios	Detectar	Tener Logs y alertas de acceso	se debe contar con un sistema de seguridad que permite almacenar información sobre la autenticación de los usuarios y generar alertas tempranas de irregularidades	X	X	X

Fuente: CIS. (M2020). [Sitio Web]. CIS Controls Cloud Companion Guide. [Consultado el 03 de abril de 2022]. Disponible en: https://www.cisecurity.org/white-papers/cis-controls-cloud-companion-guide/

Contar con una buena gestión y monitoreo de los logs y eventos ayudará a identificar de manera temprana cualquier anomalía que se presente en los sistemas de información, un atacante podría pasar desapercibido por mucho tiempo si no se tienen en cuenta políticas y controles como los que se pueden observar en la tabla 9.

Tabla 9. Políticas de Seguridad y Control 4

Monitoreo, Administracion y análisis de logs				Aplicabilidad modelo de servicio		
Tipo	**Función de Seguridad**	**Control**	**Descripción**	**IaaS**	**PaaS**	**SaaS**
Red	Detectar	Utilizar varios servidores de NTP	Se debe mantener al menos 3 orígenes de servicio horario para los dispositivos y servidores	X		
Red	Detectar	Activar los logs de auditoria	Se debe asegurar que todos los elementos tengan habilitados los eventos de auditoria tanto en sistemas como en equipos de red	X	X	
Red	Detectar	Almacenar los eventos	Se debe contar con un espacio de almacenamiento centralizado donde se puedan salvaguardar los logs generados por los sistemas	X	X	X
Red	Detectar	Analizar los logs	Se debe contar con un sistema de análisis de logs que permita identificar anomalías mediante correlaciones	X	X	X

Fuente: CIS. (M2020). [Sitio Web]. CIS Controls Cloud Companion Guide. [Consultado el 03 de abril de 2022]. Disponible en: https://www.cisecurity.org/white-papers/cis-controls-cloud-companion-guide/

Se deben tener fuertes controles para la defensa contra la propagación de software malicioso, sin importar el tipo de entorno de nube es una amenaza que siempre estará presente, algunos controles para la línea base se pueden observar en la tabla 10.

Tabla 10. Políticas de Seguridad y Control 5

Antimalware				Aplicabilidad modelo de servicio		
Tipo	**Función de Seguridad**	**Control**	**Descripción**	**Iaa S**	**Paa S**	**Saa S**
Dispositivos	Proteger	Utilizar un software de antivirus centralizado y actualizado	Se debe contar con una solución antimalware que permite la reacción temprana ante ataques y debe permanecer actualizada	X	X	
Dispositivos	Proteger	Centralizar los logs del antimalware	se debe enviar todos los eventos encontrados a un sistema centralizado que permita su análisis y la generación de alertas	X	X	
Red		Habilitar eventos para query de DNS	se debe habilitar el análisis de query DNS para identificar la búsqueda de nombres de dominios conocidos como maliciosos	X	X	

Fuente: CIS. (M2020). [Sitio Web]. CIS Controls Cloud Companion Guide. [Consultado el 03 de abril de 2022]. Disponible en: https://www.cisecurity.org/white-papers/cis-controls-cloud-companion-guide/

En la siguiente tabla se observan algunas políticas relacionadas con los protocolos de red que se pueden tener en cuenta en la línea base de seguridad, se enfocan básicamente en tener control sobre los puertos y servicios, una red que interconecta la nube con los ambientes on premise debe contar con sistemas de vigilancia e inspección de tráfico.

Tabla 11. Políticas de Seguridad y Control 6

Gestion de Protocolos de Red				Aplicabilidad modelo de servicio		
Tipo	**Función de Seguridad**	**Control**	**Descripción**	**Iaa S**	**Paa S**	**Saa S**
Dispositivos	Identificar	Asociar puertos activos con las aplicaciones	Se debe tener un inventario de las aplicaciones y los puertos y protocolos que usa para su ejecución	X	X	
Dispositivos	Proteger	Asegurar que solo los puertos y protocolos permitidos están en ejecución	Se debe asegurar que las aplicaciones están utilizando solo los puertos permitidos, se debe tener un sistema de firewall capaz de asegurar el proceso	X	X	X
Dispositivos	Detectar	Realizar escaneo de puertos	Se debe realizar con regularidad un escaneo de puertos sobre la red para identificar irregularidades de exposición	X	X	X
Dispositivos	Proteger	Implementar WAF	Se debe tener un sistema de aseguramiento para las aplicaciones que permita validar y analizar el tráfico que pasa a través de ellas	X	X	X

Fuente: CIS. (M2020). [Sitio Web]. CIS Controls Cloud Companion Guide. [Consultado el 03 de abril de 2022]. Disponible en: https://www.cisecurity.org/white-papers/cis-controls-cloud-companion-guide/

El punto de restablecimiento de la organización ante un desastre mayor se basa en sus sistemas de respaldo y recuperación, es indispensable contar con políticas que permitan fortalecer estas actividades en todos los ámbitos de cómputo, on premise y nube por igual, en la tabla 12 se pueden observar algunos elementos a tener en cuenta en la línea base de seguridad.

Tabla 12. Políticas de Seguridad y Control 7

Recuperación de Datos				Aplicabilidad modelo de servicio		
Tipo	**Función de Seguridad**	**Control**	**Descripción**	**IaaS**	**PaaS**	**SaaS**
Información	Proteger	Asegurar respaldos automatizados	Se debe tener todos los sistemas de información respaldados con herramientas automatizadas	X	X	X
Información	Proteger	Probar la integridad de los respaldos	Se debe realizar procesos de restauración controlados para determinar que los respaldos son íntegros y útiles	X	X	X
Información	Proteger	Proteger los respaldos	Se deben asegurar los respaldos en medios físicos o digitales que tengan cifrado	X	X	X

Fuente: CIS. (M2020). [Sitio Web]. CIS Controls Cloud Companion Guide. [Consultado el 03 de abril de 2022]. Disponible en: https://www.cisecurity.org/white-papers/cis-controls-cloud-companion-guide/

