



TIC



MGGTI.GE.ST.04 - Guía de computación en la nube 2.0

Ministerio de Tecnologías de la Información y las Comunicaciones

MGGTI



Carina Murcia Yela – Ministra de Tecnologías de la Información y las Comunicaciones
Giovanny Andrés López Cabezas - Viceministro de Transformación Digital
Lucy Elena Urón Rincón - Directora de Gobierno Digital
Lucy Estella Palacios Valoyes - Subdirectora de Estándares y Arquitectura de TI
Andrés M. Ruíz Gómez – Profesional Subdirección de Estándares y Arquitectura de TI
Olga Regina Garzón Pupo - Profesional Subdirección de Estándares y Arquitectura de TI
Nelson A. Pardo Moreno - Profesional Subdirección de Estándares y Arquitectura de TI
Jairo A. Riascos Muñoz – Contratista Subdirección de Estándares y Arquitectura de TI
Johan Barrios Rodgers – Club de Gobierno
Ana María Gutiérrez Urquijo – Club de Gobierno
Frederick Nicolai Ferro – Universidad Nacional Sede Medellín

Ministerio de Tecnologías de la Información y las Comunicaciones
Viceministerio de Transformación Digital
Dirección de Gobierno Digital

Versión	Observaciones
Versión 1 19/12/2025	Guía de computación en la nube 2.0 Empresarial en entidades públicas en Colombia

Comentarios, sugerencias o correcciones pueden ser enviadas al correo electrónico:
gobiernodigital@mintic.gov.co

Guía de computación en la nube 2.0
V 1.0

Este documento de la Dirección de Gobierno Digital se encuentra bajo una Licencia Creative Commons Atribución 4.0 Internacional



HISTORIA

VERSIÓN	FECHA	CAMBIOS INTRODUCIDOS
0.9	12/08/2017	Emisión de la guía para consulta pública.
1.0	15/05/2018	Ajustes a la guía por comentarios realizados por la industria y partes interesadas.
2.0	19/12/2025	Enfoque en cómo gobernar arquitecturas complejas (Multi-Cloud/Híbrida), FinOps y DevSecOps. Énfasis en Automatización y Medición: Se reafirman las 5 características NIST (Autoservicio, Elasticidad, etc.), pero se interpretan bajo el prisma de la automatización total (IaC), la transparencia y la medición (FinOps). Descripción de las capacidades básicas de cada modelo. Seguridad y Responsabilidad Compartida: Se detalla la responsabilidad estricta del gobierno en cada capa. Se priorizan los modelos PaaS y Serverless por su eficiencia y se incluye la adopción de Cloud Native. Valor Estratégico y FinOps: El enfoque pasa del ahorro a la Optimización de Valor (FinOps). Se añaden como beneficios clave el acceso a IA/ML, la Sostenibilidad (Green Cloud) y la Resiliencia Multi-Cloud. Mandato de Adopción y Multi-Cloud: El lineamiento MAE.LI.AT.04 del MRAE 3.0 [18] se actualiza como un mandato para Adoptar prioritariamente arquitecturas Híbridas y Multi-Cloud, reconociendo la necesidad de múltiples proveedores. Gobernanza Proactiva: Se detallan los pilares de la evaluación: FinOps (como eje de la gestión de costos), DevSecOps (como eje de la seguridad) y la Soberanía de Datos (como eje del cumplimiento normativo).



DERECHOS DE AUTOR

A menos que se indique de forma contraria, el copyright (traducido literalmente como derecho de copia y que, por lo general, comprende la parte patrimonial de los derechos de autor) del texto incluido en este documento es del Ministerio de Tecnologías de la Información y las Comunicaciones. Se puede reproducir gratuitamente en cualquier formato o medio sin requerir un permiso expreso para ello, bajo las siguientes condiciones:

El texto particular no se ha indicado como excluido y por lo tanto no puede ser copiado o distribuido.

- La copia no se hace con el fin de ser distribuida comercialmente.
- Los materiales se deben reproducir exactamente y no se deben utilizar en un contexto engañoso.
- Las copias serán acompañadas por las palabras "copiado/distribuido con permiso del Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia. Todos los derechos reservados".
- El título del documento debe ser incluido al ser reproducido como parte de otra publicación o servicio.

Si se desea copiar o distribuir el documento con otros propósitos, debe solicitar el permiso entrando en contacto con la Subdirección de Estándares y Arquitectura de TI del Ministerio de Tecnologías de la Información y las Comunicaciones de la República de Colombia.



Tabla de contenido

1.	INTRODUCCIÓN.....	8
1.1.	OBJETIVOS DE LA GUÍA.....	9
1.2.	ALCANCE DE LA GUÍA.....	9
1.3.	LINEAMIENTOS DEL MARCO DE REFERENCIA ASOCIADOS CON ESTA GUÍA	9
1.4.	TÉRMINOS Y DEFINICIONES.....	10
2.	COMPUTACIÓN EN LA NUBE	12
2.1.	DEFINICIÓN.....	12
2.2.	CARACTERÍSTICAS ESENCIALES.....	14
2.3.	ACTORES.....	15
2.4.	MODELOS DE SERVICIO	25
2.5.	MODELOS DE IMPLEMENTACIÓN.....	32
2.6.	BENEFICIOS DE IR A LA NUBE	35
3.	COMPUTACIÓN EN LA NUBE EN COLOMBIA.....	39
3.1.	CONTEXTO NORMATIVO	39
3.2.	ASPECTOS PARA CONSIDERAR A LA HORA DE IR A LA NUBE	40
4.	NUEVAS TECNOLOGÍAS Y ESTADO DEL ARTE	51
4.1.	LA INTELIGENCIA ARTIFICIAL (IA) SE CONVIERTE EN EL NÚCLEO	51
4.2.	EL AUGE DEL CLOUD NATIVO Y SERVERLESS.....	53
4.3.	EDGE COMPUTING Y BAJA LATENCIA.....	56
4.4.	ESTRATEGIAS MULTI-CLOUD E HÍBRIDAS	59
4.5.	ENFOQUE EN SEGURIDAD, CUMPLIMIENTO NORMATIVO Y FINOPS	61
4.6.	SOSTENIBILIDAD Y COMPUTACIÓN CUÁNTICA.....	64
5.	MITOS Y REALIDADES DE LA COMPUTACIÓN EN LA NUBE	67
5.1.	LA TRANSFORMACIÓN DEL GASTO	69
5.2.	LOS TRES PILARES DE FINOPS PARA EL SECTOR PÚBLICO.....	69
5.3.	ALINEACIÓN CON EL MRAE 3.0.....	71
6.	ASPECTOS LEGALES Y JURÍDICOS VIGENTES	71
6.1.	PRIORIZACIÓN DE LA NUBE (LEY 1955 DE 2019).....	71
6.2.	DIRECTRICES PRESIDENCIALES Y ESTÁNDARES DEL MINTIC (DIRECTIVA PRESIDENCIAL 03 DE 2021)	72



6.3.	EL MODELO DE RESPONSABILIDAD COMPARTIDA Y SEGURIDAD	72
6.4.	PROTECCIÓN DE DATOS PERSONALES (LEY 1581 DE 2012).....	72
6.5.	CONTRATACIÓN MEDIANTE AGREGACIÓN DE DEMANDA	72
6.6.	ALINEACIÓN CON EL MRAE 3.0.....	72
7.	BIBLIOGRAFÍA.....	73



Tabla de figuras

Figura 1 Características esenciales – NIST	15
Figura 2 Modelos de Servicios - NIST	16
Figura 3 Actividades principales de un Proveedor de la nube.....	20
Figura 4 Proveedor de nube – Orquestación del Servicio	21
Figura 5 Proveedor de nube – Administración del servicio en la nube.....	23
Figura 6 Modelos de servicio.....	25
Figura 7 Nube privada en sitio	32
Figura 8 Nube privada subcontratada	33
Figura 9 Nube comunitaria en sitio.....	34
Figura 10 Nube comunitaria subcontratada	34
Figura 11 Nube pública	35
Figura 12 Implementación convergencia de la Cloud Híbrida y Multi-Cloud.....	61
Figura 13 Ciclo de vida para FINOPS en la nube	70

Lista de tablas

Tabla 1 Actores de computación en la nube	17
Tabla 2 Actividades del consumidor y proveedor de la nube	18
Tabla 3 Viabilidad Técnica y Estrategia.....	42
Tabla 4 Gestión Económica y Optimización Continua.....	43
Tabla 5 Contratación y Adquisición	44
Tabla 6 Beneficios de Cloud Native	55
Tabla 7 Estrategia para adoptar Cloud Native	56
Tabla 8 Arquitectura Edge Cloud Mesh para Gobierno	58
Tabla 9 Mitos y realidades de la nube	69
Tabla 10 Aspectos financieros para tener en cuenta para migrar a la nube	69



1. INTRODUCCIÓN

Este documento contribuye a establecer definiciones y criterios actualizados para identificar si una persona, natural o jurídica, pública o privada, es un proveedor de servicios de computación en la nube. Asimismo, presenta las consideraciones avanzadas para tener en cuenta a la hora de contratar este tipo de servicios, enfocándose en la gobernanza, la seguridad de la información y la optimización financiera. Ofrece, además, una estructura que permitirá a los actores identificarse y determinar su rol dentro del ecosistema de la nube en constante evolución.

Con el fin de proporcionar criterios y definiciones en referencia a la computación en la nube para Colombia, el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) desarrolla y actualiza esta guía. Más allá de las características tradicionales (modelos de servicios e implementación IaaS, PaaS, SaaS), este documento incorpora los nuevos pilares de la nube moderna a 2025, incluyendo:

- **Arquitecturas Cloud Native:** Enfoque en contenedores (Kubernetes) y la computación sin servidor (Serverless).
- **Estrategias Distribuidas:** Consideraciones avanzadas para entornos Multi-Cloud e Híbridos complejos.
- **Nuevos Imperativos de Gobernanza:** Inclusión de FinOps (gestión financiera de la nube), DevSecOps (seguridad por diseño) y Sostenibilidad como criterios de evaluación esenciales.
- **Integración de IA/ML:** La nube como plataforma primordial para el desarrollo y despliegue de la Inteligencia Artificial.

En Colombia, los servicios de computación en la nube siguen gozando de beneficios tributarios (Ley 1819 de 2016) y el Marco de Referencia de Arquitectura Empresarial (MRAE) del Estado Colombiano refuerza el mandato de que las entidades públicas deben adoptar la nube como estrategia central de la infraestructura digital. [18] Esta directriz exige que el sector público vaya más allá de la simple evaluación, enfocándose en la gobernanza segura de arquitecturas Multi-Cloud e Híbridas para garantizar la soberanía de los datos, la resiliencia y la eficiencia en la atención de las necesidades de los grupos de interés. Es clave entender que el papel de la nube ha evolucionado de un centro de costo a un habilitador estratégico de la misión pública.

También hay que dejar claro que este documento mantiene su rol de orientación y no constituye una norma o especificación técnica de cumplimiento obligatorio. Su propósito es facilitar la contratación, impulsar la adopción responsable y ofrecer criterios claros para determinar la adecuada clasificación de los proveedores y la correcta implementación de los servicios de la nube bajo los estándares tecnológicos y de seguridad más recientes.



1.1. OBJETIVOS DE LA GUÍA

- Proveer a los interesados una orientación estratégica para entender y gobernar la nube moderna, enfocándose en la adopción de arquitecturas Cloud Native (contenedores, serverless) y la gestión de modelos distribuidos (Edge Computing, Multi-Cloud).
- Ofrecer una definición formal de computación en la nube, sus modelos de servicio (IaaS, PaaS, SaaS) y sus modelos de implementación (privada, pública, híbrida y comunitaria), que sirva como base técnica y legal para los Acuerdos Marco de TI y las políticas de adquisición del Estado.
- Presentar un marco integral de aspectos y criterios de evaluación al momento de adquirir, proveer o modernizar servicios en la nube. Esto incluye la priorización de:

Seguridad y Cumplimiento (DevSecOps): Garantizar la soberanía del dato y el modelo de Confianza Cero (Zero Trust).

Gobernanza Financiera (FinOps): Implementar estrategias de optimización de costos y gestión de la inversión en la nube.

Sostenibilidad: Considerar la eficiencia energética y el impacto ambiental en las decisiones de despliegue de infraestructura.

Capacidades Avanzadas: Evaluar la integración de servicios de Inteligencia Artificial (IA) y Machine Learning (ML) como motor de la innovación pública.

1.2. ALCANCE DE LA GUÍA

La presente guía, además de ofrecer definiciones fundamentales sobre el modelo de computación en la nube (incluyendo IaaS, PaaS y SaaS), busca que las organizaciones puedan identificarse o clasificarse con precisión dentro de la compleja red de actores y los modelos de servicios Multi-Cloud e Híbridos que dominan la tendencia actual. Así mismo, proporciona un conjunto de criterios avanzados y consideraciones estratégicas que deben ser evaluadas y tenidas en cuenta a la hora de adquirir este tipo de servicios, con un foco especial en la continuidad operativa, la responsabilidad fiscal y la innovación.

1.3. LINEAMIENTOS DEL MARCO DE REFERENCIA ASOCIADOS CON ESTA GUÍA

La presente guía apoya, facilita y profundiza el cumplimiento y la adopción del siguiente lineamiento del dominio de Servicios Tecnológicos, en línea con la versión más reciente del Marco de Referencia de Arquitectura Empresarial del Estado Colombiano (MRAE 3.0) [18]:

MAE.LI.AT.04 Arquitecturas de referencia de la entidad de la arquitectura tecnológica: Las entidades de la administración pública serán las responsables de definir y evolucionar las arquitecturas de referencia en lo referente a los componentes de



arquitectura tecnológica, con el propósito de orientar el diseño de cualquier arquitectura de solución bajo parámetros, patrones y atributos de calidad definidos por la entidad, teniendo en cuenta los principios de diseño de servicios digitales, los componentes estructurales y su comportamiento con otros subsistemas e interfaces, definidos en el Manual de Gobierno digital.

La Dirección de Tecnologías y Sistemas de la Información o quien haga de sus veces debe adoptar de manera prioritaria y estratégica la posibilidad de prestar o adquirir los Servicios Tecnológicos haciendo uso de arquitecturas de la Nube, abarcando las modalidades Pública, Privada, Híbrida y Multi-Cloud, para atender con agilidad, resiliencia y eficiencia (FinOps) las necesidades de los grupos de interés.

- **Mandato de Adopción (Cloud-First Mandate):** La nube ya no es una opción a "evaluar", sino la estrategia de infraestructura digital por defecto para la modernización de los sistemas del Estado.
- **Expansión del Modelo Híbrido/Multi-Cloud:** Se reconoce que la arquitectura óptima incluye a menudo una combinación de nube privada (para soberanía de datos) y múltiples nubes públicas (Multi-Cloud) para aprovechar las capacidades especializadas (IA, Serverless) y garantizar la resiliencia y la gestión de costos.
- **Gobernanza Integrada:** La adopción del lineamiento debe estar acompañada por la implementación de disciplinas clave como DevSecOps (para la seguridad continua) y FinOps (para la gestión eficiente del gasto operativo en la nube).

1.4. TÉRMINOS Y DEFINICIONES

- **Aprovisionamiento:** Capacidad de automatización bajo demanda (On-Demand) y escalabilidad de los servicios de la nube. Implica la capacidad de proporcionar, modificar o desmantelar recursos de infraestructura (cómputo, almacenamiento, red) de manera programática y en tiempo real, a menudo mediante el uso de Infraestructura como Código (IaC)."
- **Arquitectura de Referencia:** Diseño de alto nivel y guía estratégica utilizada como plantilla para la concepción de arquitecturas de solución más específicas. Incluye principios de diseño que guían decisiones clave sobre plataformas Cloud Native, modelos Multi-Cloud/Híbridos, gobernanza (FinOps) y los requisitos de DevSecOps que deben respetarse. Es la base para la alineación tecnológica con el MRAE 3.0. [18]
- **Capa media:** En el contexto moderno, se refiere a los servicios de integración y conectividad que median entre la lógica de negocio y las capas inferiores. Incluye plataformas de API Gateway, Service Mesh (malla de servicios) para microservicios y servicios de message queuing o streaming que garantizan la comunicación y el tránsito seguro de información entre sistemas distribuidos. [2]
- **Centro de Datos:** Instalación física utilizada para alojar y mantener los sistemas de Tecnologías de la Información (TI). En el contexto de la nube, se



distingue entre Centros de Datos Tradicionales (on-premise) y los Centros de Datos Hiperescalares de los proveedores de nube, caracterizados por su alta densidad, eficiencia energética, extrema virtualización y alcance geográfico global. [15]

- **Cloud Native (Nativo de la Nube):** Metodología de desarrollo que aprovecha las ventajas inherentes del cloud computing. Las aplicaciones se diseñan utilizando microservicios, empaquetadas en contenedores y desplegadas dinámicamente con orquestadores (Kubernetes), utilizando pipelines de CI/CD para lograr agilidad, resiliencia y escalabilidad extrema.
- **Conexión dedicada:** Conexión privada y permanente que garantiza un ancho de banda fijo y predecible entre la infraestructura on-premise de una entidad gubernamental y la red de un proveedor de nube. Es fundamental para cargas de trabajo críticas que exigen baja latencia, alto rendimiento y cumplimiento riguroso de seguridad.
- **DevSecOps:** Extensión de la práctica DevOps que integra la seguridad en cada fase del ciclo de vida de desarrollo. Requiere automatizar herramientas de seguridad (escaneo de vulnerabilidades, gestión de secretos, revisión de políticas) dentro de los pipelines de CI/CD, asegurando la seguridad por diseño en las aplicaciones críticas del gobierno.
- **Edge Computing (Computación en el Borde):** Práctica de procesar y almacenar datos lo más cerca posible de la fuente de generación (dispositivos IoT, cámaras, sensores), en lugar de enviarlos a un centro de datos central. Es crucial para servicios públicos que requieren baja latencia y toma de decisiones en tiempo real (seguridad pública, tráfico inteligente).
- **Entorno de desarrollo integrados (IDE):** Herramientas de programación que combinan un editor de código, compilador, depurador y constructor de interfaz. La tendencia actual es el uso de IDEs Basados en la Nube (Cloud IDEs), que son accesibles vía web y se integran directamente con repositorios de código (Git), pipelines de CI/CD y plataformas de contenedores, facilitando el desarrollo colaborativo y el DevOps.
- **FinOps (Financial Operations):** Disciplina cultural que promueve la responsabilidad financiera en el uso de la nube a través de la colaboración entre los equipos de finanzas, tecnología y negocio. Su objetivo es optimizar continuamente el valor de la nube, mediante la visibilidad de costes, la presupuestación y la optimización del uso de recursos.
- **Implementación del servicio:** Todas las actividades automatizadas necesarias para configurar, desplegar y hacer disponible un servicio o una aplicación en el entorno de la nube. Este proceso se gestiona principalmente a través de Pipelines de Integración Continua y Despliegue Continuo (CI/CD) y la orquestación de contenedores, garantizando la velocidad, la fiabilidad y la reversibilidad del despliegue.
- **Incidente:** Cualquier evento no planificado que interrumpe o reduce la calidad de un servicio de TI. En la nube, la gestión de incidentes se apoya en la observabilidad avanzada (métricas, logs, trazas) y en la Inteligencia Artificial (AIOps) para correlacionar alertas, predecir fallas y automatizar la respuesta.