8.3 CONSISTENCIA DE RECURSOS

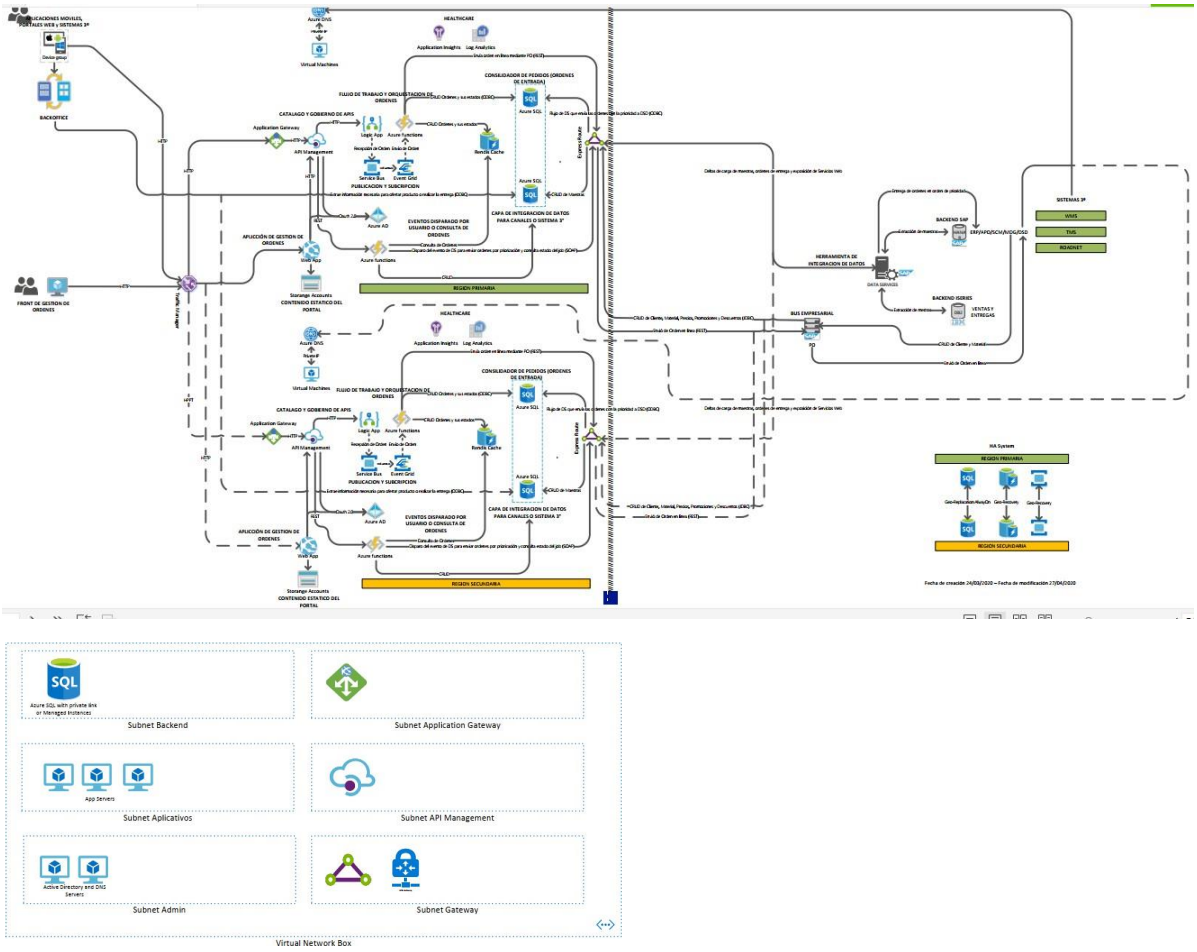
En los entornos tradicionales de cómputo se pueden encontrar diferentes tipos de sistemas de información los cuales son conformados por equipos de hardware y aplicaciones, cada uno de estos recursos suelen tener un manejo particular para su administración y seguridad, normalmente los arquitectos de TI deben poder tener la capacidad de generar diseños en los que haya una armonía entre el sistema que se requiere implementar y la infraestructura que lo precede, esto permite al equipo de TI poder responder de una manera eficiente ante cualquier eventualidad que se presente.

Cuando una organización decide adoptar la tecnología Cloud como parte de sus soluciones tecnológicas, se debe ser coherente con el mismo tipo de diseños, en un ambiente de nube hibrida, ésta se vuelve una extensión de los recursos tecnológicos

y los arquitectos y administradores de Cloud deben poder realizar la convergencia de estos dos mundos[33], para dar un ejemplo sobre como tener una consistencia de los recursos en un ambiente de nube hibrida se puede tomar la construcción de una aplicación web de pedidos.

Al pensar en la construcción de una aplicación se deben conocer los componentes que la conforman para poder elegir acertadamente los recursos de nube que se requieren, además si deben tener una interacciones con componentes onpremise es muy importante que también cumplan con características adicionales, la figura 14 muestra una arquitectura para componentes en la nube de Microsoft Azure.

Figura 14. Arquitectura Aplicación Nube Hibrida



Fuente: Propia

[33] ALQARNI,TURKI y BARNAWI, AHMED. (2019). A Cloud adoption framework: assessing the factors and determinants of adoption cloud computing technology. [En línea]. [Consultado el 02 de octubre de 2022]. Disponible en: https://www.mecsj.com/uplode/images/photo/A_Cloud_adoption_framework.pdf

La arquitectura propuesta en la figura anterior contiene una gran cantidad de componentes en la nube, permite el transito seguro de una aplicación pensada para la fuerza de ventas de una compañía y se puede observar que trabaja en alta disponibilidad para dos regiones geográficamente dispersas. La descripción del diseño en la arquitectura es el siguiente:

El pedido de un vendedor llega a través de su dispositivo móvil, éste es enviado al BackOffice y lo recibe un componente que permite realizar un balanceo de cargas por nombre DNS llamado Traffic manager, éste componente es capaz de tomar la decisión de cuál es el camino con mejor performance a nivel de latencia de red para redirigir la petición a una región o a otra, al hacerlo lo recibe otro componente llamado Application Gateway el cual tiene funciones de WAF y es capaz de analizar la petición web realizada por el dispositivo del vendedor y colocarle la primer capa de seguridad, el sistema está diseñado para exposición de API ’s por lo que se utiliza un componente llamado API Managment que es será el encargado de consolidar todas las API ‘s desarrolladas en un único punto de acceso y que puedan ser consumidas por la aplicación, el application Gateway traslada entonces la petición al Api Management para que pueda redireccionarlo al API que requiera según la solicitud de pedido, al interactuar con las API ‘s, éstas tienen toda la lógica del proceso y consiste en almacenar todas las peticiones en un Bus que posteriormente será entregado a una base de datos, el componente de Azure AD le permitirá a la aplicación tener un nivel de autenticación que está integrado con Directorio Activo el cual está siendo sincronizado con el directorio activo on premise a través del componente AzureAD Sync, las loggic app y evento Grid son componentes que permiten realizar ejecuciones programadas de ciertas tareas, en el caso del diseño que se presenta, se utilizan para estar llevando los pedidos que se almacenan en el service Bus a la base de datos cada cierto tiempo durante todo el día, para el tema de monitoreo y gestión de eventos se tienen los componentes llamados Application Insigth y Log Analytics Workspace donde se alojarán todos los eventos producidos por cada uno de los componentes de la solución, toda la conectividad de red se realiza a través de enlaces privados las bases de datos PaaS, las API ‘s y las aplicaciones web pueden trabajar de manera interna dejando como único punto de acceso público el traffic manager y el application Gateway, por lo que se puede crear una subnet para cada grupo de componentes y así se obtiene una correcta segmentación de redes, para terminar, se debe tener una estrecha comunicación con los componentes onpremise ya que son la fuente y destino final de la información, por medio de un componente llamado Express Route, se puede realizar una interconexión privada y dedicada hacia el Data Center on premise con lo cual ya se pueden acceder a los recursos de la organización como ERP y otros sistemas internos como el Directorio Activo y los DNS corporativos, ésta conexión permite que la información sea transportada de manera íntegra y segura de un lado a otro.

Es así entonces que tener una correcta lógica en la organización y creación de los recursos, permite que haya consistencia en ellos y al final se logra que todos los componentes de la solución en un entorno hibrido o en cualquiera, sean adecuadamente administrables y sustentables en el tiempo, genera que los incidentes de seguridad y operatividad puedan ser identificados de manera oportuna y se pueden extender las políticas entre ambos ambientes Cloud y Onpremise.

8.4 LINEA BASE DE IDENTIDAD

Uno de los aspectos más importantes en el momento de contemplar servicios Cloud es el tema de la identidad, el concepto de IAM (Identity and Access Management) toma mucha fuerza al momento de asegurar sistemas de nube públicas e hibridas. Cuando una organización decide que adoptará la nube hibrida como su nuevo esquema de trabajo, se generan preocupaciones como el hecho de que un mal manejo de la autenticación puede comprometer no solo sus recursos de nube si no también sus elementos onpremise ya que de alguna manera están interconectados, tener una gobernanza definida sobre los controles que se deben tomar para identificar el usuario o aplicación que va a interactuar con los recursos, es un punto clave para el éxito de la adopción de los sistemas Cloud[34].

Los sistemas de manejo de identidad son los principales responsables de almacenar, controlar y asegurar el manejo de credenciales de los componentes de una organización, éste debe ser extensivo a la nube para poder tener un control centralizado, para poder analizar lo que implica una gobernanza sobre las identidades, se deben evaluar varios aspectos, primero se deben tener claras las capas que componen los sistemas de identidad[35].

Gestion de Cuentas: Básicamente es el proceso de proporcionar una identidad a un usuario o una aplicación dentro de la organización independientemente de su rol, está definida por la información que pueda servir para identificar quien la está utilizando.

---

[34] HABIBA,UMME y MASOOD, RAHAT. Cloud identity management security issues & solutions. [En línea]. [Consultado el 02 de octubre de 2022]. Disponible en: https://link.springer.com/content/pdf/10.1186/s40294-014-0005-9.pdf

[35] ODUN,ISAAC y ABAYOMI, TEMIDAYO. (2019). Cloud Identity Management – A Critical Analysis. [En línea]. [Consultado el 02 de octubre de 2022]. Disponible en: https://www.researchgate.net/profile/Isaac-Odun-Ayo/publication/333402738_Cloud_Identity_Management_-_A_Critical_Analysis/links/5cebeb90458515026a5f48a9/Cloud-Identity-Management-A-Critical-Analysis.pdf

Autenticación: Una de las partes fundamentales es poder determinar que el usuario es quien dice ser, para esto se utilizan métodos como contraseñas, doble factor de autenticación, biometría u otros medios que permitan asegurar el proceso.

Autorización: En este punto se debe poder controlar los niveles de acceso que tiene el usuario en cualquier sistema de información, esto permite poder sesgar el uso e intromisión al sistema de información para que no se comprometa la privacidad o integridad de los datos.

Federación: Este elemento toma fuerza actualmente cuando las organizaciones están utilizando servicios Cloud, es posible generar accesos desde una organización a otra creando relaciones de confianza entre los sistemas de autenticación y la identidad de los usuarios puede romper los límites de estar solo dentro de la organización principal.

Auditoria: Se debe tener un sistema robusto de control que permita identificar oportunamente los eventos, así se puede obtener información de quien se encuentra en el sistema y que tareas puede estar ejecutando.

Para poder definir una línea base de identidad exitosa se deben conocer las diferentes categorías para los sistemas de identidad, una organización puede tener un sistema de autenticación principal, pero dada las circunstancias con sistemas de terceros, pueden aparecer sistemas que solo interactúan con ciertos tipo de autenticación, esto sucede en muchas ocasiones con servicios entre diferentes proveedores de nube o desarrollos propietarios, se tiene entonces las diferentes clasificaciones de sistemas de identidades[36].

IAM Aislado: Son utilizados por defecto por muchos sistemas de información donde es la aplicación quien maneja todo el tema de autenticación y autorización en un mismo servidor, se manejan diferentes usuarios y contraseñas, u otros métodos, para que sea validada la identidad del usuario, el inconveniente con este tipo de IAM es que se debe tener uno por servicio en la organización, lo cual hace demasiado engorroso el tema de gobierno.

IAM Centralizado: Comúnmente son los sistemas de autenticación más conocidos en las medianas y grandes empresas, consta de sistemas dedicados para el proceso de autenticación, en donde las aplicaciones se dirigen para consultar y validar el proceso de identificación de un usuario, existe un protocolo estandarizado

[36] ISHAQ AZHAR, MOHAMMED. CLOUD IDENTITY AND ACCESS MANAGEMENT – A MODEL PROPOSAL. [En línea]. [Consultado el 02 de octubre de 2022]. Disponible en: https://www.researchgate.net/profile/Ishaq-Azhar-Mohammed/publication/353887567_CLOUD_IDENTITY_AND_ACCESS_MANAGEMENT_-_A_MODEL_PROPOSAL/links/61169d070c2bfa282a41f553/CLOUD-IDENTITY-AND-ACCESS-MANAGEMENT-A-MODEL-PROPOSAL.pdf

para este tipo sistemas llamado LDAP (Lightweight Directory Access Protocol) el cual es muy usado por plataformas como OpenLDAP o Microsoft Active Directory, estos sistemas permiten tener un punto único de contacto para las aplicaciones y allí delegar el proceso de autenticación, una vez que suceda, la aplicación se encarga de administrar los niveles de autorización del usuario. Un IAM centralizado permite poder generar políticas de seguridad de acceso únicas para todos los sistemas de información, se puede generar una línea base para que sea mandatorio para toda la organización y así mitigar en gran medida los riesgos de acceso. Este sistema puede ser extendido desde el data center onpremise hacia los servicios de nube, la nube hibrida permite hacer uso de los sistemas de autenticación de la organización para que siempre haya un solo punto único de contacto, la nube asignará permisos de acceso a los recursos y los revocará en cuanto el usuario sea dado de baja del sistema de autenticación, esto asegura que haya un gobierno controlado de la identidad y los accesos.[37]

IAM Federados: Adoptar y aprovisionar servicios en la nube genera nuevos mecanismos de autenticación para poder intercambiar información de manera segura, se vuelve de vital importancia tener mecanismos por medio de los cuales se tenga un equilibrio en cuanto a seguridad y experiencia de usuario, así poder compartir y transmitir información entre aplicaciones de diferentes organizaciones[38], en una nube hibrida se puede realizar este tipo de federaciones entre los servicios Cloud y los servicios on premise.