- **Interfaz:** Conexión funcional o punto de interacción entre dos sistemas, programas o componentes. En la nube moderna, las interfaces más comunes son las APIs (Interfaces de Programación de Aplicaciones), que permiten a los microservicios interactuar entre sí y son la base de los servicios gubernamentales que se integran con terceros.
- **Multi-Cloud (Nube Múltiple):** Estrategia de despliegue que utiliza servicios de múltiples proveedores de nube pública simultáneamente. Permite al gobierno mitigar el riesgo de vendor lock-in, aumentar la resiliencia (recuperación ante desastres) y seleccionar la mejor herramienta de cada proveedor para sus cargas de trabajo.
- **Serverless (Sin Servidor):** Modelo de PaaS (Plataforma como Servicio) donde el proveedor de la nube gestiona completamente la infraestructura de cómputo, permitiendo a los desarrolladores enfocarse solo en el código de las funciones. El usuario solo paga por el tiempo de ejecución exacto, siendo un pilar clave para la optimización de costos (FinOps) y la agilidad.
- **Soberanía de Datos:** Principio legal y político que estipula que los datos están sujetos a las leyes y regulaciones de la nación donde están almacenados o procesados. Para el gobierno, esto es un requisito fundamental que influye en la selección de las regiones geográficas de los proveedores de nube y en el uso de modelos de Nube Privada o Nube Híbrida.
- **Zero Trust (Confianza Cero):** Marco de seguridad que establece que ninguna persona, dispositivo o aplicación (dentro o fuera del perímetro) debe ser confiable por defecto. Todo intento de acceso debe ser verificado continuamente. Es el estándar de seguridad moderno para proteger los datos sensibles del gobierno en entornos distribuidos.

2. COMPUTACIÓN EN LA NUBE

2.1. DEFINICIÓN

No existe una definición aceptada universalmente; sin embargo, existen organismos internacionales cuyos objetivos son la estandarización de Tecnologías de la Información y, en particular, de computación en la nube (Cloud Computing en inglés). Uno de los organismos más reconocidos es el Instituto Nacional de Estándares y Tecnología (National Institute of Standards and Technology - NIST) que define la computación en la nube como:

“Es un modelo que permite el acceso ubicuo, adaptable, y por demanda en red a un conjunto compartido de recursos computacionales configurables (por ejemplo: redes, servidores, almacenamiento, aplicaciones y servicios) que se pueden aprovisionar y liberar rápidamente con un mínimo de esfuerzo de gestión o interacción del proveedor de servicios.” [3]

También existen otras definiciones, sin embargo, para el caso colombiano se acogió la definición del NIST 800 - 145 Y NIST – CSF 2.0. [17] Al analizar y detallar la definición es importante tener claridad de los siguientes conceptos:



- **Acceso adaptable:** Ya no se refiere solo a conveniente, sino a la capacidad de los servicios de la nube para ajustar dinámicamente sus interfaces y rendimiento a diferentes dispositivos, anchos de banda y necesidades específicas del consumidor. Implica una adaptabilidad programática para el consumidor (por ejemplo, mediante API, Interfaces de Línea de Comando o Consola Web).
- **Acceso bajo Demanda (On-Demand Self-Service):** La capacidad del consumidor de aprovisionar (contratar) y liberar unilateralmente y de forma automática recursos de cómputo (tiempo de servidor, almacenamiento, capacidad de red) sin requerir interacción humana con el proveedor de servicio de la nube. Es un pilar clave para la elasticidad y la eficiencia del modelo.
- **Acceso Ubicuo (Broad Network Access):** La capacidad de acceder a los servicios de la nube a través de mecanismos de red estándar (como internet) utilizando diversos dispositivos cliente, tanto fijos como móviles (teléfonos, tabletas, laptops). Es una de las cinco características esenciales que definen la nube según la NIST.
- **Aprovisionar:** En el ámbito de computación en la nube el aprovisionamiento es la acción de contratar, abastecer o asignar recursos computacionales durante un periodo de tiempo determinado. De igual manera estos recursos pueden ser liberados de acuerdo con la necesidad del usuario.
- **Aprovisionamiento Elástico Rápido (Rapid Elasticity):** Capacidad de los recursos de cómputo para ser aprovisionados, escalados y desescalados rápidamente, a menudo de forma automática e instantánea, para ajustarse a los cambios en la demanda. Para el consumidor, la capacidad disponible parece ser ilimitada y puede ser adquirida en cualquier momento y en cualquier cantidad.
- **Cloud Native (Nativo de la Nube):** Metodología de desarrollo de aplicaciones que utiliza los modelos de Serverless y Contenedores (Kubernetes) para aprovechar al máximo las capacidades de elasticidad, resiliencia y escalabilidad de la nube.
- **Computación en la Nube (Nube):** Modelo que permite el acceso ubicuo, conveniente y bajo demanda a un pool compartido de recursos de cómputo configurables (redes, servidores, almacenamiento, aplicaciones y servicios), que pueden ser rápidamente aprovisionados y liberados con un esfuerzo de gestión mínimo y con interacción mínima del proveedor de servicio." NIST SP 800-145.
- **Medición del Servicio (Measured Service):** Los sistemas de la nube controlan y optimizan automáticamente el uso de recursos, mediante la capacidad de medición de algún tipo de métrica (almacenamiento, procesamiento, ancho de banda, número de usuarios activos). El uso es transparente para el proveedor y el consumidor. Este pilar es la base para la adopción de la disciplina FinOps.
- **Nube:** El término nube viene del uso común del símbolo de una nube para referirse usualmente a Internet, Aunque no todo lo que está en internet es computación en la nube.



- **Serverless (Sin Servidor):** Modelo de PaaS donde el proveedor gestiona completamente la infraestructura, la asignación de recursos y el escalado. Los usuarios ejecutan código (Funciones como Servicio - FaaS) y solo pagan por el tiempo de cómputo consumido.

2.2. CARACTERÍSTICAS ESENCIALES

El modelo de computación en la nube, según NIST, se compone de cinco características esenciales, tres modelos de servicio y cuatro modelos de despliegue [3]. Las cinco características fundamentales que todo servicio de computación en la nube debe poseer son:

- **Autoservicio bajo demanda (On-demand self-service):** Esta característica se apalanca en la Infraestructura como Código (IaC). Las entidades de gobierno deben usar plataformas de aprovisionamiento automatizado y portales de servicios para garantizar que el autoservicio sea instantáneo, auditable y esté alineado con las políticas internas de FinOps (para controlar el gasto antes de aprovisionar).
- **Acceso amplio a la red (Broad network access):** El acceso amplio se extiende al concepto de Edge Computing. La nube no solo debe ser accesible desde dispositivos centrales, sino que debe permitir el procesamiento de datos y la inferencia de modelos de IA cerca del punto de interacción (el borde), utilizando redes de alta velocidad como el 5G para mantener el acceso y la latencia baja.
- **Conjunto común de recursos (Resource pooling):** Los recursos computacionales son puestos a disposición de los consumidores, los cuales comparten diferentes recursos físicos y virtuales asignados dinámicamente y por demanda. Ejemplos de recursos incluyen almacenamiento, procesamiento, memoria y ancho de banda. Esta característica es esencial para la eficiencia y sostenibilidad. La alta densidad de recursos compartidos (Multiplexación Estadística) es lo que permite las economías de escala y la reducción de la huella de carbono al maximizar la utilización de los servidores físicos. El MRAE 3.0 debe asegurar que la agrupación de recursos no comprometa el cumplimiento de la Soberanía de Datos ni los estrictos requisitos de aislamiento lógico requeridos para la información gubernamental. [18]
- **Rápida elasticidad (Rapid elasticity):** Los recursos proporcionados deben poder crecer o decrecer en cualquier momento, en algunos casos automáticamente, con el fin de escalar rápidamente y responder a la demanda de los usuarios. Esta capacidad se manifiesta en el auge de las arquitecturas Serverless y la orquestación de contenedores. La elasticidad debe ser instantánea y granular. Es la clave para que las entidades gubernamentales manejen grandes eventos (declaraciones fiscales o elecciones) de manera eficiente, pagando solo por el cómputo exacto utilizado.
- **Servicio medible (Measured service):** Los sistemas en la nube automáticamente controlan y optimizan el uso de los recursos dotándose de

capacidades para medir su rendimiento en un nivel de abstracción suficiente para la naturaleza del servicio proporcionado. Además, dicho control debe permitir ser monitoreado y reportado de manera transparente al proveedor del servicio y al consumidor. El Servicio Medible es el fundamento técnico de la disciplina FinOps. La transparencia de la medición es vital para que las agencias de gobierno puedan tomar decisiones informadas sobre la asignación de presupuestos, optimizar sus recursos y garantizar la responsabilidad fiscal en su gasto en la nube. Las métricas ya no se limitan al uso, sino que incluyen la observabilidad de rendimiento (AIOps) y, cada vez más, el impacto energético/ambiental.

2.3. ACTORES

Los actores según NIST, representan los participantes dentro del modelo de computación en la nube. Un actor puede ser una entidad, una persona o parte de una organización, que participa en una transacción o proceso y realiza tareas dentro del modelo de computación en la nube [4] [5]. Cabe aclarar que un mismo actor puede cumplir diferentes roles del modelo.

El siguiente diagrama representa una arquitectura de referencia de alto nivel y tiene por objeto facilitar la comprensión de los requisitos, usos, características y estándares de la computación en nube.

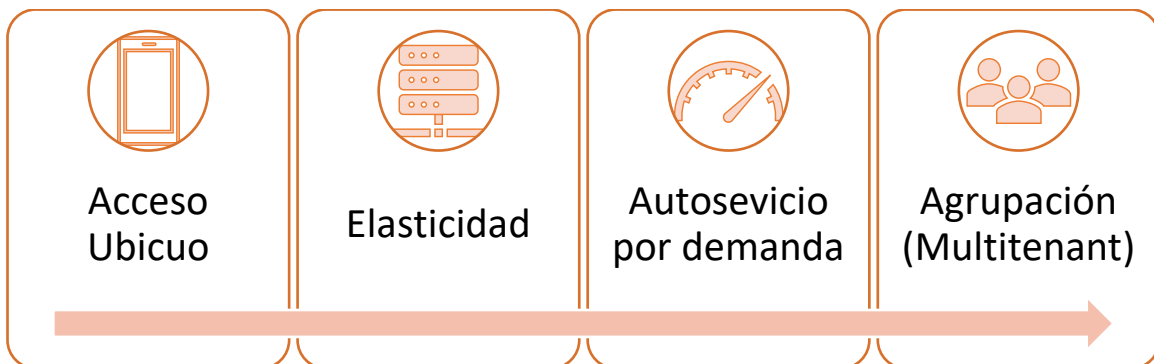


Figura 1 Características esenciales – NIST



Figura 2 Modelos de Servicios - NIST

Como se muestra en la Figura 1, la arquitectura de referencia del NIST para la computación en nube define cinco actores principales: consumidor de nube, proveedor de nube, auditor de nube, corredor o agente de nube y operador de nube. Cada actor es una persona natural o jurídica que participa en una transacción o proceso y/o realiza tareas en la computación en la nube. La Tabla 1 enumera brevemente los actores definidos en la arquitectura de referencia de computación en la nube propuesta por el NIST [4][5].

Actor	Definición
Consumidor de nube	Es el principal actor del servicio de computación en la nube. Un consumidor de nube representa a una persona u organización que mantiene una relación comercial y utiliza el servicio de un Proveedor de nube. El consumidor de nube consulta el catálogo de servicios de un proveedor de nube, solicita el servicio adecuado, establece contratos de nivel de servicio (ANS) con el proveedor de nube y utiliza el servicio. Puede elegir libremente un proveedor de nube con mejores precios y términos más favorables.
Proveedor de nube	Es el responsable de poner un servicio a disposición de las partes interesadas. Un proveedor de nube adquiere y gestiona la infraestructura informática necesaria para proporcionar los servicios, ejecuta el software en la nube que proporciona los servicios y hace lo necesario

Actor	Definición
	para entregar los servicios en la nube a los consumidores de nube a través del acceso a la red.
Auditor de nube	Este actor puede realizar una evaluación independiente de los servicios en la nube, las operaciones del sistema de información, el rendimiento y la seguridad de la implementación de la nube.
Corredor o agente de nube	Un corredor o agente de la nube gestiona el uso, el rendimiento y la prestación de servicios en la nube y negocia las relaciones entre los proveedores de nube y los consumidores de nube.
Operador de nube	Un operador de nube proporciona conectividad y transporte de servicios en la nube tanto a proveedores de nube como también podría hacerlo a los consumidores de nube.

Tabla 1 Actores de computación en la nube

2.3.1. Actividades del consumidor de nube

Dependiendo de los servicios solicitados, las actividades y escenarios de uso pueden ser diferentes entre los consumidores de nube como se muestra en la siguiente tabla [4][5]:

Modelos de servicio	Actividades del Consumidor	del	Actividades del Proveedor
SaaS (Software como servicio)	Usa la aplicación o los servicios para soportar procesos de negocio.		Instala, administra, mantiene y soporta la aplicación de software en una infraestructura de nube.
PaaS (Plataforma como servicio)	Desarrolla, prueba (testing), despliega y administra aplicaciones alojadas en un sistema de nube (Cloud).		Gestiona la infraestructura de cómputo de la plataforma y ejecuta el software de nube que proporciona los componentes de la plataforma como las bases de datos y otros componentes de capa media para el intercambio de información (middleware).
IaaS (Infraestructura como servicio)	Crea/instala, administra y monitorea los servicios operacionales de la infraestructura de TI.		Ejecuta el software de la nube necesario para que los recursos informáticos estén disponibles para el consumidor de nube



Modelos de servicio	Actividades del Consumidor	del	Actividades del Proveedor
			IaaS a través de un conjunto de interfaces de servicios y abstracciones de recursos de cómputo, como máquinas virtuales e interfaces de red virtual. El proveedor de nube IaaS tiene control sobre el software de nube que controla el hardware que hace posible el aprovisionamiento de estos servicios de infraestructura a los consumidores de nube.

Tabla 2 Actividades del consumidor y proveedor de la nube

Las aplicaciones SaaS se hacen accesibles a través de una red (usualmente Internet) a los consumidores SaaS. Los consumidores de SaaS pueden ser organizaciones que proporcionan a sus miembros acceso a aplicaciones de software, usuarios finales que utilizan directamente aplicaciones de software o administradores de aplicaciones de software que configuran aplicaciones para usuarios finales.

Los consumidores de SaaS pueden ser facturados en función del número de usuarios finales, el tiempo de uso, el ancho de banda consumido en la red, la cantidad de datos almacenados, la duración de los datos almacenados, entre otros.

Los consumidores de PaaS pueden emplear las herramientas y recursos de ejecución proporcionados por los proveedores de nube para desarrollar, probar, implementar y administrar las aplicaciones alojadas en un entorno de computación en la nube.

Los consumidores de PaaS pueden ser desarrolladores de aplicaciones que diseñan e implementan software de aplicación, probadores de software que ejecutan y prueban aplicaciones en entornos basados en la nube, implementadores de aplicaciones que publican aplicaciones en la nube y administradores de aplicaciones que configuran y supervisan el rendimiento de aplicaciones en una plataforma. Los proveedores de PaaS pueden facturar según el procesamiento, el almacenamiento de la base de datos y los recursos de red consumidos por la aplicación PaaS, así como la duración del uso de la plataforma, entre otros.

Los consumidores de IaaS tienen acceso a computadoras virtuales, almacenamiento accesible en red, componentes de infraestructura de red y otros recursos informáticos fundamentales en los que pueden implementar y ejecutar software arbitrario. Los consumidores de IaaS pueden ser desarrolladores de sistemas,



administradores de sistemas y administradores de TI que estén interesados en crear, instalar, administrar y monitorear servicios de gestión de infraestructura de TI.

Los consumidores IaaS disponen de las capacidades para acceder a estos recursos informáticos y se les factura de acuerdo con la cantidad o duración de los recursos consumidos, como las horas de CPU utilizadas por los ordenadores virtuales, el volumen y la duración de los datos almacenados, el ancho de banda consumido, el número de direcciones IP usadas para ciertos intervalos, entre otros.

2.3.2. Actividades proveedor de nube

Un proveedor de servicios de computación en la nube (desde Colombia o desde el exterior), despliega, configura, mantiene y actualiza la operación de las aplicaciones de software en una infraestructura de nube (propia, compartida, o apoyada con otros proveedores) para que los servicios se aprovisionen en los niveles de servicio esperados para los consumidores de nube. El proveedor de SaaS asume la mayoría de las responsabilidades en la gestión y control de las aplicaciones y la infraestructura, mientras que los consumidores de la nube tienen un control administrativo limitado de las aplicaciones [4][5].

El proveedor de PaaS gestiona la infraestructura de cómputo de la plataforma y ejecuta el software de nube que proporciona los componentes de la plataforma como las bases de datos y otros componentes de capa media para el intercambio de información (middleware). El proveedor de PaaS normalmente también soporta el proceso de desarrollo, despliegue y administración del consumidor de PaaS, proporcionando herramientas tales como entornos de desarrollo integrados (IDE), control de versiones en la nube, kits de desarrollo de software (SDK), herramientas de implementación y administración. El proveedor de PaaS no tiene control sobre las aplicaciones hospedadas (el control lo tiene el consumidor de SaaS), pero posiblemente si lo tiene sobre la configuración del entorno de hospedaje, así mismo, no tiene o tiene acceso limitado a la infraestructura subyacente de la plataforma, como la red, los servidores, los sistemas operativos o el almacenamiento.

El proveedor de IaaS provee los recursos informáticos físicos subyacentes al servicio, incluidos los servidores, las redes, el almacenamiento y la infraestructura de alojamiento. El proveedor de nube ejecuta el software de la nube necesario para que los recursos informáticos estén disponibles para el consumidor de IaaS a través de un conjunto de interfaces de servicios y abstracciones de recursos de cómputo, como máquinas virtuales e interfaces de red virtual. El consumidor de IaaS a su vez utiliza estos recursos de computación, como una computadora virtual, para sus necesidades de computación fundamentales.

Comparado con los consumidores de SaaS y PaaS, un consumidor de IaaS tiene acceso a formas más fundamentales de recursos de computación y más componentes de software, incluyendo el sistema operativo y la red. Por otro lado, el

proveedor de IaaS tiene control sobre el software físico de hardware y nube que hace posible el aprovisionamiento de estos servicios de infraestructura, por ejemplo, servidores físicos, equipos de red, dispositivos de almacenamiento, sistema operativo host e hipervisores para la virtualización.