Hay dos estándares de autenticación federada que se han vuelto muy populares en los temas de Cloud, OAuth y SAML.

SAML (Security Assertion Markup Language): Es un sistema que permite el intercambio de información en cuando temas de autenticación y autorización, está basado en el framework de XML y se define en dos condiciones para el transporte de la información Aserción y Carga del mensaje la cual asume tres roles esenciales en el uso de este sistema de IAM, proveedor de identidad que define a la organización que provee la información sobre el usuario, permite autenticar y autorizar y se encarga de entregar el token del usuario autenticado para que pueda continuar el proceso de acceso, luego se encuentra el proveedor de servicios quien

[37] ODUN,ISAAC y ABAYOMI, TEMIDAYO. (2019). Cloud Identity Management – A Critical Analysis. [En línea]. [Consultado el 02 de octubre de 2022]. Disponible en: https://www.researchgate.net/profile/Isaac-Odun-Ayo/publication/333402738_Cloud_Identity_Management_-_A_Critical_Analysis/links/5cebeb90458515026a5f48a9/Cloud-Identity-Management-A-Critical-Analysis.pdf

[38] NAIK, NITIN y JENKINS PAUL. Securing Digital Identities in the Cloud by Selecting an Apposite Federated Identity Management from SAML, OAuth and OpenID Connect. [En línea]. [Consultado el 02 de octubre de 2022]. Disponible en: https://pure.port.ac.uk/ws/portalfiles/portal/12189621/SAML_OAuth_and_OpenIDConnect_Naik.pdf

es el encargado de recibir el token y procesarlo de manera que se pueda generar el acceso a la aplicación y por último el usuario que es la entidad que inicia todo el proceso, no necesariamente debe ser un ser humano, también puede ser iniciada por un servicio o un API que requiera acceso.[39]La figura 15 muestra el flujo que sigue la autenticación realizada por SAML.

Figura 15. Autenticación y Autorización SAML

Fuente: NAIK, NITIN y JENKINS PAUL. Securing Digital Identities in the Cloud by Selecting an Apposite Federated Identity Management from SAML, OAuth and OpenID Connect. [En línea]. [Consultado el 02 de octubre de 2022]. Disponible en: https://pure.port.ac.uk/ws/portalfiles/portal/12189621/SAML_OAuth_and_OpenIDConnect_Naik.pdf

OAuth (Open Authorization): Es uno de los protocolos que se está usando con mayor fuerza en la actualidad, es un sistema de identidades flexible que permite delegar el sistema de autenticación a un sistema de terceros, que al final le proveerá un insumo en forma de token, que le permitirá a la aplicación poder confirmar su autenticidad y posteriormente definirle los roles y niveles de acceso a los que tiene derecho.

Oauth toma 4 roles clave para el proceso de acceso de un usuario, servidor de recursos (**SR**) que aloja los datos del usuario y que están protegidos por el sistema Oauth, propietario del recurso (**PR**), que es el usuario de la aplicación y quien tiene derecho de acceder a los datos, Oauth Consumidor/cliente (**OAC**), que es la aplicación encargada de realizar un requerimiento al API de autenticación para

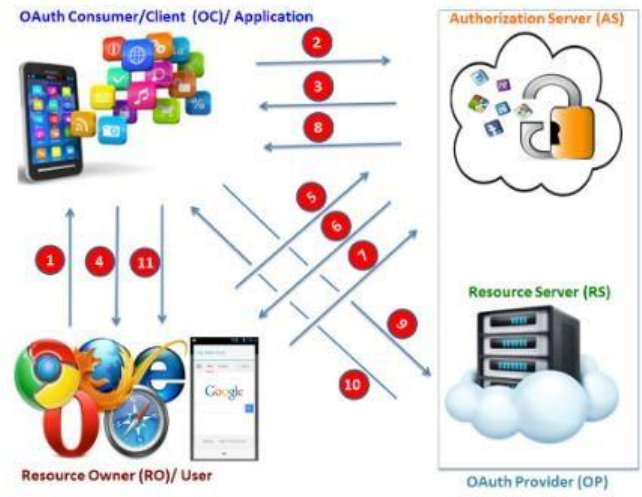
[39] NAIK, NITIN y JENKINS PAUL. Securing Digital Identities in the Cloud by Selecting an Apposite Federated Identity Management from SAML, OAuth and OpenID Connect. [En línea]. [Consultado el 02 de octubre de 2022]. Disponible en: https://pure.port.ac.uk/ws/portalfiles/portal/12189621/SAML_OAuth_and_OpenIDConnect_Naik.pdf

obtener el token con el titular de los datos, servidor de autorización (**SA**), que permite el acceso luego de haber recibido el token para finalizar el proceso[40].

En la siguiente figura se describe como seria el proceso de autenticación utilizando el método de Oauth en donde:

1. **PR** Inicio de sesión en la aplicación y solicitud de acceso desde una organización diferente
2. **OAC** Solicitud por un Token y una llave
3. **SA** Emite el Token
4. **OAC** envía una dirección URL HTTPS que contiene el token y las llaves del usuario y realiza la petición de acceso
5. **PR** Inicia sesión en el sistema con el token proporcionado
6. **SA** Consulta si el usuario está habilitado o no para el acceso
7. **PR** Autoriza el acceso a los recursos
8. **SA** Genera un token de acceso y redirige a OAC
9. **OAC** Envía el token de acceso y adquiere los recursos para el usuario
10. **SR** envía los recursos a OAC
11. **OAC** entrega los recursos al usuario

Figura 16. Autenticación y Autorización OAUTH



Fuente: NAIK, NITIN y JENKINS PAUL. Securing Digital Identities in the Cloud by Selecting an Apposite Federated Identity Management from SAML, OAuth and OpenID Connect. [En línea]. [Consultado el 02 de octubre de 2022]. Disponible en: https://pure.port.ac.uk/ws/portalfiles/portal/12189621/SAML_OAuth_and_OpenIDConnect_Naik.pdf

[40] NAIK, NITIN y JENKINS PAUL. Securing Digital Identities in the Cloud by Selecting an Apposite Federated Identity Management from SAML, OAuth and OpenID Connect. [En línea]. [Consultado el 02 de octubre de 2022]. Disponible en: https://pure.port.ac.uk/ws/portalfiles/portal/12189621/SAML_OAuth_and_OpenIDConnect_Naik.pdf

El diseño y arquitectura de aplicaciones seguras dependen de una muy buena estructura en la línea base de autenticación, todos estos métodos se pueden llevar a cabo en las infraestructuras y ambientes de nube hibrida, aumentan considerablemente la protección de acceso a las aplicaciones y permiten que disminuyan notablemente los riesgos en el proceso de adopción en la nube.

8.5 IMPLEMENTACION ACELERADA

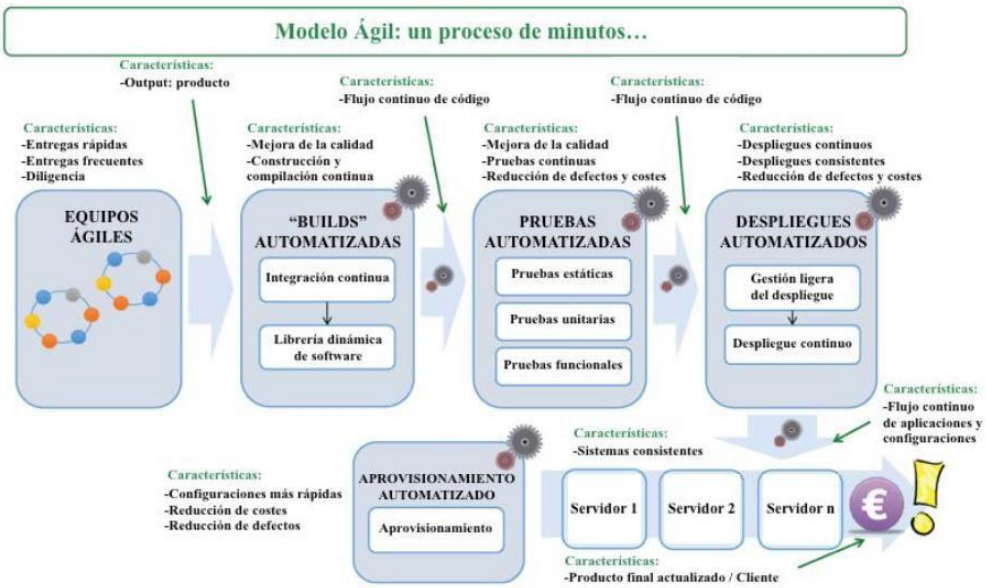
Las tecnologías Cloud permiten a las organizaciones a crecer de manera ágil pudiendo realizar implementaciones de manera rápida, la infraestructura como código es una de las características que todos los proveedores de nube ofrecen y es un método eficiente para realizar despliegues, una de las grandes diferencias entre el Cloud y los servicios Onpremise radica en este componente[41], y en una nube hibrida se deben contemplar todos los elementos que involucran una solución ya que puede alojar elementos de ambos lados, para obtener un gobierno completo de la infraestructura se deben tener herramientas capaces de generar flujos de aprobaciones y despliegues que culminen en el aprovisionamiento de una mejora o una funcionalidad nueva en determinado sistema de información, también servirá como medio para reducir el tiempo que toma la reconstrucción de un sistema ante una falla catastrófica como una recuperación ante desastres ya sea física o de seguridad. La organización debe contar con un modelo operativo y personal capacitado para poder generar esas nuevas habilidades organizativas, estructuralmente se debe tener un esquema que permita un control de cambios que cumpla con las necesidades requeridas, compuesto de personal que esté directamente implicado con el proceso y pueda tomar decisiones.

Acelerar los procesos de despliegue permiten que los cambios se puedan ver reflejados en el corto plazo y se puedan integrar mejoras de manera más oportuna, por ejemplo, si se encuentra una vulnerabilidad o un bug en algún sistema de información, los desarrolladores podrán tomar acciones rápidas y a través de un flujo en una aplicación diseñada para tema de DevOps, poder obtener aprobaciones y despliegues continuos, consiguiendo así reducir la brecha entre el hallazgo del problema y su solución. En los procesos de aprovisionamiento automatizado de infraestructura en la nube es muy relevante incurrir en metodología de desarrollo de software, todos los componentes que se encuentran en los proveedores de nube se

[41] SANCHEZ GOMEZ,CARLOS. [en línea]. Estudio de herramientas de despliegue continuo de aplicaciones, y sus ventajas competitivas en un mundo marcado por la agilidad. Grado Universitario en Ingeniería Informática. Universidad Carlos III de Madrid, 2020. [Consultado el 02 de octubre de 2022]. Disponible en: https://e-archivo.uc3m.es/bitstream/handle/10016/29802/TFG_Carlos_Sanchez_Gomez.pdf?sequence=1&isAllowed=y

puede crear a partir de líneas de código como si fuesen un software en desarrollo, a través de sistemas DevOps se pueden generar pipelines que permitan a los administradores de TI crear un ambiente a partir de una arquitectura en cuestión de unos minutos, para ello se deben tener unos estándares a nivel organizacional en tipos de recursos, estándares de nombramiento, capacidades y niveles básicos de acceso, esto permite que se puedan usar procesos como los modelos ágiles para administrar la nube. En la figura 17 se observa el proceso de un despliegue ágil al momento de realizar un desarrollo y su despliegue.

Figura 17. Despliegue Ágil de Infraestructura en la nube



Fuente: SANCHEZ GOMEZ,CARLOS. [en línea]. Estudio de herramientas de despliegue continuo de aplicaciones, y sus ventajas competitivas en un mundo marcado por la agilidad. Grado Universitario en Ingeniería Informática. Universidad Carlos III de Madrid, 2020. [Consultado el 02 de octubre de 2022]. Disponible en: https://e-archivo.uc3m.es/bitstream/handle/10016/29802/TFG_Carlos_Sanchez_Gomez.pdf?sequence=1&isAllowed=y

Dadas estas necesidades nacen también algunas aplicaciones que permiten lograr estos objetivos de despliegue acelerado en la nube, Terraform por ejemplo es un sistema diseñado para administrar y gobernar la infraestructura como código y se puede utilizar con diferentes proveedores de nube, permite mantener todo el diseño de una arquitectura almacenado para un despliegue o actualización rápida, no obstante las plantillas allí creadas deben estar en un constante mantenimiento, los

proveedores de nube van actualizando sus servicios e infraestructura, lo que implica que puede haber características deprecadas en el código que al utilizarse ya no estén disponibles para su ejecución, lo que generaría un error de despliegue[42].

Es un reto para el tema de gobierno de TI lograr alcanzar este nivel de madurez y normalmente las organizaciones dejan este componente de lado y se vuelve una deuda técnica en el largo plazo, si se adopta esta disciplina desde momentos tempranos de la adopción, será mucho más fácil poder responder frente a las necesidades de cada proyecto o iniciativa que se presenta.