Las actividades de un proveedor de nube pueden describirse en cinco áreas principales, como se muestra en la Figura 3, un proveedor de nube lleva a cabo sus actividades en las áreas de despliegue de servicios, orquestación de servicios, gestión o administración de servicios en la nube, seguridad y privacidad.

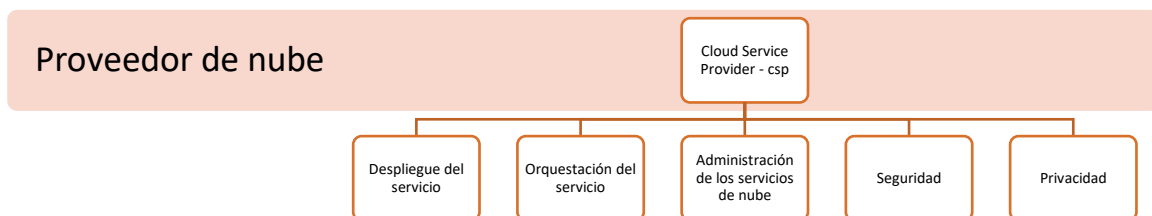


Figura 3 Actividades principales de un Proveedor de la nube.

Despliegue de servicio: Una infraestructura de nube puede operarse en uno de los siguientes modelos de implementación: nube pública, nube privada, nube de comunidad o nube híbrida. Las diferencias se basan en la forma exclusiva en que están dados los recursos de computación a un consumidor de nube.

Orquestación del servicio: Se refiere a la composición de los componentes del sistema con el fin de proporcionar servicios en la nube a los consumidores de nube. La Figura 4 muestra un diagrama de pila genérico de esta composición que subyace al suministro de servicios en la nube.

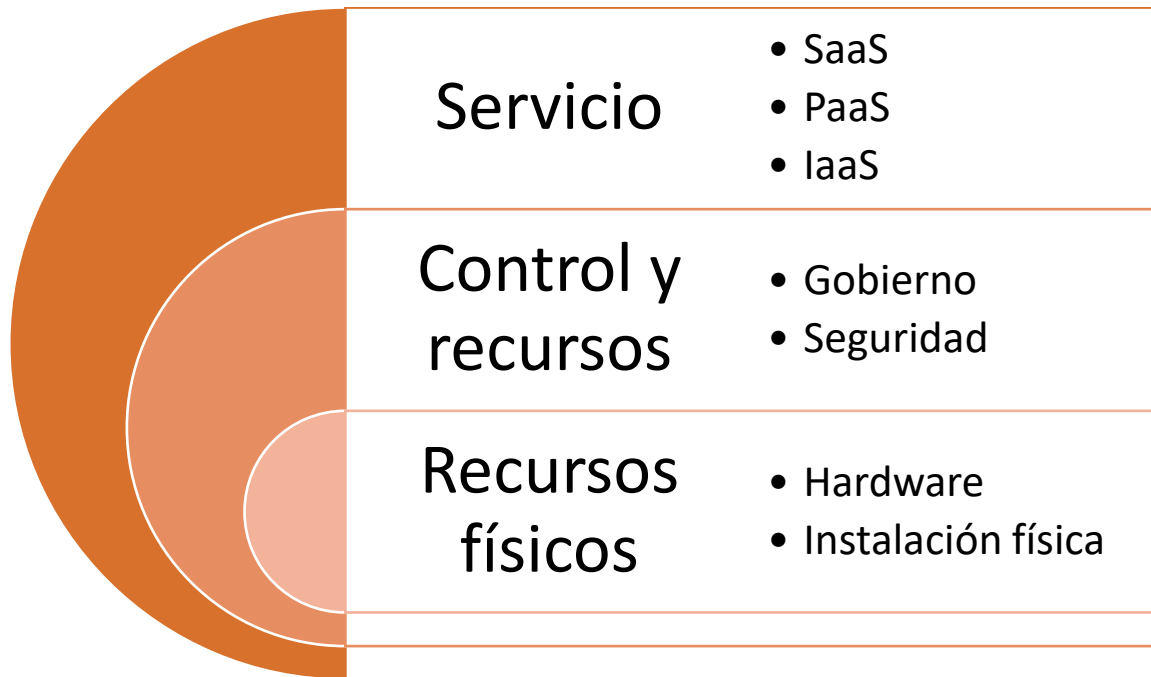


Figura 4 Proveedor de nube – Orquestación del Servicio

En esta representación se utiliza un modelo de tres capas, que representa la agrupación e integración de tres tipos de componentes del sistema que los proveedores de nube deben componer para entregar sus servicios.

En el modelo mostrado en la Figura 4, la parte superior es la capa de servicio, donde los proveedores de nube definen interfaces para que los consumidores de nube accedan a los servicios informáticos. Las interfaces de acceso de cada uno de los tres modelos de servicio se proporcionan en esta capa. Es posible, aunque no es necesario, que las aplicaciones SaaS puedan ser construidas sobre componentes PaaS y que los componentes PaaS puedan ser construidos sobre los componentes IaaS.

Las relaciones de dependencia opcionales entre los componentes SaaS, PaaS e IaaS se representan gráficamente como componentes que se apilan unos sobre otros, mientras que la inclinación de los componentes representa que cada uno de los componentes de servicio puede mantenerse por sí mismo. Por ejemplo, una aplicación SaaS se puede implementar y alojar en máquinas virtuales desde una nube IaaS o puede implementarse directamente encima de los recursos de la nube sin utilizar máquinas virtuales IaaS.

La capa media del modelo es la capa de abstracción y control de recursos. Esta capa contiene los componentes del sistema que los proveedores de nube utilizan para



proporcionar y administrar el acceso a los recursos de computación física a través de la abstracción de software. Algunos ejemplos de componentes de abstracción de recursos incluyen elementos de software como hipervisores, máquinas virtuales, almacenamiento de datos virtuales y otras abstracciones de recursos informáticos. El aspecto de control de esta capa se refiere a los componentes de software que son responsables de la asignación de recursos, el control de acceso y la supervisión del uso. Esta es la estructura de software que enlaza los numerosos recursos físicos subyacentes y sus abstracciones de software para permitir la agrupación de recursos, la asignación dinámica y la medición del servicio.

La capa más baja de la pila es la capa de infraestructura que incluye los recursos físicos (hardware, redes, almacenamiento y otros aspectos de planta física). Esta capa incluye recursos de hardware, tales como computadoras (CPU y memoria), redes (enrutadores, firewalls, conmutadores, enlaces de red e interfaces), componentes de almacenamiento (discos duros) y otros elementos físicos de infraestructura de computación. También incluye recursos de instalaciones, tales como calefacción, ventilación y aire acondicionado (HVAC), energía, comunicaciones, entre otros.

Siguiendo las convenciones de arquitectura del sistema, la posición horizontal, es decir, la superposición, en un modelo que representa las relaciones de dependencia - los componentes de la capa superior dependen de la capa inferior adyacente para funcionar. La capa de abstracción y control de recursos expone los recursos de la nube virtual sobre la capa de recursos físicos y soporta la capa de servicios donde las interfaces de servicios en la nube están expuestas a los consumidores de la nube, mientras que los consumidores de la nube no tienen acceso directo a los recursos físicos.

Administración de los servicios en la nube: esta actividad incluye todas las funciones relacionadas con los servicios que son necesarios para la gestión y operación de los servicios requeridos o propuestos a los consumidores de nube. Como se ilustra en la Figura 5, la administración del servicio en la nube se puede describir desde la perspectiva del soporte empresarial, el aprovisionamiento y la configuración, y desde la perspectiva de los requisitos de portabilidad e interoperabilidad.

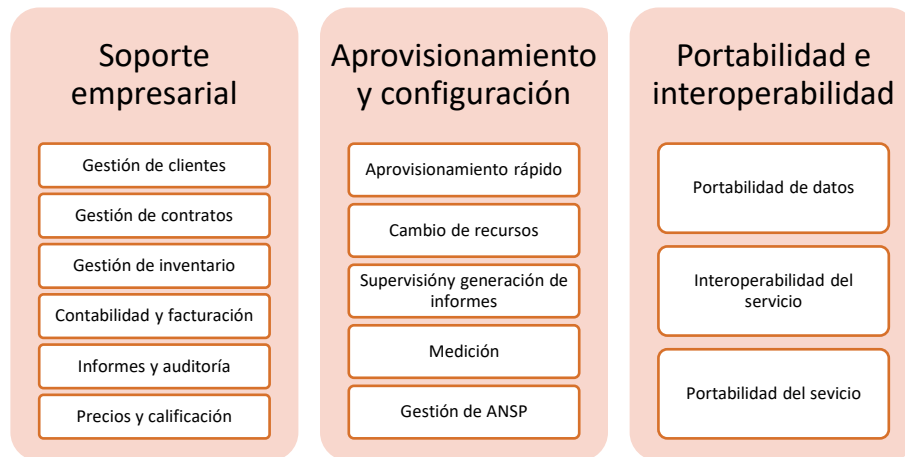


Figura 5 Proveedor de nube – Administración del servicio en la nube

Soporte empresarial o de negocios: El soporte empresarial implica el conjunto de servicios relacionados con los negocios que se ocupan de los clientes y los procesos de apoyo. Incluye los componentes utilizados para ejecutar operaciones empresariales orientadas al cliente.

Aprovisionamiento y configuración: Se refiere a las actividades del proceso que el proveedor debe ejecutar como parte de sus operaciones internas. Cuanto más maduras sean las capacidades de los proveedores en esta área, más efectiva y eficiente será la prestación del servicio. Una de las formas de aprovisionamiento que debería ofrecer un proveedor de nube es el aprovisionamiento rápido que consiste en proveer recursos, capacidades y servicios de manera automática cuando se cumpla una regla (umbral entre otros) establecida.

Portabilidad e Interoperabilidad: Los proveedores de nube deben proporcionar mecanismos para apoyar la portabilidad de los datos, la interoperabilidad de los servicios y la portabilidad del sistema. La portabilidad de datos es la capacidad de los usuarios de la nube para copiar objetos de datos dentro o fuera de una nube o para usar un disco para la transferencia de datos a disposición del usuario sin intervención del proveedor.

La interoperabilidad de los servicios es la capacidad de los usuarios de la nube para usar sus datos y servicios a través de múltiples proveedores de nube con una interfaz de administración unificada. La portabilidad del sistema permite la migración de una instancia de máquina virtual totalmente detenida o una imagen de máquina de un proveedor a otro proveedor, o migrar aplicaciones y servicios y su contenido de un proveedor de servicios a otro.



Cabe señalar que varios modelos de servicios en la nube pueden tener diferentes requisitos en relación con la portabilidad y la interoperabilidad. Por ejemplo, IaaS requiere la capacidad de migrar los datos y ejecutar las aplicaciones en una nueva nube. Por lo tanto, es necesario capturar imágenes de máquinas virtuales y migrar a nuevos proveedores de nube que pueden utilizar diferentes tecnologías de virtualización. Cualquier extensión específica del proveedor de las imágenes de las máquinas virtuales (VM por sus siglas en inglés Virtual Machine), debe eliminarse o registrarse al ser portada. Mientras que, para SaaS, el foco está en la portabilidad de datos, y por lo tanto es esencial para realizar extracciones de datos y copias de seguridad en un formato estándar.

2.3.3. Actividades del Auditor de nube

Un auditor de nube es una tercera parte (o una parte de la misma organización) que puede realizar una verificación independiente de los controles del servicio en la nube y así mismo, realizar auditorías para verificar la conformidad con las normas mediante la revisión de pruebas objetivas. Un auditor de nube puede evaluar los servicios proporcionados por un proveedor de nube en términos de controles pertinentes de seguridad, impacto sobre la privacidad, rendimiento, etc. [4][5]. Cabe aclarar que, por algún acuerdo de confidencialidad expreso entre proveedor y cliente, el auditor vería disminuido el alcance en la auditoría realizada. Por lo anterior es necesario que se establezca el alcance de la auditoría sin dejar excluidos los ANS respectivos, las características esenciales de un modelo de computación en la nube.

2.3.4. Actividades del corredor u agente (Intermediario) de nube

Un corredor de nube proporciona servicios comerciales y de apoyo a las relaciones (intermediación comercial), y servicios de soporte técnico (agregación, optimización e intermediación técnica) [4][5].

Intermediación de servicios: Un corredor de nube mejora un servicio añadiendo alguna capacidad específica y proporcionando servicios de valor agregado a los consumidores de nube. La mejora puede ser la gestión del acceso a servicios en la nube, gestión de identidades, informes de rendimiento, seguridad mejorada, etc.

Agregación de servicios: Un corredor de nube combina e integra varios servicios en uno o más servicios nuevos. El corredor (intermediario) proporciona integración de datos y asegura el movimiento seguro de datos entre el consumidor de nube y varios proveedores de nube.

Servicios de optimización: Este servicio es similar a la agregación de servicios, sin embargo, el corredor o intermediario tiene la flexibilidad de elegir y agregar servicios de varios proveedores. Por ejemplo, un proveedor puede agregar y seleccionar los servicios a partir del ranking obtenido por el cumplimiento de acuerdos de nivel de servicio.

2.3.5.Actividades del operador de nube

Un operador de nube actúa como un “intermediario” que proporciona conectividad y transporte de servicios en la nube entre los consumidores de nube y los proveedores de nube. Los operadores de nube proporcionan acceso a los consumidores a través de redes, telecomunicaciones. La distribución de servicios en la nube es normalmente proporcionada por operadores de redes y telecomunicaciones o un agente de transporte [4][5].

Hay que tener en cuenta que un proveedor de la nube establecerá ANS con un operador de nube para proporcionar servicios consistentes con el nivel de ANS ofrecidos a los consumidores de nube y puede requerir que el proveedor de nube proporcione conexiones seguras y dedicadas entre los consumidores de nube y los proveedores de nube.

2.4. MODELOS DE SERVICIO

La computación en la nube basa su arquitectura haciendo una separación entre infraestructura, plataforma y aplicaciones, como se ilustra en la figura 6 [5]:

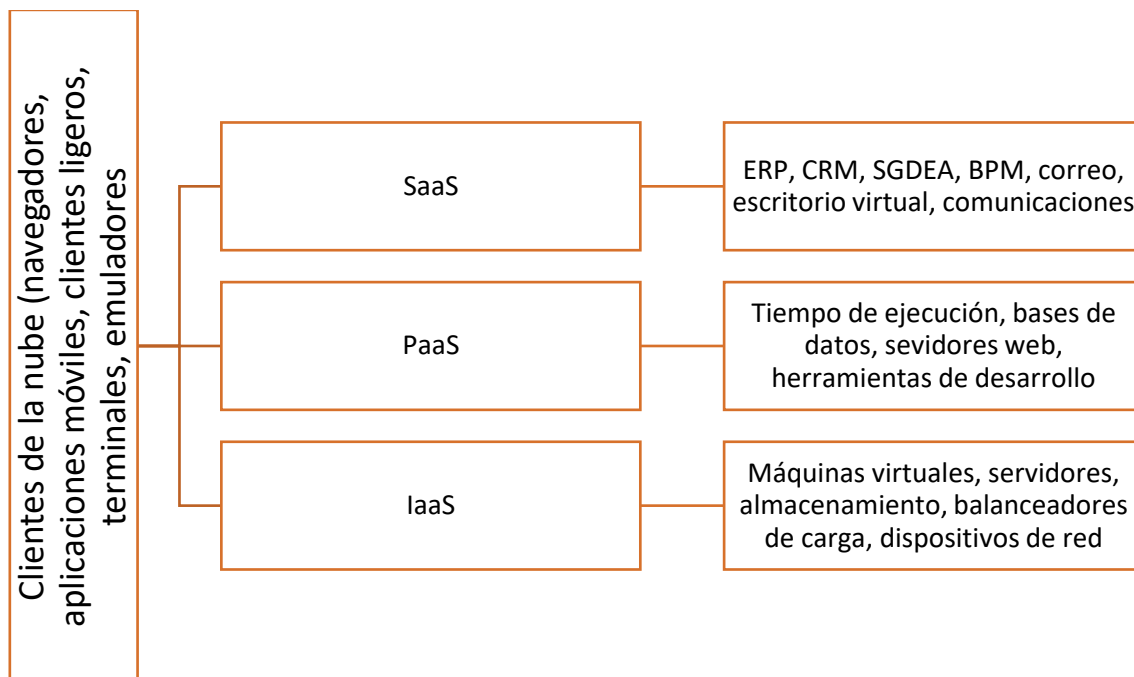


Figura 6 Modelos de servicio



2.4.1. Software como Servicio (Software as a Service – SaaS)

La capacidad proporcionada al consumidor consiste en utilizar las aplicaciones del proveedor que se ejecutan en una infraestructura de computación en la nube. Las aplicaciones son accesibles desde varios dispositivos cliente a través de una interfaz de cliente ligero (como un navegador web) o una interfaz de programa.

El consumidor no gestiona ni controla la infraestructura subyacente de la nube (red, servidores, sistemas operativos, almacenamiento), ni las capacidades de las aplicaciones individuales, con la única excepción de los ajustes de configuración específicos del usuario (por ejemplo, gestión de usuarios, roles y permisos).

El proveedor de SaaS es responsable del mantenimiento, la operación, el soporte, la seguridad de la infraestructura subyacente y, crucialmente, debe garantizar los estándares de cumplimiento normativo de la plataforma, mientras que la entidad gubernamental es responsable de la seguridad de sus datos y la correcta configuración del acceso (IAM) dentro de la aplicación.

A continuación, se presentan ejemplos de servicios de tipo SaaS, destacando su evolución y su relevancia para el sector público: SaaS [5]:

- **Aplicaciones de Productividad y Colaboración:** Incluye correo electrónico, procesamiento de texto, hojas de cálculo, presentaciones y herramientas de videoconferencia. La facturación es típicamente por usuario o por suscripción.
- **Gestión de la Relación con el Ciudadano (CRM) y Centro de Contacto:** Aplicaciones de CRM dispuestas en la nube para gestionar la interacción, el servicio al ciudadano y la automatización de la fuerza de ventas.
- **Herramientas de Colaboración Unificada:** Software que permite a los equipos de trabajo colaborar de forma remota, integrando chat, gestión de proyectos y compartición de documentos, vital para la continuidad del negocio gubernamental.
- **Gestión de Contenidos y Documentos (ECM/DMS):** Servicios que permiten el acceso a herramientas en la nube para gestionar la producción, el archivo, la trazabilidad y el acceso seguro a contenidos y documentos oficiales, haciendo cumplir flujos de trabajo de aprobación y gestión de versiones.
- **Finanzas y Gestión Tributaria:** Aplicaciones para la gestión de procesos financieros, procesamiento de gastos, facturación y plataformas especializadas en la gestión tributaria y presupuestal.
- **Gestión de Recursos Humanos (HRIS):** Software para administrar funciones de recursos humanos, nómina, capacitación y gestión del talento dentro de las entidades.
- **Planificación de Recursos Empresariales (ERP):** Sistemas integrados web, dispuestos en la nube para administrar recursos internos y externos. Para que



- sea un SaaS, debe ser facturado por demanda o suscripción y cumplir con la característica de Medición del Servicio definida por el NIST.
- **Correo electrónico y aplicaciones de oficina:** Aplicaciones para correo electrónico, procesamiento de texto, hojas de cálculo, presentaciones, etc., dispuestos en la nube y con facturación según el uso.
 - **Facturación:** Servicios de aplicación dispuestos en la nube, para gestionar la facturación de los clientes basándose en el uso y las suscripciones a productos y servicios.
 - **Recursos Humanos:** Software para gestionar las funciones de recursos humanos dentro de las empresas.
 - **Aplicaciones de ventas:** Las aplicaciones web dispuestas en la nube, facturación, compra y venta de productos y/o servicios, realización de pedidos, seguimiento de comisiones, etc.
 - **IA Generativa como Aplicación (GenAI SaaS):** Aplicaciones listas para usar que integran modelos fundacionales de Inteligencia Artificial (IA) para tareas específicas, como la redacción automatizada de documentos legales, la transcripción automática de reuniones o el análisis de sentimientos en interacciones ciudadanas, sin que el usuario tenga que gestionar los modelos subyacentes.
 - **Observabilidad y Monitoreo SaaS:** Herramientas que ofrecen una visión unificada del estado operativo y de seguridad de toda la infraestructura tecnológica, sin requerir que la entidad hospede la plataforma de monitoreo.

Bajo el modelo SaaS, la entidad gubernamental debe enfocarse en las funciones de Gobernar, Identificar y Proteger del NIST CSF 2.0: [17]

- **Gobernar (GOVERN):** Establecer políticas claras sobre el uso aceptable de los datos y el cumplimiento de las leyes de privacidad y soberanía dentro de la aplicación SaaS.
- **Identificar (IDENTIFY):** Implementar la gestión rigurosa de identidad y acceso (IAM) dentro de la plataforma SaaS, asegurando que solo el personal autorizado tenga acceso a los datos, de acuerdo con el principio de Zero Trust.
- **Proteger (PROTECT):** Asegurar que las configuraciones de seguridad específicas de la aplicación (cifrado, permisos de compartición) protejan los datos sensibles del Estado, complementando la seguridad de la infraestructura provista por el CSP.

2.4.2. Plataforma como Servicio (Platform as a Service – PaaS)

Este modelo de servicio proporciona al consumidor la posibilidad de construir, desplegar y escalar en la infraestructura de nube aplicaciones creadas por el mismo consumidor (o adquiridas a un tercero) utilizando lenguajes de programación, bibliotecas, servicios y herramientas soportadas por el proveedor de nube. El consumidor mantiene el control sobre las aplicaciones, los datos, y la gestión de



acceso e identidad (IAM), pero no gestiona ni controla la infraestructura subyacente de la nube (servidores, sistemas operativos o almacenamiento).

El proveedor de PaaS es responsable del mantenimiento, la operación, el soporte, y la seguridad del sistema operativo y las plataformas de runtime. Este modelo es el principal habilitador de la metodología DevSecOps para las entidades gubernamentales, ya que permite a los desarrolladores centrarse en el código de la misión sin preocuparse por la gestión de parches y la infraestructura.

Esta capacidad no excluye necesariamente el uso de lenguajes de programación compatibles, bibliotecas, servicios y herramientas de otras fuentes, lo que fomenta las estrategias Multi-Cloud.

A continuación, algunos ejemplos de servicios tipo PaaS [5]:

- **Inteligencia de Negocios:** Plataformas para la creación de aplicaciones como paneles, sistemas de informes y análisis de datos.
- **Base de datos:** Servicios que ofrecen soluciones de base de datos relacionales escalables o almacenes de datos no SQL escalables.
- **Desarrollo y pruebas:** Plataformas para el desarrollo y los ciclos de pruebas de desarrollo de aplicaciones, que se expanden y se contraen según sea necesario.
- **Integración:** Plataformas de desarrollo para la construcción de aplicaciones de integración en la nube y dentro de la empresa.
- **Implementación de aplicaciones:** Plataformas adecuadas para el desarrollo de aplicaciones de uso general.

También, algunos ejemplos de servicios PaaS que son fundamentales para la modernización del gobierno:

- **Contenedores y Orquestación (CaaS):** Plataformas que facilitan el despliegue, escalado y gestión de aplicaciones empaquetadas en contenedores (por ejemplo, servicios gestionados de Kubernetes). Este es el pilar central de las arquitecturas Cloud Native.
- **Computación sin Servidor (Serverless Computing):** Plataformas que ejecutan código de función bajo demanda (Functions as a Service – FaaS), eliminando por completo la gestión del servidor. Es ideal para tareas impulsadas por eventos, microservicios y para la optimización de costos (FinOps).
- **Plataformas de Base de Datos Gestionadas:** Servicios que ofrecen soluciones de base de datos relacionales, NoSQL, o almacenes de datos escalables (Data Warehouses) con el aprovisionamiento, los parches de seguridad y el backup automatizado por el proveedor.
- **Plataformas de Desarrollo y Pruebas (DevSecOps):** Plataformas que proporcionan entornos preconfigurados para el desarrollo, las pruebas funcionales y las pruebas de rendimiento. Estas plataformas se integran con



pipelines de Integración Continua y Despliegue Continuo (CI/CD) que ejecutan escaneos de seguridad automáticamente.

- **Plataformas de Integración y API Management:** Plataformas de desarrollo para la construcción de aplicaciones que integran sistemas en la nube y sistemas on-premise, incluyendo la gestión de API Gateways y la mediación de mensajes.
- **Plataformas de Machine Learning (MLOps): Servicios** que proporcionan los entornos, pipelines y herramientas necesarias para el ciclo de vida completo de la Inteligencia Artificial (IA), entrenamiento de modelos, versionamiento, despliegue, y monitoreo del rendimiento de los modelos en producción (MLOps).
- **Internet de las Cosas (IoT) y Edge Platforms:** Plataformas diseñadas para ingestar, procesar y gestionar datos a escala masiva provenientes de sensores y dispositivos IoT/Edge, proporcionando las herramientas de runtime para el procesamiento de baja latencia.

Bajo el modelo PaaS, la entidad gubernamental debe enfocarse en las siguientes áreas de Seguridad y Cumplimiento del NIST CSF 2.0 y MRAE 3.0: [17] [18]

- **Protección de la Aplicación y del Código (PROTECT):** La entidad es totalmente responsable de la seguridad de las aplicaciones que despliega, lo que requiere la implementación de DevSecOps para la revisión continua de vulnerabilidades en el código fuente.
- **Gestión de Identidad y Acceso (IAM):** El control estricto sobre quién puede acceder a las plataformas PaaS y a los entornos de ejecución es esencial.
- **Configuración de Servicios:** La entidad debe configurar correctamente los servicios de la plataforma (reglas de firewall de bases de datos, permisos de contenedores) para evitar exposiciones accidentales, cumpliendo con la función Proteger del NIST CSF 2.0. [17]
- **Soberanía de Datos:** Asegurar que las bases de datos y los entornos de runtime cumplan con la residencia de datos requerida por la normativa nacional.

2.4.3. Infraestructura como Servicio (Infrastructure as a Service – IaaS)

Este modelo de servicio proporciona al consumidor de nube las capacidades de procesamiento (máquinas virtuales y bare metal), almacenamiento, redes virtuales y otros recursos de cómputo fundamentales. El consumidor es capaz de desplegar y ejecutar software arbitrario, que puede incluir sistemas operativos, middleware y aplicaciones. El consumidor no gestiona ni controla la infraestructura física subyacente de la nube (centros de datos, hardware de virtualización). Sin embargo, tiene control total y responsabilidad directa sobre los sistemas operativos instalados, el middleware, el runtime, el almacenamiento, las aplicaciones implementadas y un control limitado de componentes de red selectos (por ejemplo, configuración de firewalls de red virtual y tablas de enrutamiento). IaaS es la base para construir infraestructuras complejas, especialmente para la migración de sistemas legados que



aún no son Cloud Native o para soportar plataformas que requieren acceso directo al nivel del sistema operativo.

En IaaS, el proveedor de nube es responsable de la capa hasta el Hipervisor, mientras que la entidad de gobierno es responsable de todas las capas desde el Sistema Operativo hacia arriba. Esto incluye crucialmente la aplicación de parches de seguridad (patch management) en el sistema operativo, la configuración de firewalls y la protección de los datos.

A continuación, algunos ejemplos de servicios tipo IaaS [5]:

- **Bare Metal (Metal Desnudo):** Servidores físicos dedicados, aprovisionados a través de la nube, para cargas de trabajo que requieren acceso directo al hardware o rendimiento extremo (Cómputo de Alto Rendimiento).
- **Cómputo (Máquinas Virtuales):** Recursos de servidor provisionados dinámicamente (CPU, memoria, GPU) para ejecutar sistemas basados en la nube. Se incluyen Máquinas Virtuales (VMs) usadas para la migración (Lift & Shift) de sistemas legados.
- **Computación por lotes:** Este servicio permite procesar cargas de trabajo que requieren informática de alto rendimiento (high-performance computing, HPC), análisis de grandes volúmenes de datos ("big data") y otras cargas de trabajo que requieran grandes cantidades de capacidad según demanda. No requieren de una alta disponibilidad, pero pueden requerir un alto rendimiento.
- **Almacenamiento:** Capacidad de guardado de datos ampliamente escalable que puede utilizarse para alojar aplicaciones, copias de seguridad, archivos, entre otros siempre y cuando se garantice autoaprovisionamiento y las demás características esenciales de la computación en las nubes antes mencionadas.
- **Almacenamiento Elástico:** Capacidad de guardado de datos masivamente escalable en distintas modalidades:
 - Almacenamiento de Bloque: Usado como disco duro para las máquinas virtuales.
 - Almacenamiento de Archivo: Usado para sistemas de archivos compartidos (shared filesystems).
 - Almacenamiento de Objetos: Para grandes volúmenes de datos no estructurados (archivos multimedia, logs, backups) con acceso vía API, siendo el pilar para los proyectos de Big Data del gobierno.
- **Copia de seguridad y recuperación:** Servicios de copia de seguridad y recuperación de sistemas de archivos y almacenes de datos sin procesar en servidores y equipos de escritorio, siempre y cuando se garantice el autoaprovisionamiento y las demás características esenciales de la computación en las nubes antes mencionadas.
- **Redes de Distribución de Contenido (CDN) y Edge Services:** Redes de servidores especializados distribuidos geográficamente que aceleran la distribución de contenido estático y dinámico a los usuarios finales. Son vitales



para garantizar la disponibilidad y baja latencia de los portales web gubernamentales de alta concurrencia.

- **Gestión de Infraestructura (Infraestructura como Código - IaC):** Herramientas que permiten administrar, verificar y desplegar servicios IaaS de manera centralizada y automatizada. Esta capacidad es fundamental para el cumplimiento del FinOps y el control de la arquitectura.
- **Infraestructura para Edge Computing:** Servidores IaaS desplegados en ubicaciones geográficas más cercanas a los usuarios o dispositivos IoT para soportar el procesamiento de datos en el borde de la red, asegurando la baja latencia para servicios críticos.
- **Redes de distribución de contenido (CDN):** Una red de distribución de contenido es una gran red de servidores especializados distribuidos geográficamente que acelera la distribución de contenido web y multimedia a dispositivos conectados a Internet. La técnica principal que utiliza una red de distribución de contenido (CDN) para acelerar la distribución de contenido web a los usuarios finales es el almacenamiento en caché perimetral, que consiste en almacenar réplicas de contenido estático de texto, imagen, audio y vídeo en varios servidores alrededor del "perímetro" de Internet, de modo que las solicitudes de los usuarios se pueden responder mediante un servidor perimetral cercano, en lugar de mediante un servidor de origen lejano.
- **Gestión de servicios:** Son servicios que permiten y facilitan la administración de plataformas de infraestructura en la nube. Estas herramientas aseguran rapidez en el despliegue, gestión y control de servicios IaaS sobre la nube. Un ejemplo en este caso es el software de capa media que permite administrar, verificar mediante informes de uso, desplegar servicios de IaaS (almacenamiento, servidores, ampliación de infraestructura TI automática, empaquetadores) de manera centralizada.
- **Servicios tecnológicos de Internet de las cosas (Internet of Things, IoT):** Estos servicios hacen referencia a infraestructura como sensores, cámaras, y otros dispositivos incluidos las aplicaciones de software que permiten su gestión y administración. Estos servicios se caracterizan por alta disponibilidad, capacidad flexible y escalable, interacción con dispositivos móviles, interoperabilidad y alta seguridad.

Debido al alto nivel de control, IaaS impone la mayor responsabilidad de seguridad al consumidor. Las entidades deben centrarse en:

- **PROTEGER el Sistema Operativo (PROTECT):** El gobierno es responsable del endurecimiento del sistema operativo (OS hardening), la gestión de parches, la instalación de antivirus/antimalware, y la configuración de los firewalls a nivel de VM.
- **GESTIONAR la Configuración (GOVERN):** Asegurar que todas las configuraciones de red, almacenamiento y cómputo virtual cumplan con los requisitos de Zero Trust y las políticas de seguridad del MRAE 3.0 (segmentación de red virtual y políticas de cifrado). [18]

- **RECUPERAR ante Falla (RECOVER):** Implementar estrategias de backup y Disaster Recovery (DR) para las aplicaciones, los datos y los sistemas operativos alojados en IaaS, garantizando la continuidad de la misión pública.

2.5. MODELOS DE IMPLEMENTACIÓN

Existen diferentes tipos de nubes [4] de acuerdo con las necesidades, al modelo de servicio ofrecido y a su despliegue, todo depende de dónde se encuentran instaladas las aplicaciones y qué clientes pueden usarlas, están los siguientes modelos:

2.5.1. Nube privada (Private cloud)

Una nube privada da a una sola organización de consumidores el acceso exclusivo y el uso de la infraestructura y los recursos computacionales. Puede ser administrado por la organización del consumidor de nube o por un tercero, y puede ser alojado en las instalaciones de la organización (por ejemplo, nubes privadas en el sitio) o subcontratado a una compañía de alojamiento (es decir, nubes privadas externalizadas) [4][5]. La Figura 7 y 8 representan una nube privada en el sitio y una nube privada subcontratada, respectivamente.

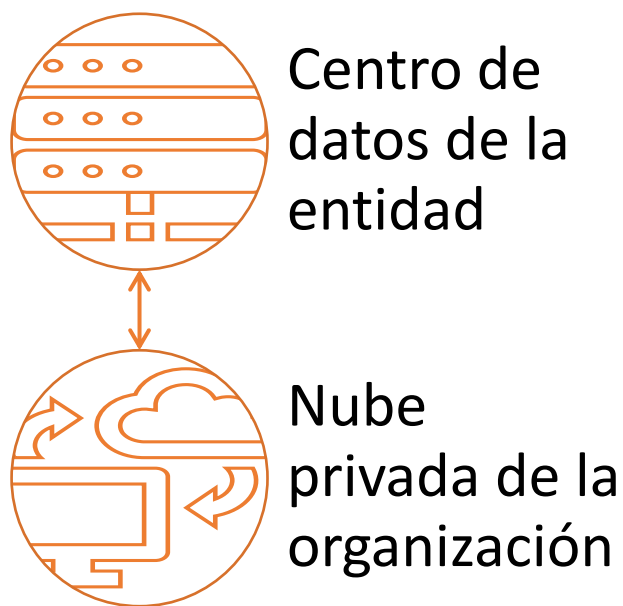


Figura 7 Nube privada en sitio

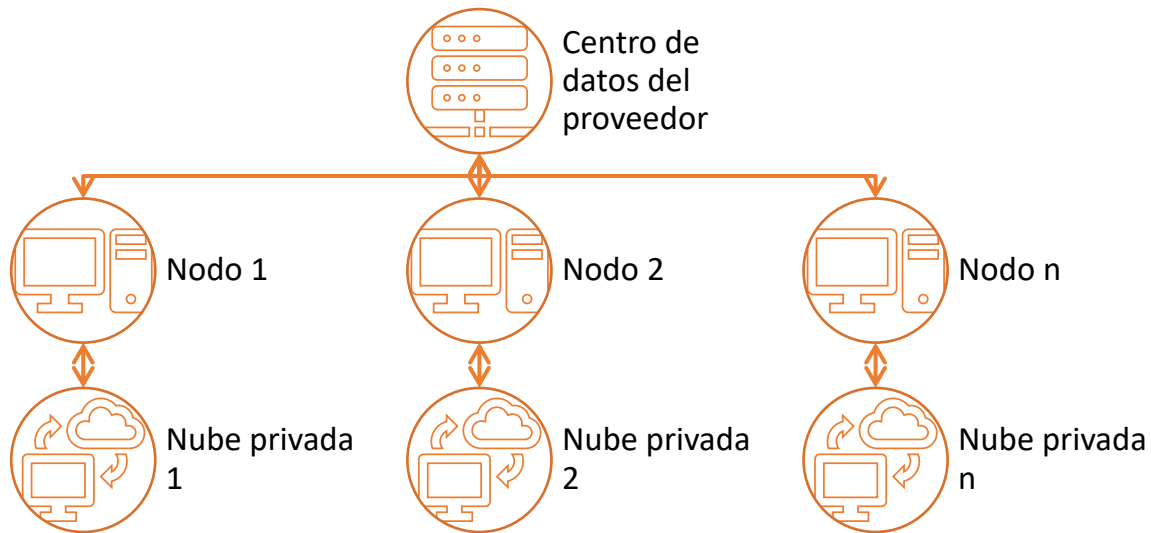


Figura 8 Nube privada subcontratada

2.5.2. Nube comunitaria (Community cloud)

Una nube comunitaria sirve a un grupo de consumidores que han compartido preocupaciones tales como objetivos de misión, seguridad, privacidad y política de cumplimiento, en lugar de servir a una organización como lo hace una nube privada. De forma similar a las nubes privadas, una nube comunitaria puede ser administrada por las organizaciones o por un tercero, y puede implementarse en las instalaciones del cliente (es decir, en la nube de la comunidad) o subcontratada a una compañía de hosting.

La Figura 9 muestra una nube comunitaria en el sitio compuesta de varias organizaciones participantes. Un consumidor de nube puede acceder a los recursos de la nube local, y también a los recursos de otras organizaciones participantes a través de las conexiones entre las organizaciones asociadas.

La Figura 10 muestra una nube de comunidad externalizada, donde el lado del servidor es subcontratado a una empresa de hosting. En este caso, una nube de comunidad externalizada construye su infraestructura fuera de la organización y sirve a un conjunto de organizaciones que solicitan y consumen servicios en la nube.