[42] HUERLO QUINTERO,JURGEN RONALDO. [en línea]. TERRAFORM COMO HERRAMIENTA PARA AUTOMATIZAR LA CREACIÓN DE INFRAESTRUCTURAS SIGUIENDO EL CONCEPTO “INFRAESTRUCTURA COMO CÓDIGO". Tesis de Grado Ingeniería sistemas y computación. Universidad Católica del Ecuador, 2020. [Consultado el 02 de octubre de 2022]. Disponible en: https://repositorio.pucese.edu.ec/bitstream/123456789/2602/1/Huerlo%20Quintero%20Jurgen%20Ronaldo.pdf

9 CONCLUSIONES

Se logró establecer un entendimiento sobre el concepto de nube y de los diferentes modelos que se pueden encontrar allí, nube pública, nube privada y nube hibrida, explicando sus componentes y características al definir los elementos más relevantes como capacidades, disponibilidad, conectividad y elementos de seguridad que pueden encontrarse en cada una de ellas, también se determinaron, con base a la explicación dada, cuáles son los casos o necesidades en los que aplica cada modelo de nube, se realizaron comparaciones sobre sus ventajas y desventajas.

Se comparó los esquemas tradicionales de cómputo y los nuevos servicios de nube, se pudo determinar que los componentes de cada uno tienen grandes diferencias en cuanto a su administración y diseño, evidenciando que la tecnología de nube tiene unos beneficios adicionales en varios de los pilares más importantes que se compararon como la disponibilidad, escalabilidad y seguridad de la información, además, de acuerdo a lo expuesto, la empresas pueden generar más valor al realizar una convergencia de sus centros de datos con la nube, sacando el mayor provecho al crear un ambiente hibrido, esto se puede lograr dado que los proveedores de estas tecnologías ya están preparados para hacerlo.

Se demostró en el capítulo 8, la importancia de la creación de un buen gobierno para el manejo de la nube hibrida, detallando cada una de las disciplinas, líneas base de seguridad, consistencia de los recursos, costos, identidades e implementación, se explicaron diferentes modalidades de aseguramiento y control que se pueden llevar a cabo para controlar de manera eficiente la migración o expansión en la nube, como políticas de seguridad, métodos de autenticación y diseños de recursos para ambientes híbridos, mostrando como las organizaciones pueden tener una adopción controlada de estas tecnologías.

.

10 RECOMENDACIONES

Intentar abarcar un tema tan amplio como la tecnología en la nube siempre dejará ansias por más conocimiento, es un tema relativamente nuevo en el mercado en comparación con los esquemas tradicionales y por eso es importante recomendar que la documentación que se genere como este proyecto, se divulgue y se comparta para que más usuarios y organizaciones puedan romper con los paradigmas de la tecnología y la seguridad y puedan optar por darle una oportunidad a estos nuevos esquemas de servicios.

La seguridad informática es un tema que puede volverse complejo y generar temores al adoptar tecnologías como la nube, se recomienda abordar más técnicamente los temas de redes y conectividad que pueden envolver una solución de nube hibrida ya que se convierte en un factor importante para el éxito de una arquitectura digital.

Al adicionar nuevos procesos tecnológicos al catálogo de servicios de TI se deben activar mecanismos que permitan el gobierno y la administración de estos, se recomienda profundizar en estándares internacionales de la seguridad informática y como se adaptan a las nuevas tecnologías de nube, para poder integrarlos a TI y alinearlos con los objetivos estratégicos de la organización.

11 BIBLIOGRAFIA

ALQARNI,TURKI y BARNAWI, AHMED. (2019). A Cloud adoption framework: assessing the factors and determinants of adoption cloud computing technology. [En línea]. [Consultado el 02 de cotubre de 2022]. Disponible en: https://www.mecsj.com/uplode/images/photo/A_Cloud_adoption_framework.pdf

AWS.(2020).[Sitio Web]. Seguridad, identidad y conformidad de AWS. [Consultado el 03 de abril de 2022]. Disponible en: https://aws.amazon.com/es/products/security/?nc=sn&loc=2

AWS. [Sitio Web]. AWS PrivateLink concepts. [Consultado el 25 de septiembre de 2022]. Disponible en: https://docs.aws.amazon.com/vpc/latest/privatelink/concepts.html

BAEZA, TADEO ROBERTO. [en línea]. El cómputo en la nube como factor de competitividad en las empresas. Tesis Ingeniera de Sistemas. Universidad Juárez Autónoma de Tabasco,2019. [Consultado el 25 de septiembre de 2022]. Disponible en: https://www.academia.edu/31073353/Ensayo_de_C%C3%B3mputo_en_la_Nube_como_factor_de_competitividad_empresarial

BOROUFAR, AMIR. [en línea]. Software Delivery in Multi-Cloud Architecture. Tesis maestria en ingenieria informática. Politecnico Di Torino, 2020. [Consultado el 03 de abril de 2022]. Disponible en: https://webthesis.biblio.polito.it/16753/1/tesi.pdf

CCNCERT. (2019). [Sitio Web]. Decálogo de ciberseguridad. Madrid. [Consultado el 03 de abril de 2022]. Disponible en: https://www.ccn-cert.cni.es/documentos-publicos/1153-decalogo-de-ciberseguridad/file.html

CIS . (M2020). [Sitio Web]. CIS Controls Cloud Companion Guide. [Consultado el 03 de abril de 2022]. Disponible en: https://www.cisecurity.org/white-papers/cis-controls-cloud-companion-guide/

DÍAZ ARIZA, WILSON DANIEL. [en línea]. computación en la nube y su seguridad. [Consultado el 03 de abril de 2022]. Disponible en: http://repository.unipiloto.edu.co/handle/20.500.12277/2785

DIEZ HUERTAS,LUCAS. [en línea]. arquitectura y diseño de seguridad de aplicaciones en la nube pública. Tesis Maestria en Seguridad de las Tecnologías de la Información y de las Comunicaciones. UOC, Repositorio Institucional Universitat Oberta de Catalunya, 2020. [Consultado el 03 de abril de 2022]. Disponible en: http://openaccess.uoc.edu/webapps/o2/handle/10609/118427

ESCUNTAR ESCOBAR, CYNTHYA LISBETH. [en línea].estudio comparativo de centro de procesamiento de datos orientado hacia la mediana empresa. Tesis Ingeniera de Sistemas. pontificia universidad católica del ecuador,2018.