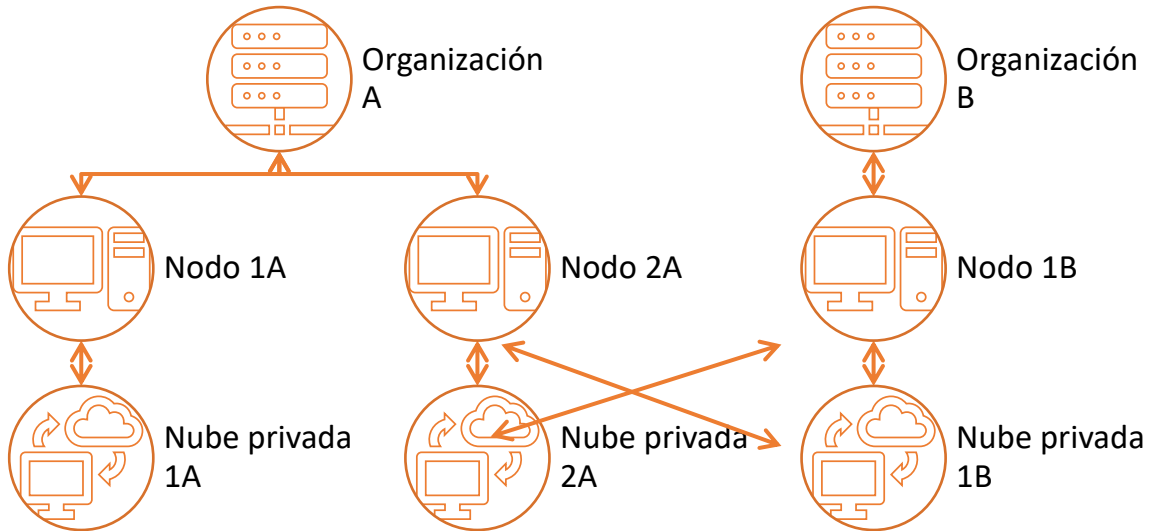


Figura 9 Nube comunitaria en sitio

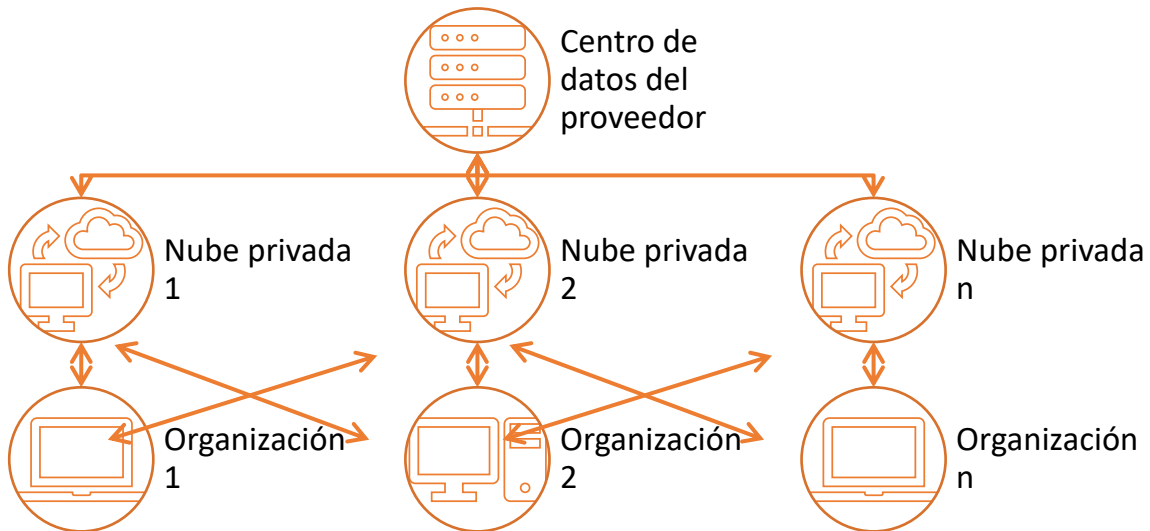


Figura 10 Nube comunitaria subcontratada

2.5.3. Nube pública (Public cloud)

Una nube pública es aquella en la que la infraestructura en nube y los recursos informáticos se ponen a disposición del público en general a través de una red pública y es propiedad de una organización que vende servicios en la nube y sirve a una diversa cantidad de clientes. La Figura 12 presenta una vista simple de una nube pública y sus clientes.

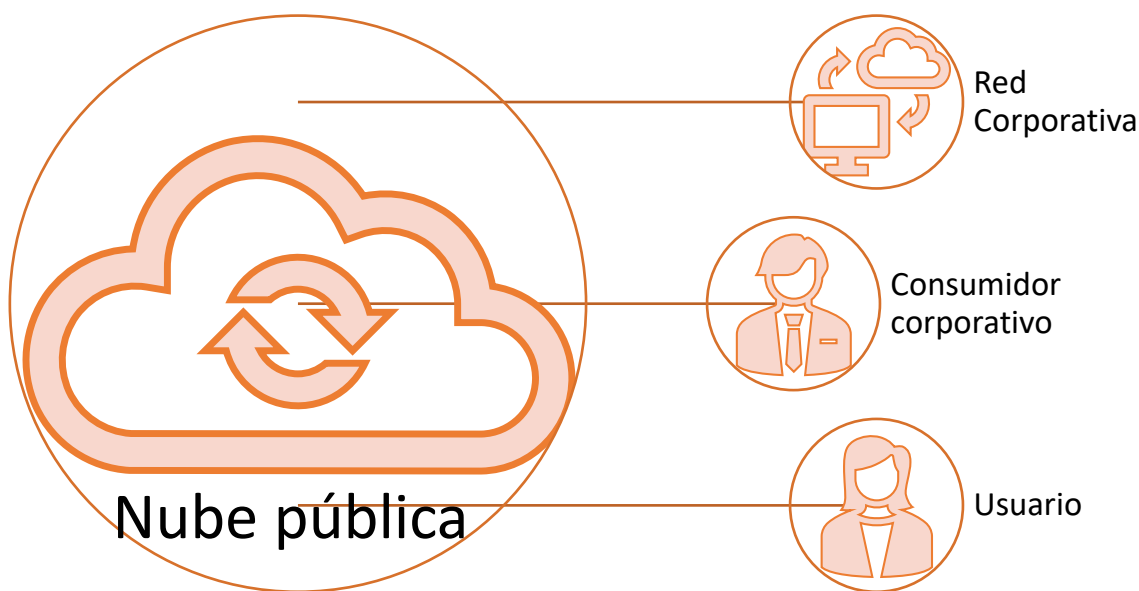


Figura 11 Nube pública

2.5.4. Nube híbrida (Hybrid cloud)

Una nube híbrida es una composición de dos o más nubes (en el sitio privado, en el sitio de la comunidad, fuera del sitio privado, fuera del sitio de la comunidad o público) que siguen siendo entidades distintas, pero están unidas por tecnología común entre las partes o propietaria que permite la portabilidad de datos y aplicaciones entre las nubes.

2.6. BENEFICIOS DE IR A LA NUBE

Como es conocido, la computación en la nube ofrece beneficios que permiten mayor flexibilidad para conectar y operar una empresa u organización desde cualquier lugar y en cualquier momento a través de la red.



La computación en la nube ha trascendido el beneficio operativo para tener un rol estratégico para el sector público, alineado con el MRAE 3.0 y los pilares de seguridad del NIST CSF 2.0. [17] [18] La nube ofrece la flexibilidad y la resiliencia necesarias para operar servicios de gobierno desde cualquier lugar y en cualquier momento, a través de la red, mientras habilita la innovación. Los beneficios clave que el modelo de computación en la nube provee a las entidades públicas son:

2.6.1. Gobernanza Financiera y Optimización de Costos (FinOps)

La nube permite la migración de un modelo de gasto de capital (CapEx) a un modelo de gasto operativo (OpEx). Este cambio no solo se traduce en la reducción de costos de infraestructura y mantenimiento (TCO), sino en la optimización continua del valor de la nube a través de la disciplina FinOps.

- **Pago por Consumo Exacto:** La posibilidad de pagar únicamente por la capacidad o servicio utilizado efectivamente elimina el sobredimensionamiento y los costos de capacidad ociosa.
- **Gestión Activa del Gasto:** Los costos operacionales de TI (anteriormente dedicados a mantenimiento, licencias y soporte) se reasignan a inversiones estratégicas que tienen un impacto directo en la misión y los procesos de negocio.
- **Visibilidad y Responsabilidad:** La medición granular del servicio (característica NIST) permite a las áreas de TI y Finanzas rastrear el gasto por proyecto, equipo o servicio, promoviendo una cultura de responsabilidad financiera.

2.6.2. Escalabilidad y Elasticidad Dinámica (Cloud Native)

Los servicios de la nube ofrecen la agilidad para desplegar nuevos servicios o trámites y la elasticidad para responder a las demandas de capacidad y procesamiento con precisión.

- **Escalado Automático:** Los recursos (cómputo, almacenamiento) pueden crecer o decrecer automáticamente y en tiempo real, respondiendo a la demanda de los usuarios. Esto es especialmente útil para la prestación de servicios que tienen picos de alta concurrencia (plazos de impuestos, votaciones electrónicas, servicios de ayuda social en emergencias).
- **Habilitador Cloud Native:** Esta elasticidad es el pilar de arquitecturas modernas como Serverless y Contenedores, donde el escalado no se limita a servidores, sino a microservicios granulares.

2.6.3. Reducción de Costos y Riesgos de Obsolescencia Tecnológica

La tecnología avanza aceleradamente, haciendo que la inversión en activos fijos (servidores, hardware de red, licenciamiento perpetuo) conlleve un alto riesgo de obsolescencia.



- **Transferencia de Riesgo al Proveedor:** Cuando las entidades adquieren servicios en la nube, el riesgo de obsolescencia tecnológica se traslada al Proveedor de Servicios en la Nube (CSP), ya que la entidad paga solo por el uso del servicio actualizado.
- **Mantenimiento Perpetuo:** El proveedor es responsable de las actualizaciones de hardware y firmware, y de aplicar parches de seguridad a la infraestructura subyacente, liberando a la entidad gubernamental de la carga de gestionar sistemas legados y sus vulnerabilidades.

2.6.4. Acceso Prioritario a Capacidades Estratégicas (IA y Serverless)

Los CSPs invierten constantemente miles de millones en la actualización de sus plataformas. Esto otorga a las organizaciones de todos los tamaños acceso inmediato a la misma tecnología de punta y capacidades avanzadas, lo cual es un habilitador directo de la misión pública.

- **Inteligencia Artificial y Machine Learning:** Acceso a plataformas gestionadas de MLOps y servicios de IA Generativa que aceleran la toma de decisiones basada en datos y modernizan la interacción con el ciudadano.
- **Servicios Cloud Native:** Acceso a modelos Serverless y Edge Computing que garantizan el rendimiento y la baja latencia para servicios críticos.
- **Seguridad Avanzada:** Acceso a servicios de Zero Trust, gestión de identidad y herramientas de detección de amenazas impulsadas por IA, que de otra forma serían prohibitivamente costosas para adquirir e implementar localmente.

2.6.5. Resiliencia, Continuidad del Negocio y Recuperación (NIST CSF 2.0)

Las capacidades de respaldo, alta disponibilidad, continuidad del negocio y Recuperación ante Desastres (DR) son características inherentes y diseñadas en la arquitectura Multi-Cloud.

- **Alta Disponibilidad Geográfica:** La posibilidad de replicar datos y servicios automáticamente en múltiples zonas de disponibilidad o regiones geográficas del proveedor, minimizando el tiempo de inactividad.
- **Recuperación Rápida:** Los planes de DR se vuelven programáticos y automáticos (Infraestructura como Código), reduciendo drásticamente el Tiempo Promedio de Recuperación (MTTR) en caso de fallos mayores o desastres.

2.6.6. Seguridad y Cumplimiento por Diseño (DevSecOps)

La nube permite a las entidades centrar sus esfuerzos en las funciones Identificar, Proteger y Gobernar del NIST CSF 2.0. [17]



- **Reducción de Riesgos Técnicos:** La adopción de DevSecOps dentro de la nube permite automatizar la seguridad en el ciclo de vida de la aplicación, reduciendo el riesgo de vulnerabilidades en el código.
- **Seguridad a Escala:** La entidad aprovecha la inversión masiva del proveedor en seguridad física y lógica (certificaciones internacionales, seguridad de red y cifrado por defecto), lo que le permite concentrar sus limitados recursos de seguridad en la protección de sus datos y aplicaciones.
- **Trazabilidad y Auditoría:** Los servicios de medición y logging de la nube proporcionan una trazabilidad completa del acceso y el uso de los datos, esencial para los requisitos de Cumplimiento Normativo del gobierno.

2.6.7. Agilidad y Despliegue Continuo (CI/CD)

La adquisición de soluciones y servicios de la nube reduce el tiempo de salida y despliegue de nuevos servicios o trámites, reducción del time to market gracias a la automatización y la estandarización.

- **Implementación Rápida:** La capacidad de aprovisionar infraestructura y plataformas en minutos, en lugar de meses, acelera el ciclo de innovación y la capacidad de la entidad para responder a nuevas leyes o necesidades ciudadanas.
- **Flexibilidad en la Funcionalidad:** Permite aumentar o disminuir las capacidades y funcionalidades (ancho de banda, capacidad de procesamiento) de forma automatizada y sin fricciones.

2.6.8. Enfoque Estratégico en la Misión Pública

Al delegar al proveedor la responsabilidad del mantenimiento, operación y soporte de la infraestructura subyacente, los líderes de Tecnología pueden concentrar sus recursos humanos y financieros en aspectos más estratégicos y de planeación que impactan directamente sobre los procesos de negocio de la organización.

El equipo de TI se transforma de un equipo de mantenimiento de infraestructura a un equipo de ingeniería de valor centrado en la creación de aplicaciones que modernizan el servicio al ciudadano, en línea con la visión estratégica del MRAE 3.0. [18]

2.6.9. Sostenibilidad y Responsabilidad Ambiental

La migración a la nube contribuye directamente a los objetivos de sostenibilidad del gobierno.

- **Eficiencia Energética:** Los centros de datos hiperescalares son significativamente más eficientes en el uso de energía y agua que los centros de datos tradicionales gubernamentales, al tiempo que utilizan un mayor porcentaje de energía renovable.



- **Optimización de Recursos:** La elasticidad y el uso eficiente de los recursos (mediante el Resource Pooling) reduce la cantidad total de *hardware* requerido a nivel nacional, disminuyendo la huella de carbono total de la infraestructura digital del Estado.

3. COMPUTACIÓN EN LA NUBE EN COLOMBIA

3.1. CONTEXTO NORMATIVO

La legislación colombiana consagra como uno de sus principios rectores de las Tecnologías de la Información y las Comunicaciones la neutralidad tecnológica cuyo concepto fue definido en la Ley de TIC 1341 del 30 de Julio de 2009 y se ratifica en el decreto 1078 de 2017 artículo 2.2.9.1.1.1 de la estrategia de Gobierno Digital (GD). Este principio plantea: “El Estado garantizará la libre adopción de tecnologías, teniendo en cuenta recomendaciones, conceptos y normativas de los organismos internacionales competentes e idóneos en la materia, que permitan fomentar la eficiente prestación de servicios, contenidos y aplicaciones que usen Tecnologías de la Información y las Comunicaciones y garantizar la libre y leal competencia, y que su adopción sea armónica con el desarrollo ambiental sostenible. [10] [11]

Así mismo, el Marco de Referencia de Arquitectura Empresarial (MRAE 3.0) para la gestión de TI adopta entre sus principios fundamentales el de Neutralidad Tecnológica. Este principio plantea que el Estado no debe privilegiar tecnologías ni proveedores específicos, fomentando un ecosistema de innovación abierta. [18]

Por lo tanto, las entidades del Estado deben realizar una evaluación rigurosa, objetiva y continua de las alternativas de inversión, aplicando criterios integrales para obtener la mejor relación valor/costo/beneficio a lo largo del tiempo. Las entidades públicas, especialmente al adoptar servicios de computación en la nube, deben evaluar y justificar la selección de servicios y tecnología de manera objetiva, siendo deseable que la estrategia de adopción cumpla con los siguientes imperativos:

- **Estrategia Multi-Cloud e Híbrida:** La Neutralidad Tecnológica se cumple al evitar el bloqueo a un solo proveedor (vendor lock-in) mediante la adopción de una estrategia Multi-Cloud e Híbrida. Esto permite que las cargas de trabajo más críticas y con requisitos de soberanía permanezcan en entornos privados, mientras que las cargas de trabajo escalables y de innovación se despliegan en el proveedor de nube que ofrezca la mejor combinación de servicio y coste.
- **Gobernanza de Costos (FinOps):** La evaluación costo/beneficio debe ser continua y formalizada a través de la disciplina FinOps. Esto exige que las entidades no solo comparen precios de inicio, sino que gestionen, midan y optimicen activamente el gasto operativo en la nube, asegurando que el proveedor seleccionado siga siendo la opción de mejor valor a medida que evolucionan las necesidades del servicio.



- **Adopción de Estándares Abiertos (Cloud Native):** Se debe priorizar el uso de tecnologías abiertas y portables, como contenedores (Kubernetes) y APIs estándar, para garantizar que las aplicaciones gubernamentales puedan moverse entre diferentes proveedores o entornos (públicos y privados) sin reingeniería significativa, reforzando la neutralidad.
- **Cumplimiento Normativo y Resiliencia:** La justificación objetiva debe incluir la capacidad del proveedor para asegurar la Soberanía de Datos y ofrecer la resiliencia geográfica (Disaster Recovery) necesaria para garantizar la continuidad de la misión pública.

De otro lado, la Agencia Nacional de Contratación Pública - Colombia Compra Eficiente (CCE), con el apoyo técnico del Ministerio de TIC (MinTIC), ha avanzado en la estructuración de la estrategia de contratación para la nube, facilitando a las entidades estatales la adopción de arquitecturas modernas. La evolución de los Acuerdos Marco de TI (AM) relacionados con la computación en la nube reflejan la madurez del sector público:

- **Servicios de Centro de Datos/Nube Privada (I, II y subsiguientes generaciones):** Estos AM fueron diseñados para la adquisición de infraestructura fundamental para soportar la Nube Privada e Híbrida. Son esenciales para aquellas cargas de trabajo que requieren cumplir con estrictos requisitos de soberanía de datos, residencia local y control físico, alineados con la función GOVERN del NIST CSF 2.0. [17]
- **Servicios de Nube Pública (II y III generación en estructuración/implementación):** Estos Acuerdos Marco de TI le permitieron a las Entidades Estatales adquirir los servicios de este tipo, mediante un proceso ágil y transparente; aprovechando el poder de compra del Estado para generar economías de escala y adquirir servicios de TI con características técnicas uniformes, generando importantes ahorros al Estado Colombiano.
- **Servicios de Nube Pública (AM IV - Adopción de Hiperescaladores):** Este acuerdo marco es el más reciente y se enfoca en la contratación de servicios de proveedores líderes a nivel mundial. Este AM fue la vía principal para que el Estado colombiano implemente una estrategia Multi-Cloud [6]. Los futuros acuerdos marcos de nube serán acogidos técnicamente por parte de la guía para cumplir con los estándares de contratación vigentes.

3.2. ASPECTOS PARA CONSIDERAR A LA HORA DE IR A LA NUBE

La decisión de adoptar servicios en la nube para entidades gubernamentales ya no es una cuestión de *si*, sino de *cómo* y *qué gobernar*. La estrategia de adopción debe ser integral, cubriendo los aspectos de seguridad, cumplimiento normativo, viabilidad técnica, y gestión financiera, en estricta alineación con el MRAE 3.0 y el marco de seguridad del NIST CSF 2.0. [17] [18]



3.2.1. Gobernanza, Seguridad y Cumplimiento Normativo

Este es el aspecto más crítico para el sector público y se rige por el modelo de Responsabilidad Compartida.

ASPECTO	CRITERIO	ACCIÓN
Soberanía y Residencia de Datos	¿Dónde se almacenarán y procesarán los datos sensibles?	La entidad debe verificar que el proveedor y los Acuerdos Marco garanticen la residencia de los datos dentro de la jurisdicción requerida por la ley colombiana. Esto puede requerir el uso de Nubes Soberanas o una estricta estrategia Híbrida.
Modelo de Responsabilidad Compartida	¿Qué capa de la seguridad es responsabilidad del proveedor y cuál de la entidad?	La entidad debe entender su responsabilidad en cada modelo de servicio (IaaS, PaaS, SaaS) e implementar políticas de Zero Trust y DevSecOps para la protección de sus datos, aplicaciones y configuraciones.
Alineación con el NIST CSF 2.0 [17]	¿Cómo se gestionará el riesgo continuo?	Las actividades de seguridad en la nube deben mapearse a las funciones del NIST CSF 2.0: Gobernar, Identificar, Proteger, Detectar, Responder y Recuperar (GOVERN, IDENTIFY, PROTECT, DETECT, RESPOND, RECOVER). El enfoque debe ser proactivo, centrado en la protección del dato y la identidad (Identity and Access Management – IAM).

Tabla Gobernanza, Seguridad y Cumplimiento Normativo

3.2.2. Viabilidad Técnica y Estrategia de Arquitectura

El enfoque debe ser la modernización (Cloud Native) y no simplemente la réplica de la infraestructura existente (Lift & Shift).

ENFOQUE	CRITERIO	ACCIÓN
Estrategia Multi-Cloud/Híbrida	¿Se requiere un solo proveedor o múltiples?	Se debe definir una estrategia que aproveche los beneficios de la Multi-Cloud (evitar vendor lock-in, resiliencia) y la Nube Híbrida (integración con sistemas legados on-premise y control de datos sensibles). La arquitectura debe ser portable usando estándares como Kubernetes.
Evaluación del Catálogo de Servicios (PaaS y Serverless)	¿El proveedor ofrece servicios avanzados para la innovación?	Se debe priorizar el uso de modelos PaaS y Serverless (en lugar de IaaS puro) para la construcción de nuevas aplicaciones, ya que maximizan la escalabilidad, reducen la carga operativa y mejoran la eficiencia. Se debe evaluar la madurez de los servicios de IA/ML del proveedor.
Conectividad y Desempeño (Latencia)	¿Cuál es la latencia requerida por la aplicación crítica?	Para servicios que requieren baja latencia (Edge Computing, sistemas en tiempo real), se debe evaluar la proximidad de las regiones de la nube y el uso de Conexiones Dedicadas (ExpressRoute, Direct Connect) para garantizar el rendimiento.

Tabla 3 Viabilidad Técnica y Estrategia

3.2.3. Gestión Económica y Optimización Continua (FinOps)

La gestión financiera en la nube requiere una disciplina continua que trascienda la simple comparación inicial de costos.

GESTIÓN	CRITERIO	ACCIÓN
FinOps (Gobernanza Financiera)	¿Cómo se controlará y optimizará el gasto elástico?	Implementar procesos FinOps desde el inicio. Esto incluye la visibilidad de costos mediante tagging (etiquetado) obligatorio de recursos, el establecimiento

GESTIÓN	CRITERIO	ACCIÓN
		de presupuestos y alertas, y la optimización continua del uso (apagado de recursos ociosos, compra de instancias reservadas).
Modelo de Facturación y Transparencia	¿El modelo de facturación es lo suficientemente granular y transparente?	Se debe asegurar que los reportes del proveedor permitan una asignación precisa de costos a las unidades de negocio, facilitando la rendición de cuentas.
Estrategia de Sostenibilidad (Green Cloud)	¿Cómo se integra el coste energético en la toma de decisiones?	La evaluación de costos debe incluir la consideración del consumo energético y la huella de carbono del proveedor, priorizando aquellos que se alineen con los objetivos de sostenibilidad del Estado.

Tabla 4 Gestión Económica y Optimización Continua

3.2.4. Modelo de Contratación y Adquisición

La forma en que se contrata el servicio debe reflejar la naturaleza dinámica y cambiante de la nube.

ASPECTO	CRITERIO	ACCIÓN
Acuerdos de Nivel de Servicio (SLA)	¿El SLA cubre las métricas críticas del servicio gubernamental?	Se deben revisar los acuerdos de disponibilidad, tiempo de respuesta y garantía de soporte. Para servicios críticos (SaaS), el SLA debe ser riguroso.
Garantía de Portabilidad y Salida	¿Qué tan fácil es cambiar de proveedor o revertir la migración?	Se deben incluir cláusulas que garanticen la portabilidad de los datos y la transferencia de las cargas de trabajo a otro proveedor o de vuelta a un entorno on-premise sin penalizaciones excesivas, reforzando la Neutralidad Tecnológica.

ASPECTO	CRITERIO	ACCIÓN
Regulaciones de Contratación Pública (CCE)	¿Cómo se utilizan los Acuerdos Marco IV y V?	Se debe asegurar que la adquisición de servicios se realice a través de los Acuerdos Marco de CCE aplicables (Nube Privada, Nube Pública IV, Nuevos AM), aprovechando los términos negociados y estandarizados por el Estado.

Tabla 5 Contratación y Adquisición

3.2.5. Aprovechamiento de servicios

Dentro del ámbito de la Gestión de Servicios [5], que significa proveer, acondicionar y habilitar un servicio, para que el usuario final se pueda beneficiar con él, satisfaciendo sus requerimientos con la calidad acordada. En otras palabras, el aprovisionamiento de servicios de computación en la nube debe ser provisto bajo demanda acorde con los acuerdos de nivel de servicios y demás condiciones contractuales, de una manera eficiente en tiempo, costo y uso de recursos. [13]

Como se mostró anteriormente, una de las características esenciales de la computación en la nube es el Autoservicio bajo demanda (On-demand self-service) donde un consumidor puede de manera unilateral proveer capacidades de computación (almacenamiento, procesamiento entre otros) según sea necesario o automáticamente, prácticamente sin interacción con el proveedor de servicios. Por lo anterior, es necesario aclarar que los Acuerdos Marco (AM) de Nube Pública y Nube Privada II generación, habilitados por Colombia Compra Eficiente, buscan ser instrumentos que faciliten la adquisición de estos servicios para las Entidades del Estado, sin embargo, en concordancia con las leyes colombianas referentes al presupuesto y gasto público, esta característica esencial de autoaprovisionamiento es limitada según el valor y servicios definidos en las ordenes de compras emitidas por cada Entidad Estatal a través de la Tienda Virtual del Estado Colombiano (TVEC). Así pues, es necesario que las entidades del Estado tengan en cuenta esta limitante al momento de adquirir servicios de Nube Pública y Nube Privada a través de los AM de TI.

3.2.6. Migración y portabilidad

Las organizaciones que revisan como alternativa la computación en la nube, deben ser conscientes que pueden tener que cambiar de proveedor en el futuro, en especial si se utilizan servicios de computación en la nube contratados a través de los Acuerdos Marco de TI, en donde, dado que se tiene un bien o servicio de características uniformes, el único diferenciador que queda es el precio, de manera



que el proceso de adjudicación se da al proveedor que cotee el menor valor por los servicios de nube solicitados y cotizados a través de la Tienda virtual del Estado Colombiano (TVEC) y dicha adjudicación no siempre se realiza por el periodo de vigencia del AM, el cual puede ser en algunos casos de 2 años prorrogable a 3, si no que corresponde más a las condiciones de planificación de cada entidad.

La contratación de servicios de computación en la nube por parte de las entidades públicas debe garantizar la portabilidad de los datos entre los prestadores de servicios en el menor tiempo posible. Deben existir reglas claras que permitan a la entidad propietaria de la información (contratante) acceder a toda su información y poderla migrar nuevamente a sus sistemas o a otros proveedores del servicio con total garantía de la integridad de la información y sin incurrir en costos adicionales [11] [12].

Para ello deben existir cláusulas que garanticen que, al término del contrato ya sea por decisión del contratante, del proveedor del servicio, por eventos tales como quiebra o insolvencia entre otros, toda la información suministrada por los usuarios y almacenada por los proveedores pueda ser restituida a los usuarios o a terceros designados por estos, recuperada por los usuarios con herramientas provistas por el proveedor, sin contratiempos. La migración y la portabilidad suelen ser parte del plan de continuidad de las entidades.

3.2.7.Escalonamiento

Hay que tener presente que no es necesario migrar de inmediato ni en su totalidad todos los servicios de tecnologías de la información (TI) a la nube. Se recomienda realizar este paso gradualmente e iniciar con pequeños pasos. Para mover los servicios a la nube hágase los siguientes cuestionamientos:

- ¿Qué vale la pena migrar a la nube de manera inmediata?
- ¿Qué puede esperar?
- ¿Qué aplicaciones es preferible mantener internas en el futuro previsible?

Este abordaje permite que se migren a la nube las aplicaciones que determine la entidad, manteniendo (sin migrar a la nube) las que según el caso se considere adecuado mantener alojadas en centros de datos propios.

3.2.8.Seguridad

Es fundamental reconocer que la seguridad es un aspecto transversal de la arquitectura que abarca todas las capas del modelo de nube según NIST [3] descrito en este documento, desde la seguridad física hasta la seguridad de las aplicaciones. Por lo tanto, las preocupaciones de seguridad en la arquitectura de computación en nube no están únicamente bajo el control de los Proveedores de Nube, sino también de los Consumidores de Nube y otros actores relevantes.



Los sistemas basados en la nube todavía necesitan abordar los requisitos de seguridad como autenticación, autorización, disponibilidad, confidencialidad, administración de identidad, integridad, auditoría, monitoreo de seguridad, respuesta a incidentes y administración de políticas de seguridad.

Aunque estos requisitos de seguridad no son nuevos, discutimos las perspectivas específicas de la nube para ayudar a discutir, analizar e implementar la seguridad en un sistema de nube [10] [11] [12].

Una forma de ver las implicaciones de seguridad desde la perspectiva del modelo de implementación es el diferente nivel de exclusividad de los usuarios en un modelo de implementación. Una nube privada está dedicada a una organización de consumidores, donde una nube pública podría tener usuarios impredecibles coexistiendo entre sí, por lo tanto, el aislamiento de la carga de trabajo es menos un problema de seguridad en una nube privada que en una nube pública (se debe tener en cuenta que los protocolos de seguridad de estas nubes se encuentran definidos en su mayoría con estándares o buenas prácticas internacionales que aseguran menos problemas de seguridad). Otra forma de analizar el impacto en la seguridad de los modelos de despliegue en la nube es usar el concepto de límites de acceso. Por ejemplo, una nube privada en el sitio puede o no necesitar controladores de límites adicionales en el límite de la nube cuando la nube privada se aloja en el sitio dentro del límite de la red de la organización de consumidor de nube, mientras que una nube privada externalizada tiende a requerir el establecimiento de tal protección perimetral en el límite de la nube [10] [11] [12].

Así mismo, es necesario hablar de seguridad compartida dado que el proveedor y el consumidor de nube tienen diferentes grados de control sobre los recursos informáticos de un sistema de nube [14]. En comparación con los sistemas de TI tradicionales, donde una organización tiene control sobre toda la pila de recursos informáticos y todo el ciclo de vida de los sistemas, los proveedores de nube y los consumidores de nube diseñan, construyen, implementan y operan sistemas basados en la nube.

La división del control significa que ambas partes ahora comparten las responsabilidades de proporcionar protecciones adecuadas a los sistemas basados en la nube. La seguridad es una responsabilidad compartida. Los controles de seguridad, es decir, las medidas utilizadas para proporcionar protecciones necesitan ser analizados para determinar qué parte está en mejor posición para implementar. Este análisis debe incluir consideraciones desde la perspectiva de un modelo de servicio, donde diferentes modelos de servicio implican diferentes grados de control entre los proveedores y los consumidores de nube. Por ejemplo, los controles de administración de cuenta para usuarios privilegiados del sistema inicial en escenarios IaaS normalmente son realizados por el Proveedor, mientras que la administración de cuentas de usuarios de aplicaciones para la aplicación desplegada en un entorno IaaS normalmente no es responsabilidad del proveedor [10] [11] [12].



3.2.9.Privacidad

Los proveedores de nube deben proteger la recopilación, el procesamiento, la comunicación, el uso y la disposición de la información personal y de la información de identificación personal en la nube de acuerdo con la normatividad vigente [14].

De acuerdo con las leyes colombianas de privacidad y tratamiento de datos personales, la información personal puede usarse para distinguir o rastrear la identidad de una persona, como su nombre, servicios parafiscales, registros biométricos etc. Aunque la computación en nube ofrece una solución flexible para recursos compartidos, software e información, también plantea desafíos de privacidad adicionales a los consumidores que usan las nubes.

3.2.10. Gestión de incidentes

Se debe definir de manera explícita y clara el proceso o procedimiento para la gestión de incidentes en donde el proveedor de nube le informe al contratante si ha ocurrido algún incidente con el servicio o se ha puesto en riesgo la seguridad de la información. El procedimiento debe indicar:

- Acciones y secuencia de las acciones a seguir durante el procedimiento
- Responsables e interlocutores,
- Tipología de incidentes incluidos en el servicio
- Procedimientos específicos ante incidentes de seguridad
- Tiempos de respuesta y resolución de incidentes
- Gestión y resolución de incidentes, entre otros que defina el proveedor de nube. [13]

3.2.11. Gestión de cambios

Las entidades deberán establecer contractualmente la obligación de mantener actualizados los sistemas para garantizar el correcto funcionamiento de estos, así como eliminar las posibles vulnerabilidades que pueden afectar los servicios de computación en la nube prestados. Para ello se podrá definir un procedimiento de coordinación en el mantenimiento de la infraestructura que soporta los servicios entre ambas partes para prevenir interrupciones o errores en la prestación del servicio; este procedimiento debe incluir la notificación con suficiente antelación de la realización de mantenimientos por parte del proveedor, identificando los tiempos en los que puede interrumpirse el servicio. La notificación deberá realizarse previa y posteriormente al mantenimiento y tras éste la entidad contratante deberá notificar la conformidad del correcto funcionamiento del servicio. [7]

Así mismo, siempre que el mantenimiento o actualización implique un cambio mayor o pueda suponer el funcionamiento incorrecto de los sistemas de la organización cliente o entidad contratante del servicio, la entidad deberá solicitar al proveedor la



habilitación de un entorno actualizado de pruebas que permita verificar el correcto funcionamiento de sus sistemas en preproducción. Se debe exigir a los proveedores informar periódicamente de los mantenimientos y actualizaciones realizados en los sistemas que albergan los sistemas del cliente.

3.2.12. Asuntos legales relacionados con la residencia física de los datos

El contratante debe asegurarse de que siempre tendrá la propiedad y el control de su información independientemente del lugar donde se almacenen los datos. Las entidades deberán evaluar y revisar el marco normativo vigente en esta materia. [13].

3.2.13. Servicio totalmente dependiente de una conexión a internet

Contratación de un mayor ancho de banda en la empresa cliente e implementación de políticas de calidad de servicio o conexiones alternas, para evitar problemas de cuellos de botella en el acceso a las aplicaciones, o accesibilidad lenta que puedan poner en juego el desempeño de las aplicaciones. Se recomienda actualizar los planes de capacidad sobre los servicios de TI y revisar condiciones técnicas como el ancho de banda, latencia del servicio y tecnologías a utilizar. Se aclara que, para nubes privadas, híbridas o comunitarias, el servicio se puede prestar a través de redes MPLS, Metroethernet entre otras.

3.2.14. Planes de continuidad del negocio (BCP) y recuperación de desastres (DRP)

Dependiendo la criticidad del servicio, los clientes o entidades contratantes pueden inspeccionar y hacer parte de las pruebas de los planes de recuperación de catástrofes y de continuidad del negocio del proveedor en la nube (sin ir en contra de los acuerdos de confidencialidad establecidos con los usuarios). Así mismo, se deben integrar a los planes de continuidad y recuperación de la entidad contratante con los planes de continuidad del negocio y recuperación del proveedor. [7]

3.2.15. Acuerdos de Nivel de servicio (ANS)

Para todos los servicios de computación en la nube se deben establecer acuerdos de nivel de servicio donde se detallen aspectos como: controles, reglamentación a cumplir, medidas de protección y seguridad, plazos de recuperación del servicio, indicadores y forma de medición de indicadores de calidad del servicio, valores mínimos aceptables de los mismos, tiempos de respuesta ante una eventual falta de disponibilidad, penalizaciones y el régimen de responsabilidad por los daños y perjuicios ocasionados por un incumplimiento del proveedor, las limitaciones al servicio o a sus garantías, solicitudes de cambio, gestión de incidentes, la regulación de la seguridad y el tratamiento de datos de carácter personal y las causas de terminación del servicio/contrato entre otros aspectos que se consideren. Se recomienda revisar las fichas técnicas de los Acuerdos Marco de TI, las cuales



contienen criterios y niveles de servicio mínimos definidos por el Estado colombiano. [13]

3.2.16. Reputación y solvencia del proveedor de servicios

Este criterio no solo aplica para servicios de computación en la nube, sino para cualquier servicio o bien a comprar. Se debe revisar la experiencia, la relación con los clientes, la estabilidad financiera del proveedor y su reputación.