[Consultado el 03 de abril de 2022]. Disponible en: http://repositorio.puce.edu.ec/handle/22000/16131

EVALUANDO CLOUD. (2020). [Sitio Web]. Modelos de servicios de Cloud computing. [Consultado el 03 de abril de 2022]. Disponible en: https://evaluandocloud.com/modelos-de-servicios-de-cloud-computing/

EVALUANDO CLOUD. (2020). [Sitio Web]. Tipos de Cloud. [Consultado el 03 de abril de 2022]. Disponible en: https://evaluandocloud.com/modelos-de-implementacion-del-cloud/

GARTNER. [Sitio Web]. IaaS, DaaS and PaaS to Witness Highest Spending Growth This Year. [Consultado el 25 de octubre de 2022]. Disponible en: https://www.gartner.com/en/newsroom/press-releases/2022-04-19-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-reach-nearly-500-billion-in-2022

GARTNER. [Sitio Web]. gartner forecasts worldwide public cloud revenue to grow 17.5 percent in 2019. [Consultado el 03 de abril de 2022]. Disponible en: https://www.gartner.com/en/newsroom/press-releases/2019-04-02-gartner-forecasts-worldwide-public-cloud-revenue-to-g

GARTNER. [Sitio Web]. Nutanix Cloud Infrastructure Ratings. [Consultado el 25 de octubre de 2022]. Disponible en: https://www.gartner.com/reviews/market/hyperconverged-infrastructure-software/vendor/nutanix/product/nutanix-cloud-infrastructure

GARTNER. [Sitio Web]. Security leaders can evaluate the emerging technologies on this Hype Cycle to secure cloud computing. [Consultado el 03 de abril de 2022]. Disponible en: https://www.gartner.com/smarterwithgartner/4-must-have-technologies-that-made-the-gartner-hype-cycle-for-cloud-security-2021

GARTNER. [Sitio Web]. Top Actions From Gartner Hype Cycle for Cloud Security, 2020. [Consultado el 03 de abril de 2022]. Disponible en: https://www.gartner.com/smarterwithgartner/top-actions-from-gartner-hype-cycle-for-cloud-security-2020

GOOGLE CLOUD.[Sitio Web]. ¿Qué es una nube híbrida?. [Consultado el 03 de abril de 2022]. Disponible en: https://cloud.google.com/learn/what-is-hybrid-cloud?hl=es

GOOGLE CLOUD. [Sitio Web]. The Google Cloud Adoption Framework. [Consultado el 25 de septiembre de 2022]. Disponible en: https://services.google.com/fh/files/misc/google_cloud_adoption_framework_white paper.pdf?hl=es

GONZÁLEZ REVELO, JUAN DAVID. [en línea]. Nube híbrida de almacenamiento para análisis de datos. Tesis Ingenieria Electrónica y de Telecomunicaciones. Universidad autónoma de occidente, 2018. [Consultado el 03 de abril de 2022].

Disponible en: https://red.uao.edu.co/bitstream/handle/10614/10605/T08247.pdf?sequence=5&isAllowed=y

GONZALES ZAMBRANO, ENRIQUE BANNER. [en línea]. Diseño de una arquitectura Cloud Híbrida para el despliegue del Portal de Operaciones en el área de SysOps de GTS en IBM del Perú. Tesis Ingeniería de Sistemas e Informática. Universidad Tecnologica del Perú, 2019. [Consultado el 03 de abril de 2022]. Disponible en: https://repositorio.utp.edu.pe/bitstream/handle/20.500.12867/2745/Enrique%20Gonzales_Trabajo%20de%20Investigacion_Bachiller_2019.pdf?sequence=1&isAllowed=y

HABIBA,UMME y MASOOD, RAHAT. Cloud identity management security issues & solutions. [En línea]. [Consultado el 02 de octubre de 2022]. Disponible en: https://link.springer.com/content/pdf/10.1186/s40294-014-0005-9.pdf

HUERLO QUINTERO,JURGEN RONALDO. [en línea]. TERRAFORM COMO HERRAMIENTA PARA AUTOMATIZAR LA CREACIÓN DE INFRAESTRUCTURAS SIGUIENDO EL CONCEPTO “INFRAESTRUCTURA COMO CÓDIGO". Tesis de Grado Ingeniería sistemas y computación. Universidad Católica del Ecuador, 2020. [Consultado el 02 de octubre de 2022]. Disponible en: https://repositorio.pucese.edu.ec/bitstream/123456789/2602/1/Huerlo%20Quintero%20Jurgen%20Ronaldo.pdf

HUTH, ALEXA y CEBULA, JAMES. The Basics of Cloud Computing. [En línea]. [Consultado el 03 de abril de 2022]. Disponible en: https://www.us-cert.gov/sites/default/files/publications/CloudComputingHuthCebula.pdf

IBM. [Sitio Web]. Nube híbrida: Lo mejor de todos los mundos. [Consultado el 03 de abril de 2022]. Disponible en: https://www.ibm.com/downloads/cas/ALVMO8PG

INCIBE. (s.f.). [Sitio Web]. Políticas de seguridad para la pyme: almacenamiento en la red corporativa. [Consultado el 03 de abril de 2022]. Disponible en: https://www.incibe.es/protege-tu-empresa/herramientas/politicas

INCIBE. (s.f.). [Sitio Web]. Servicios de seguridad en la nube SaaS. [Consultado el 03 de abril de 2022]. Disponible en: https://www.incibe.es/polo-tecnologico/estudios-informes

ISHAQ AZHAR, MOHAMMED. CLOUD IDENTITY AND ACCESS MANAGEMENT – A MODEL PROPOSAL. [En línea]. [Consultado el 02 de octubre de 2022]. Disponible en: https://www.researchgate.net/profile/Ishaq-Azhar-Mohammed/publication/353887567_CLOUD_IDENTITY_AND_ACCESS_MANAGEMENT_-_A_MODEL_PROPOSAL/links/61169d070c2bfa282a41f553/CLOUD-IDENTITY-AND-ACCESS-MANAGEMENT-A-MODEL-PROPOSAL.pdf

MICROSOFT. (2020). [Sitio Web]. Azure Security. [Consultado el 03 de abril de 2022]. Disponible en: https://azure.microsoft.com/en-us/product-categories/security/

MICROSOFT AZURE AD CONNECT. (2020). [Sitio Web]. Azure AD Connect. [Consultado el 03 de abril de 2022]. Disponible en: https://docs.microsoft.com/es-es/azure/active-directory/hybrid/whatis-azure-ad-connect

MICROSOFT AZURE AD. (2021). [Sitio Web]. Microsoft Azure AD DS. [Consultado el 03 de abril de 2022]. Disponible en: https://azure.microsoft.com/es-es/services/active-directory/

MICROSOFT HYBRID IDENTITY. (2019). [Sitio Web]. What is hybrid identity. [Consultado el 03 de abril de 2022]. Disponible en: https://docs.microsoft.com/en-us/azure/active-directory/hybrid/whatis-hybrid-identity

MICROSOFT IGNITE. [Sitio Web]. Gobernanza de la metodología para la nube. [Consultado el 25 de septiembre de 2022]. Disponible en: https://learn.microsoft.com/es-es/azure/cloud-adoption-framework/govern/methodology

MINGUILLÓN ROY, ANTONIO. (2020). [en línea]. Auditando en la nube (no en las nubes). [Consultado el 03 de abril de 2022]. Disponible en: https://www.contraloria.gob.cu/sites/default/files/documento/2020-10/Auditando%20en%20la%20nube%20%28no%20en%20las%20nubes%29.pdf

MINTIC. [Sitio Web]. Seguridad en la Nube. [Consultado el 03 de abril de 2022]. Disponible en: https://gobiernodigital.mintic.gov.co/692/articles-150518_G12_Seguridad_Nube.pdf