3.2.17. Cláusulas de derechos de proveedores y limitación de responsabilidad

Se debe poner especial atención a aquellas cláusulas incluidas en los términos de acceso a los servicios en la nube que puedan otorgar a los proveedores de servicios derechos sobre la información que pueda estar alojada en sus servidores, cualquiera que sea el propósito de ellas. Así mismo, deben examinarse con mucho cuidado las cláusulas de limitación de responsabilidad de los proveedores de los servicios por incumplimiento de las obligaciones esenciales que surgen de la relación de servicios con los usuarios. Tales cláusulas podrían afectar adversamente a los usuarios que trasladen información reservada o confidencial a la nube y a aquellos que puedan experimentar daños resultantes de incumplimientos en los términos de prestación de los servicios, sin embargo, estas cláusulas no impiden la contratación de servicios en la nube. [13]

3.2.18. Formato de autodiagnóstico como actor de la nube

El anexo denominado: "Formato de autodiagnóstico como actor de la nube" debe entenderse e interpretarse como una manera rápida de evaluar si los servicios ofrecidos por un actor determinado de la nube cumplen con lo definido en esta guía. De acuerdo con esto, es necesario que este formato sea diligenciado por los responsables TI de la organización y sea anexada toda la documentación necesaria que pruebe que dicho servicio ofrecido realmente es un servicio de computación en la nube. La información allí contenida se debe asegurar con la firma del responsable TI y debe ser salvaguardada para los diferentes fines en que pueda ser usada (auditorías, revisiones y demás).

Es necesario aclarar que cualquier servicio de computación en la nube en esencia debe cumplir con las cinco características esenciales antes descritas, alguno de los tres modelos de servicio y como mínimo desplegado en alguno de los cuatro modelos de implementación. Por lo anterior, en caso de que se evidencie la falta de alguno de estos mediante el formato en cuestión, se da por entendido que dicho servicio ofrecido está incompleto y necesita la implementación de soluciones que completen los requisitos para ser diagnosticado de manera satisfactoria. También es necesario que la organización asegure la trazabilidad de este formato y los cambios realizados en los servicios de computación en la nube, con el fin de presentar reportes si son requeridos por un auditor de nube o cualquier otra entidad competente.



Este autodiagnóstico está dirigido, por ahora, únicamente a los actores: consumidor y proveedor de nube.

El consumidor de nube podrá diligenciarlo para reconocer que el servicio que está contratando con el proveedor sí es un servicio de computación en la nube. En cualquier momento el consumidor de nube podrá informar al proveedor su inconformidad o dudas en cuanto a la prestación del servicio y clasificación del servicio.

El proveedor de nube deberá cumplir los requisitos mínimos del formato, así como también los requisitos mínimos de: gestión del servicio, portabilidad, y seguridad y privacidad [14]. Deberá anexar toda la documentación necesaria asegurando la veracidad de la información en las respuestas dadas. Para los “requisitos a tener en cuenta u opcionales”, el proveedor deberá establecer un plan de trabajo que le permita cumplirlos en el mediano plazo.

Así mismo, no se podrán auto diagnosticar los actores: auditor, corredor y operador de nube. En el caso del auditor y operador: los servicios, aunque son necesarios para garantizar un entorno de alto nivel de computación en la nube, estos no están catalogados dentro de los modelos de servicio, por ejemplo, el servicio de conectividad del operador (redes, internet, redes privadas de transporte de datos entre otros) es necesario para que la computación en la nube sea una realidad, sin embargo, este no es SaaS, PaaS o IaaS.

Por lo anterior, buscando tener un nivel de madurez en el tiempo acorde a las capacidades tecnológicas de los actores de la nube citados anteriormente, el Ministerio de TIC ha decidido no clasificarlos. En el caso del corredor o agente de nube, tampoco podrá auto diagnosticarse en virtud de que, si bien sus actividades hacen parte del modelo de referencia de NIST en una etapa avanzada y madura de la computación en la nube, dichas actividades tampoco son consideradas modelos de servicio. Sin embargo, dentro de la ruta de definición e implementación de la computación en la nube en Colombia liderada por el Ministerio TIC, se tendrán en cuenta todas las normas técnicas y las posibilidades tecnológicas (incluyendo todos los actores y actividades, estándares, entre otros) de un entorno de alto nivel que aseguren el grado de madurez esperado para los próximos años.

Nota: El auditor de nube, podrá ser una tercera parte (otra organización), o un área funcional del mismo proveedor que presta servicios en la nube. Se deberá asegurar la trazabilidad de las actividades de verificación y/o auditoria buscando así el cumplimiento de los ANS pactados y la mejora continua de los servicios. Así mismo, los servicios de auditoria si bien son necesarios para garantizar un entorno de nube de alto nivel, estos no están catalogados dentro los modelos de servicio antes citados.



4. NUEVAS TECNOLOGÍAS Y ESTADO DEL ARTE

4.1. LA INTELIGENCIA ARTIFICIAL (IA) SE CONVIERTE EN EL NÚCLEO

La convergencia de la Inteligencia Artificial (IA) y la Computación en la Nube es la base sobre la que se construirá la próxima generación de infraestructura tecnológica. La nube proporciona la potencia de cómputo y los datos necesarios para que la IA prospere, mientras que la IA inyecta inteligencia y automatización en cada capa de la nube.

Las plataformas de nube serán el epicentro para entrenar y desplegar modelos fundacionales y de IA generativa (como GPT). Los grandes proveedores (AWS, Azure, Google Cloud) están invirtiendo en hardware especializado (como las TPUs) para acelerar este proceso. La IA también automatizará las tareas de gestión de la nube (escalado, asignación de recursos, optimización de costes y mitigación de amenazas), llevando a una infraestructura más eficiente y autogestionada. Además, para mayor facilidad, cualquier empresa podrá implementar IA y ML sin la necesidad de un equipo especializado.

4.1.1. AIOps: La Nube Autogestionada

AIOps representa un cambio de paradigma de la gestión reactiva de TI a una gestión predictiva y proactiva, utilizando algoritmos de Machine Learning (ML) para automatizar y mejorar las operaciones.

- **Monitoreo Inteligente y Detección de Anomalías:** En lugar de depender de umbrales manuales, los modelos de IA analizan miles de millones de puntos de datos de telemetría (logs, métricas, trazas) en tiempo real para aprender el comportamiento "normal" del sistema. Esto permite detectar anomalías sutiles (por ejemplo, una caída anómala en el rendimiento de un microservicio) que preceden a una falla mayor, mucho antes de que un humano lo note.
- **Correlación de Eventos:** En entornos Multi-Cloud o híbridos, un solo problema puede generar miles de alertas. La IA agrupa y correlaciona estas alertas en un evento único, identificando la causa raíz del problema (por ejemplo, "un error de latencia está siendo causado por la degradación del disco en el servidor X de la Región Y"), reduciendo el tiempo de resolución (MTTR).
- **Respuesta Automatizada:** Los sistemas AIOps no solo alertan, sino que activan acciones correctivas automáticamente, como reiniciar un contenedor fallido, balancear la carga o escalar recursos.

4.1.2. Optimización de Recursos y FinOps Inteligente

- El coste y la eficiencia energética son desafíos clave en la nube. La IA se ha convertido en la herramienta principal para la optimización financiera (FinOps) y operativa.



- **Escalado Predictivo y Dinámico:** Los modelos de ML predicen con precisión las fluctuaciones de la demanda (tráfico, uso de recursos) a corto y medio plazo. Esto permite que los recursos de la nube (máquinas virtuales, capacidad de almacenamiento, bases de datos) se escalen hacia arriba o hacia abajo antes de que ocurra un pico o una caída de tráfico, maximizando la utilización y minimizando el gasto en recursos infrautilizados.
- **Optimización de Carga de Trabajo:** La IA asigna cargas de trabajo al tipo de instancia o región de nube más adecuado en función de criterios de rendimiento, coste y sostenibilidad. Por ejemplo, puede mover tareas por lotes no críticas a regiones con energía renovable en momentos de baja demanda para reducir la huella de carbono y el coste.

4.1.3.Seguridad Predictiva

La superficie de ataque crece exponencialmente con los entornos de nube distribuidos. La IA actúa como la primera línea de defensa.

- **Detección de Amenazas de Día Cero:** Los algoritmos de ML analizan patrones de tráfico, comportamiento de usuarios (UEBA) y configuraciones de red para identificar actividades maliciosas que no coinciden con ninguna firma de malware conocida, detectando ataques sofisticados en tiempo real.
- **Políticas de Zero Trust Dinámicas:** La IA evalúa continuamente el riesgo de una sesión de usuario. Si detecta un comportamiento anómalo (por ejemplo, el acceso a un archivo sensible desde una ubicación inusual), el sistema puede requerir automáticamente volver a realizar la autenticación o revocar el acceso, aplicando los principios de confianza cero de manera adaptativa.

4.1.4.Innovación Impulsada por la IA en la Nube

La nube moderna ya no es solo la infraestructura para la IA; es el facilitador que democratiza el acceso a la inteligencia más avanzada, impulsando una ola de innovación empresarial.

4.1.5.El Impacto de la IA Generativa (GenAI)

Los modelos fundacionales y la IA generativa son, sin duda, la tendencia dominante para los próximos cinco años, y su existencia depende casi por completo de la nube.

- **Plataformas de Modelos Fundacionales:** Los proveedores de nube (AWS, Azure, GCP) ofrecen plataformas que permiten a las empresas acceder, ajustar (mediante *fine-tuning* o RAG) y desplegar modelos de lenguaje grande (LLMs) pre-entrenados para tareas específicas, sin la necesidad de invertir miles de millones en entrenamiento desde cero. Esto convierte a la GenAI en una capacidad accesible.



- **Aplicaciones Nativo-IA (AI-Native):** La nube facilita la creación de una nueva clase de aplicaciones diseñadas desde cero con la IA en su núcleo. Esto incluye agentes de servicio al cliente totalmente automatizados, herramientas de desarrollo de código asistidas por IA e incluso la generación de datos sintéticos para el entrenamiento de otros modelos.
- **Democratización del Desarrollo:** El uso de IA para generar código (como *Copilots*) y simplificar la gestión de la infraestructura (Infraestructura como Código asistida por IA) reduce drásticamente las barreras de entrada para los desarrolladores y acelera el tiempo de comercialización.

4.1.6.MLOps: Industrializando la Inteligencia

El MLOps (Machine Learning Operations) es el conjunto de prácticas y herramientas en la nube que automatiza y gestiona el ciclo de vida completo de los modelos de ML, desde el desarrollo hasta la producción.

- **Pipelines de Despliegue Automatizado:** Las herramientas de MLOps en la nube permiten a los científicos de datos pasar un modelo de la experimentación a la producción en minutos, gestionando automáticamente el versionado, las pruebas y el despliegue en contenedores.
- **Monitoreo de Deriva (Drift):** La nube monitorea continuamente el rendimiento de un modelo en producción. Si el modelo comienza a degradarse (la "deriva del modelo"), el MLOps automatiza el entrenamiento iterativo con nuevos datos y el redespliegue de la versión actualizada, asegurando que el modelo mantenga su precisión y valor empresarial.

4.1.7.Nubes Verticales e IA Específica de la Industria

La IA en la nube se está volviendo menos genérica más especializada y adaptada a los desafíos únicos de cada sector.

- **Salud (Healthcare):** Nubes específicas que ofrecen IA para el diagnóstico por imágenes (visión artificial) o la investigación de fármacos, cumpliendo rigurosamente con normativas de privacidad de datos (HIPAA).
- **Finanzas (Fintech):** Soluciones de IA para detección de fraudes en tiempo real, análisis de riesgos crediticios con modelos explicables y compliance regulatorio automatizado.
- **Manufactura:** Plataformas de IA en la nube que analizan datos de sensores de equipos (IoT) para mantenimiento predictivo y optimización de la cadena de suministro, reduciendo el tiempo de inactividad de las máquinas.

4.2. EL AUGE DEL CLOUD NATIVO Y SERVERLESS

La forma en que se construyen y ejecutan las aplicaciones seguirá evolucionando hacia arquitecturas que aprovechan al máximo la nube.



4.2.1. Cloud Native

Construir aplicaciones que utilizan microservicios, contenedores (como Kubernetes) y CI/CD se convertirá en el estándar. El enfoque Cloud Native es una metodología para construir y ejecutar aplicaciones que aprovechan al máximo el modelo de cloud computing. Para las empresas de gobierno, la adopción de Cloud Native es un imperativo para modernizar los servicios públicos, mejorar la eficiencia y responder con agilidad a las necesidades ciudadanas. Cloud Native se basa en varios pilares tecnológicos y culturales que redefinen el desarrollo de software:

- **Contenedores (Containers):** Uso de tecnologías como Docker y Kubernetes para empaquetar una aplicación y todas sus dependencias. Esto garantiza que el software se ejecute de manera idéntica en cualquier entorno (desarrollo, prueba, producción, nube pública, nube privada gubernamental).
- **Microservicios:** Descomposición de grandes aplicaciones monolíticas en servicios más pequeños, independientes y desplegables. Por ejemplo, en lugar de un único sistema de gestión de impuestos, se tienen microservicios separados para "cálculo de deudas", "gestión de pagos" y "autenticación de usuarios".
- **CI/CD (Integración y Despliegue Continuos):** Automatización de todo el ciclo de vida de la aplicación, permitiendo que las nuevas características se lancen de manera rápida y fiable, a menudo varias veces al día.
- **DevOps y DevSecOps:** Un cambio cultural que une a los equipos de desarrollo y operaciones. DevSecOps añade la seguridad como una preocupación continua y automatizada en cada fase del desarrollo.
- **Computación sin Servidor (Serverless):** Funciones como Servicio (FaaS) ganarán aún más popularidad. Esto permite a los desarrolladores enfocarse puramente en el código, sin preocuparse por la infraestructura subyacente, lo que impulsa la agilidad y reduce costes.

Beneficio	Descripción y Aplicación en el Gobierno	Aplicación
Agilidad en la Respuesta Ciudadana	Permite a las entidades lanzar rápidamente nuevos servicios digitales o modificar los existentes en semanas o días, en lugar de meses.	Desplegar una nueva plataforma de ayuda social en respuesta a una emergencia o actualizar formularios de impuestos anualmente sin interrumpir el servicio.
Resiliencia y Confiabilidad	Los microservicios y contenedores están diseñados para ser resistentes a fallas. Si un microservicio falla (por ejemplo, el de consulta de	Garantizar la disponibilidad de los portales de trámites y servicios esenciales 24/7, incluso bajo picos de tráfico.



Beneficio	Descripción y Aplicación en el Gobierno	Aplicación
	multas), el resto del sistema (por ejemplo, el de renovación de licencias) sigue funcionando.	
Escalabilidad Elástica	El gobierno experimenta grandes fluctuaciones de demanda (declaración de impuestos, elecciones, inscripción a programas). Cloud Native permite escalar automáticamente los recursos en los picos y reducirlos en los valles, optimizando el uso de recursos.	Manejo eficiente de millones de solicitudes simultáneas en periodos críticos.
Optimización de Costos (OpEx)	Al usar contenedores y tecnologías <i>serverless</i> , las entidades solo pagan por el cómputo exacto que consumen (modelo <i>pay-as-you-go</i>), en lugar de comprar y mantener servidores para capacidad máxima.	Reducción del gasto operativo de TI al no incurrir en costes de infraestructura subutilizada.
Seguridad por Diseño (DevSecOps)	La seguridad se integra en el código desde el inicio. Los contenedores inmutables, por ejemplo, aseguran que, si se detecta un compromiso, el contenedor simplemente se destruye y se reemplaza con una copia limpia y verificada.	Mayor protección de datos sensibles de los ciudadanos y cumplimiento de rigurosos estándares de seguridad y privacidad.

Tabla 6 Beneficios de Cloud Native

La transición de los sistemas legados monolíticos a un entorno Cloud Native presenta desafíos únicos en el sector público tales como:

- **Sistemas Legados (Legacy):** La mayoría de los sistemas esenciales de gobierno son antiguos y monolíticos. Migrarlos a microservicios es complejo y requiere una estrategia de modernización gradual.
- **Habilidades y Talento:** El equipo y talento humano con experiencia en Kubernetes, DevOps y lenguajes de programación modernos a menudo es escaso en las plantas de personal de TI gubernamental.



- **Cumplimiento Normativo y Soberanía:** Las regulaciones de privacidad y soberanía de datos obligan a que ciertas cargas de trabajo residan en nubes privadas gubernamentales o en regiones específicas, lo que complica la gestión Multi-Cloud.

Para superar estos obstáculos, las entidades gubernamentales deben enfocarse en:

Estrategia	Descripción
Adoptar Contenedores Primero	Comenzar empaquetando aplicaciones monolíticas existentes en contenedores. Esto proporciona los beneficios de portabilidad de la nube sin tener que reescribir toda la aplicación (aún no son microservicios, pero es un paso hacia la modernización).
Inversión en Capacitación (Upskilling)	Crear programas intensivos de capacitación y certificación en DevOps, Kubernetes y MLOps para el personal existente, o establecer alianzas con el sector privado para cubrir la brecha de talento.
Gobernanza de Kubernetes	Implementar plataformas de gestión centralizada (como Kubernetes) que permitan a los desarrolladores de múltiples agencias consumir la infraestructura de manera estandarizada y segura. Esto garantiza la uniformidad en todo el ecosistema de TI del gobierno.
DevSecOps Obligatorio	La seguridad debe ser una línea de acción no negociable. Automatizar escaneos de vulnerabilidades, gestión de identidad y políticas de cumplimiento <i>dentro</i> del <i>pipeline</i> de CI/CD para garantizar la integridad y privacidad de los servicios ciudadanos.

Tabla 7 Estrategia para adoptar Cloud Native

Cloud Native es la arquitectura ideal para las empresas de gobierno que buscan dejar atrás la rigidez de los sistemas legados y adoptar una cultura de innovación, agilidad y eficiencia para servir mejor a sus ciudadanos.

4.3. EDGE COMPUTING Y BAJA LATENCIA

La computación en el borde o Edge Computing es la práctica de procesar datos en la ubicación más cercana a donde se crean o consumen, en lugar de enviarlos a un centro de datos centralizado o a la nube. En el sector gubernamental, donde la toma de decisiones rápidas, la seguridad y la cobertura geográfica son esenciales. La principal ventaja del Edge es la baja latencia, es decir, el tiempo mínimo que tarda una solicitud en viajar del dispositivo al punto de procesamiento y volver con una respuesta. Esto es vital para las aplicaciones críticas del sector público. El



procesamiento de datos se moverá más cerca de donde se generan, lo cual es crucial para tecnologías que requieren respuestas casi instantáneas.

El Edge Computing no reemplaza a la nube central, sino que la complementa en una arquitectura distribuida llamada Edge Cloud Mesh.

4.3.1. Aplicaciones Críticas de Baja Latencia en el Gobierno

La necesidad de una respuesta instantánea impulsa la adopción de Edge Computing en varios dominios gubernamentales.