MORAIS, LENILDO. (2020). Computación en la Nube: Inversión y Valor Agregado. Pernambuco. [En línea]. [Consultado el 03 de abril de 2022]. Disponible en: https://www.computing.es/cloud/opinion/1115963046301/computacion-nube-inversion-y-valor-agregado.1.html

NAIK, NITIN y JENKINS PAUL. Securing Digital Identities in the Cloud by Selecting an Apposite Federated Identity Management from SAML, OAuth and OpenID Connect. [En línea]. [Consultado el 02 de octubre de 2022]. Disponible en: https://pure.port.ac.uk/ws/portalfiles/portal/12189621/SAML_OAuth_and_OpenIDConnect_Naik.pdf

NAZARENO MONTIEL, FRANK, GUEVARA ANDRADE, JOANNA Y BLACIO, GIUSEPPE. [en línea]. Estudio de Seguridades en la Nube. Tesis Ingenieria computación. Escuela superior politécnica del litoral, 2014. [Consultado el 03 de abril de 2022]. Disponible en: https://www.dspace.espol.edu.ec/handle/123456789/25268

NOLLE, TOM. Red como servicio: El núcleo para la conectividad de nube, [En línea]. [Consultado el 03 de abril de 2022]. Disponible en:

http://searchdatacenter.techtarget.com/es/cronica/Red-como-servicio-El-nucleo-para-la-conectividad-de-nube

NUTANIX. [Sitio Web]. Enterprise Cloud Index Nutanix. [Consultado el 25 de octubre de 2022]. Disponible en: https://www.nutanix.com/mx/viewer?type=pdf&lpurl=/mx/go/enterprise-cloud-index-for-financial-services&fromCampaign=true

ODUN,ISAAC y ABAYOMI, TEMIDAYO. (2019). Cloud Identity Management – A Critical Analysis. [En línea]. [Consultado el 02 de cotubre de 2022]. Disponible en: https://www.researchgate.net/profile/Isaac-Odun-Ayo/publication/333402738_Cloud_Identity_Management_-_A_Critical_Analysis/links/5cebeb90458515026a5f48a9/Cloud-Identity-Management-A-Critical-Analysis.pdf

OSORIO MONTOYA, JOSÉ ANTONIO. [en línea]. gestión de riesgo y seguridad en computación en la nube para pymes. Tesis Especialización en Seguridad Informática. Universidad Piloto de Colombia, 2018. [Consultado el 03 de abril de 2022]. Disponible en: http://repository.unipiloto.edu.co/handle/20.500.12277/8614

PANCHANA FLORES, JOFFRE E. [en línea]. Estudio teórico conceptual sobre la computación en la nube móvil. Tesis Maestría de Gestión Estratégica de Tecnologías de la Información. Universidad de Cuenca, 2017. [Consultado el 03 de abril de 2022]. Disponible en: https://www.dominiodelasciencias.com/ojs/index.php/es/article/download/630/699

PEÑAFIEL DILLON, PABLO FRANCISCO. [en línea]. estudio para la implementación de nubes híbridas. Tesis Ingeniera de Sistemas. pontificia universidad católica del ecuador,2018. [Consultado el 03 de abril de 2022]. Disponible en: http://repositorio.puce.edu.ec/bitstream/handle/22000/14628/Tesis%20Pablo%20Pe%c3%b1afiel.pdf?sequence=1&isAllowed=y

PEREZ ROJAS, CAMILO ANDRÉS. [en línea]. cloud computing como herramienta de apalancamiento e innovación en las empresas de Colombia. Tesis administración de empresas. universidad piloto de Colombia, 2020. [Consultado el 03 de abril de 2022]. Disponible en: http://repository.unipiloto.edu.co/handle/20.500.12277/9163

QUINTANAS RIEGO, CARLOS FERNANDO. [en línea]. transformación digital y nube híbrida. Tesis Ingeniera de Sistemas. Universidad Internacional de La Rioja,2021. [Consultado el 03 de abril de 2022]. Disponible en: https://reunir.unir.net/bitstream/handle/123456789/12022/Quintas%20Riego%2c%20Carlos-Fernando.pdf?sequence=1&isAllowed=y

RED HAT. [Sitio Web]. ¿Qué es la nube híbrida?. [Consultado el 03 de abril de 2022]. Disponible en: https://www.redhat.com/es/topics/cloud-computing/what-is-hybrid-cloud

RED HAT. [Sitio Web]. ¿Qué es la seguridad de la nube híbrida?. [Consultado el 03 de abril de 2022]. Disponible en: https://www.redhat.com/es/topics/security/what-is-hybrid-cloud-security

RED HAT. [Sitio Web]. Tipos de cloud computing. [Consultado el 03 de abril de 2022]. Disponible en: https://www.redhat.com/es/topics/cloud-computing/public-cloud-vs-private-cloud-and-hybrid-cloud

RUIZ IMBAT, GEOVANNY XAVIER. [en línea]. la nube para la empresa masiva de la ciudad de quito, con base en la norma iso/iec 27017. Tesis Maestria Telecomunicaciones. Universidad Técnica del Norte, 2021. [Consultado el 03 de abril de 2022]. Disponible en: http://repositorio.utn.edu.ec/handle/123456789/11673

SAN MARTIN, RICHARD MIGUEL y WU CHONG, JOSE ANTONIO. (2021). [en línea]. Arquitectura y casos de uso de nubes híbridas en entornos regulados. [Consultado el 03 de abril de 2022]. Disponible en: https://www.aulavirtualusmp.pe/ojs/index.php/rc/article/download/2206/2593

SANCHEZ GOMEZ,CARLOS. [en línea]. Estudio de herramientas de despliegue continuo de aplicaciones, y sus ventajas competitivas en un mundo marcado por la agilidad. Grado Universitario en Ingeniería Informática. Universidad Carlos III de Madrid, 2020. [Consultado el 02 de octubre de 2022]. Disponible en: https://e-archivo.uc3m.es/bitstream/handle/10016/29802/TFG_Carlos_Sanchez_Gomez.pdf?sequence=1&isAllowed=y

THE OPEN GROUP. [Sitio Web]. TOGAF. [Consultado el 03 de abril de 2022]. Disponible en: https://pubs.opengroup.org/architecture/togaf92-doc/arch/

UNIVERSIDAD POLITECNICA SALESIANA ECUADOR. [Sitio Web]. Implementación de comunicaciones unificadas en computación en la nube y redes hibridas. [Consultado el 03 de abril de 2022]. Disponible en: https://dspace.ups.edu.ec/handle/123456789/13567

UPTIMEINSTITUTE. [Sitio Web]. Sistema de clasificación Tier. [Consultado el 01 de mayo de 2022]. Disponible en: https://es.uptimeinstitute.com/tiers