4.3.1.1. Seguridad Pública y Respuesta a Emergencias

- **Vigilancia Inteligente y Análisis de Video:** Las cámaras de seguridad y las cámaras corporales de la policía pueden procesar flujos de video localmente en el borde para detectar actividades sospechosas (objetos abandonados, multitudes inusuales) o identificar personas buscadas mediante reconocimiento facial. El procesamiento local evita el cuello de botella de la red y permite enviar alertas instantáneas a los agentes.
- **Gestión de Desastres y Tráfico:** Sensores Edge desplegados en carreteras pueden analizar las condiciones del tráfico en tiempo real y coordinar automáticamente los semáforos para abrir rutas de evacuación durante una emergencia. La comunicación es local y directa, sin depender de la red central.

4.3.1.2. Infraestructura Crítica y Servicios Esenciales

- **Mantenimiento Predictivo de Servicios:** Sensores en la red eléctrica, tuberías de agua o infraestructura de transporte público analizan constantemente vibraciones, temperaturas y flujos. El Edge Computing procesa estos datos para predecir fallas inminentes (una bomba a punto de fallar), permitiendo el mantenimiento proactivo y evitando cortes costosos y peligrosos.
- **Gestión de Redes de Suministro (Smart Grids):** La baja latencia es vital para balancear la carga de la red eléctrica en tiempo real, respondiendo a la demanda fluctuante de fuentes de energía renovable y previniendo apagones.

4.3.1.3. Defensa y Operaciones Militares

- **Procesamiento de Datos en el Campo:** Unidades desplegadas pueden usar dispositivos Edge robustos para procesar datos de inteligencia (imágenes satelitales, datos de drones) localmente, tomando decisiones operacionales en tiempo real sin tener que conectarse a un centro de mando distante.

4.3.2. La Arquitectura Edge Cloud Mesh

El Edge Computing no reemplaza a la nube central, sino que la complementa en una arquitectura distribuida llamada Edge Cloud Mesh.

Componente	Función en la Arquitectura de Gobierno
Borde (Edge)	El procesamiento ocurre en tiempo real (una cámara detectando un incendio). Se utiliza para tareas de baja latencia y volumen alto de datos.
Nube Central	Los modelos de IA se entrenan con grandes volúmenes de datos históricos (años de incidentes de tráfico) y donde se gestiona, se actualiza y se despliega el software a todos los dispositivos Edge.
Conectividad	los datos críticos del Edge se replican de forma segura en la nube central, y que las actualizaciones de los modelos se envíen al Edge de manera eficiente.

Tabla 8 Arquitectura Edge Cloud Mesh para Gobierno

4.3.2.1. El papel de la IA

La Inteligencia Artificial es el motor del Edge Computing gubernamental. Los modelos se desarrollan en el poder de cómputo de la nube y luego se llevan a los dispositivos Edge para que realicen la inferencia localmente.

- **Edge AI:** La combinación de Edge Computing (procesamiento en el borde, cerca de dispositivos IoT, fábricas, o puntos de venta) con IA permitirá tomar decisiones en tiempo real (por ejemplo, en vehículos autónomos, robótica industrial o análisis de transmisiones en directo).

4.3.3. Claves de la Adopción en el Gobierno

Implementar Edge Computing a gran escala en el sector público conlleva algunos retos específicos:

- **Estandarización y Vendor Lock-in:** La diversidad de hardware Edge puede llevar a silos tecnológicos. El gobierno necesita una estrategia que utilice plataformas estandarizadas como Kubernetes para el Edge para garantizar la interoperabilidad y evitar la dependencia de un solo proveedor.
- **Costos Operacionales (OpEx):** Si bien el Edge reduce la latencia, el costo de mantener y actualizar hardware físico distribuido puede ser significativo. Es crucial que la optimización de costes y la estrategia de FinOps consideren la vida útil y la gestión del ciclo de vida de los dispositivos Edge.
- **Seguridad y Gestión de Dispositivos:** Administrar, monitorear y actualizar miles o millones de dispositivos Edge dispersos geográficamente es un desafío logístico y de seguridad. Cada dispositivo Edge es un punto de entrada potencial a la red. El gobierno debe implementar soluciones robustas de gestión remota y seguridad de Zero Trust.



- **Consideraciones de Privacidad:** El procesamiento local de datos sensibles como imágenes o datos biométricos en el Edge reduce el riesgo de transmisión, pero requiere marcos legales y técnicos muy estrictos para garantizar que los datos personales sean anonimizados o eliminados después del procesamiento.

El Edge Computing es fundamental para la transformación digital del gobierno, permitiendo que los servicios críticos sean más rápidos, seguros y accesibles justo donde se necesitan.

4.4. ESTRATEGIAS MULTI-CLOUD E HÍBRIDAS

La mayoría de las organizaciones utilizarán una mezcla de entornos para optimizar rendimiento, coste y cumplimiento normativo. Las estrategias Multi-Cloud e Híbrida se han convertido en el estándar para la modernización de TI en el sector público. Estos modelos de despliegue son cruciales para que las entidades gubernamentales puedan equilibrar la necesidad de innovación, la optimización de costes y, lo más importante, el riguroso cumplimiento de las normativas de seguridad y soberanía de datos.

4.4.1. Estrategia Híbrida: Un Puente Necesario

El modelo Híbrido combina la infraestructura de nube pública con la infraestructura local (on-premise o nube privada). Esta combinación es a menudo la primera y más práctica etapa de la migración a la nube para una entidad de gobierno. Para aplicar esta estrategia debemos tener en cuenta:

- **Soberanía y Datos Sensibles:** La principal razón para una estrategia híbrida es la gestión de datos clasificados o altamente sensibles (registros de ciudadanos, datos de seguridad nacional, información fiscal). El modelo permite que estos datos permanezcan en una nube privada o centro de datos local bajo control directo del gobierno, cumpliendo estrictas leyes de soberanía y residencia de datos.
- **Aprovechamiento de Inversiones Existentes:** Las agencias gubernamentales tienen enormes inversiones en centros de datos e infraestructura heredada o antigua (legacy). Una estrategia híbrida permite que estos sistemas continúen operando y sirviendo a cargas de trabajo estables, mientras que la nueva infraestructura y los servicios modernos se despliegan en la nube pública.
- **Escalabilidad en el Borde:** La nube híbrida facilita la extensión de los servicios al Edge Computing. Los datos pueden ser procesados localmente (en el borde, utilizando la infraestructura privada) y solo los resultados agregados y anonimizados se envían a la nube pública para análisis a gran escala.

Se utiliza una plataforma de orquestación (a menudo basada en Kubernetes) que actúa como un plano de control unificado, permitiendo a los administradores



gestionar los recursos en la nube pública y privada con las mismas herramientas y políticas.

4.4.2. Estrategia Multi-Cloud

El modelo Multi-Cloud implica el uso de múltiples proveedores de nube pública (por ejemplo, AWS, Azure, Google Cloud, Oracle Cloud) de manera simultánea. Es una estrategia puramente de nube que busca maximizar las ventajas competitivas de cada proveedor. Para su aplicación en el Sector Gubernamental debemos tener en cuenta:

- **Evitar el Bloqueo del Proveedor (Vendor Lock-in):** Al usar varios proveedores, el gobierno mantiene la capacidad de trasladar cargas de trabajo o de negociar mejores tarifas, evitando la dependencia total de una sola empresa tecnológica. Esto es crucial para la sostenibilidad financiera a largo plazo.
- **Mejor en su Clase (Best-of-Breed):** Cada proveedor de nube sobresale en áreas específicas.
- Una agencia podría usar el ecosistema de IA y Machine Learning de un proveedor para su análisis de datos. Mientras que podría usar otro proveedor para aplicaciones que requieren una integración profunda con sistemas operativos basados en Microsoft. Y un tercero para sus servicios de cómputo elástico de alta demanda.
- **Resiliencia y Recuperación de Desastres:** La Multi-Cloud ofrece un nivel superior de resiliencia. Si un desastre natural o un ciberataque afecta gravemente la infraestructura de un proveedor en una región, las cargas de trabajo esenciales pueden conmutar rápidamente a la infraestructura de otro proveedor, garantizando la continuidad de los servicios críticos (Disaster Recovery).
- **Cumplimiento Geográfico:** Algunos países requieren que los datos se almacenen en centros de datos específicos. El uso de múltiples proveedores con distintas huellas geográficas permite a la entidad gubernamental cumplir con estas leyes de residencia de datos.

4.4.3. La Convergencia de la Cloud Híbrida y Multi-Cloud

La tendencia más avanzada es la convergencia de ambas estrategias en un entorno complejo, pero altamente optimizado. Una entidad gubernamental moderna puede operar una arquitectura que incluye:

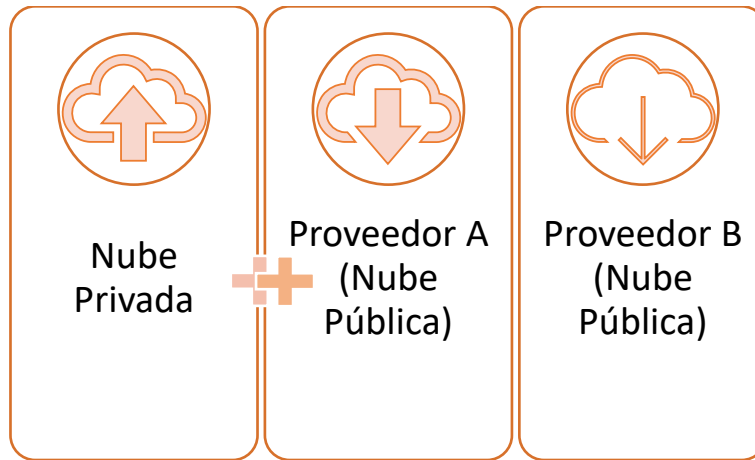


Figura 12 Implementación convergencia de la Cloud Híbrida y Multi-Cloud

Esto permite:

- **Flexibilidad Financiera:** Ejecutar las cargas de trabajo menos sensibles en el proveedor que ofrezca el mejor coste en un momento dado.
- **Seguridad y Control:** Mantener los datos más críticos en el entorno privado.
- **Innovación Rápida:** Utilizar la IA y los servicios especializados del proveedor más innovador para proyectos piloto o nuevas aplicaciones ciudadanas.

La clave del éxito para la administración pública en este modelo es la Orquestación. Se necesitan herramientas sofisticadas de gestión y observabilidad para asegurar que los microservicios se comuniquen de manera segura y eficiente a través de los diferentes entornos, manteniendo un estricto control sobre los costes y la seguridad en todo momento.

4.5. ENFOQUE EN SEGURIDAD, CUMPLIMIENTO NORMATIVO Y FINOPS

La complejidad de los entornos de nube exige nuevas prioridades de gestión. Para las empresas de gobierno, la migración a la nube va más allá de la tecnología; es un ejercicio de confianza pública, cumplimiento legal y responsabilidad fiscal. Por ello, la Seguridad, el Cumplimiento Normativo y el FinOps (Gestión Financiera de la Nube) se convierten en pilares estratégicos.

4.5.1. Zero Trust y DevSecOps

La naturaleza distribuida y abierta de la nube exige un cambio del perímetro de seguridad tradicional a un enfoque centrado en la identidad y el dato.



4.5.1.1. Modelo de Responsabilidad Compartida

Se debe entender claramente que la seguridad en la nube es un modelo de responsabilidad compartida.

- **Proveedor de Nube (CSP):** Es responsable de la seguridad de la nube (la infraestructura física, el hardware, la red del centro de datos).
- **Entidad Gubernamental:** Es responsable de la seguridad en la nube (los datos, las aplicaciones, la configuración de la red, la gestión de identidad y acceso).

Se debe auditar y asegurar activamente sus configuraciones de acceso (IAM) y cifrado, ya que los errores humanos en la configuración son la principal causa de brechas de seguridad.

4.5.1.2. Zero Trust (Confianza Cero)

La seguridad en el gobierno ya no puede basarse en confiar en todo lo que está dentro de la red. El modelo Zero Trust exige verificar explícita y continuamente a cada usuario, dispositivo y aplicación antes de otorgar acceso a cualquier recurso. Implementación rigurosa de la Autenticación Multifactor (MFA) para todos los empleados y el acceso a datos sensibles. Segmentación de la red para que, si una parte es comprometida, el atacante no pueda moverse lateralmente a otros sistemas críticos.

4.5.1.3. DevSecOps

La seguridad debe integrarse automáticamente en cada etapa del desarrollo de software. Es importante la automatización de escaneos de vulnerabilidades en el código y en las configuraciones de infraestructura como código (IaC) antes de que se desplieguen. Esto garantiza que las aplicaciones gubernamentales, como portales de trámites o bases de datos fiscales, se lancen con la seguridad integrada y no como un añadido de último momento.

4.5.2. Cumplimiento Normativo y Soberanía de Datos

Para las entidades de gobierno, el cumplimiento normativo se rige por leyes y políticas específicas (leyes de transparencia, protección de datos personales). La nube debe facilitar el cumplimiento, no complicarlo.

4.5.2.1. Soberanía y Residencia de Datos

Las leyes requieren que ciertos datos nacionales permanezcan geográficamente dentro de las fronteras del país. El gobierno debe seleccionar proveedores de nube que garanticen la residencia de datos en regiones específicas y que ofrezcan



soluciones de Nube Soberana (servicios de nube con gobernanza y acceso operativo limitado a las leyes y entidades nacionales).

4.5.2.2. Nubes Verticales para el Sector Público

Los proveedores de nube están desarrollando ofertas específicas para el sector público, a menudo llamadas Nubes Gubernamentales o Government Clouds. Estas plataformas ofrecen conjuntos de servicios que están certificados para cumplir con los estándares de seguridad y cumplimiento normativo más exigentes del gobierno (FedRAMP en EE. UU., o regulaciones locales de protección de datos), reduciendo la carga de auditoría de la agencia.

4.5.2.3. Auditoría y Trazabilidad Automatizada

La nube genera un rastro de auditoría completo (logs de acceso, logs de configuración, logs de red). Se debe hacer uso de servicios de gestión de logs y análisis de IA para monitorear automáticamente el cumplimiento de las políticas. Si una configuración de seguridad se desvía de la política aprobada (por ejemplo, una base de datos se vuelve accesible públicamente), el sistema notifica o corrige automáticamente la desviación, garantizando el cumplimiento continuo.

4.5.3. Gobernanza y Optimización Financiera

La nube no es más barata. Sin una gestión financiera estricta, los costes pueden dispararse. FinOps es una disciplina que combina finanzas, tecnología y negocios para llevar la responsabilidad financiera al modelo operativo de la nube.

4.5.3.1. Visibilidad de Costes y Presupuestos

El gobierno necesita saber quién gasta qué y por qué. Es importante realizar una implementación de etiquetas (tagging) obligatorias en todos los recursos de la nube (Etiqueta: `Proyecto=Modernizacion\_Fiscal`, `Agencia = Ministerio X`). Esto permite a los equipos de Finanzas rastrear el gasto por departamento o proyecto y establecer presupuestos.

4.5.3.2. Optimización de la Demanda y Descuentos

La naturaleza elástica de la nube debe ser gestionada activamente para el ahorro. El uso de la IA para identificar recursos subutilizados o inactivos que puedan ser apagados (especialmente fuera del horario laboral). Compra de Instancias Reservadas (RIs) o Planes de Ahorro para cargas de trabajo estables a largo plazo (portales web principales) para obtener descuentos significativos.



- **Gestión de la Migración:** Antes de migrar una aplicación, se debe realizar una evaluación de FinOps para determinar el coste operativo esperado y asegurar que el beneficio económico justifique la transición.

4.5.3.3. Cultura de Responsabilidad Financiera

Integrar métricas de costes en los cuadros de mando de los equipos técnicos. Los ingenieros y desarrolladores deben ser responsables del coste de los recursos que consumen, creando una cultura de eficiencia en el uso de los servicios en la nube. El éxito de FinOps es cultural.

4.6. SOSTENIBILIDAD Y COMPUTACIÓN CUÁNTICA

La Sostenibilidad y la Computación Cuántica representan los límites de la responsabilidad y la innovación, respectivamente, en la adopción de la nube por parte del gobierno. Ambos temas, aunque dispares, convergen en la infraestructura de la nube, ofreciendo herramientas para optimizar recursos y resolver problemas de escala nacional que antes eran inabordables.

4.6.1. Sostenibilidad como Servicio (Green Cloud)

La eficiencia energética y la reducción de la huella de carbono serán un factor de diferenciación. Los proveedores de nube seguirán invirtiendo en centros de datos más ecológicos para ayudar a sus clientes a cumplir sus objetivos de sostenibilidad. La sostenibilidad se ha convertido en una métrica clave para medir la eficiencia y la responsabilidad ambiental de las operaciones gubernamentales. Dado que los centros de datos consumen grandes cantidades de energía, el uso de la nube se percibe como una forma de reducir la huella de carbono del sector público.

4.6.1.1. Reducción de la Huella de Carbono del Gobierno

- **Consolidación Inteligente:** Al migrar de centros de datos gubernamentales a centros de datos de hiperescaladores (grandes proveedores de nube), el gobierno se beneficia de economías de escala que son inherentemente más eficientes. Los proveedores de nube invierten miles de millones en energías renovables (solar, eólica) y en métodos de enfriamiento más eficientes que una entidad gubernamental promedio no podría costear. El gobierno puede priorizar la migración a proveedores que se hayan comprometido públicamente con la neutralidad de carbono o que publiquen métricas detalladas de PUE - Power Usage Effectiveness, garantizando que su infraestructura digital esté alineada con los objetivos climáticos nacionales.
- **Optimización del Cómputo con IA:** La Inteligencia Artificial ya mencionada en el contexto de AIOps se aplica directamente a la sostenibilidad. La IA optimiza el uso de la electricidad dentro de los centros de datos (por ejemplo, regulando el enfriamiento en tiempo real) y asegura que los recursos de la nube se



utilicen al máximo antes de aprovisionar nuevos servidores físicos. Implementación de políticas de Green FinOps que incluyan la métrica de carbono junto con el costo. Esto podría implicar priorizar el despliegue de cargas de trabajo en regiones geográficas de un proveedor de nube que utilicen un porcentaje mayor de energía verde.

4.6.1.2. Nube para la Sostenibilidad (Sustainability as a Service)

La nube no solo ayuda al gobierno a ser más sostenible, sino que le proporciona las herramientas para gestionar la sostenibilidad en toda la nación.

- **Análisis de Datos Ambientales a Escala:** Las entidades de gobierno recopilan inmensas cantidades de datos ambientales (calidad del aire, patrones climáticos, deforestación, monitoreo de cuencas). La nube ofrece la capacidad de almacenamiento y el poder de análisis de Big Data para procesar estos datos de forma eficiente, permitiendo a las agencias ambientales tomar decisiones basadas en modelos predictivos avanzados.
- **Modelado de Ciudades Inteligentes (Smart Cities):** Plataformas en la nube y Edge Computing se combinan para modelar y simular el impacto de nuevas políticas urbanas (tráfico, gestión de residuos, consumo de energía) antes de su implementación, optimizando la infraestructura de la ciudad para la eficiencia energética.

4.6.2. Computación Cuántica en la Nube (Quantum Computing)

La computación cuántica aún está en sus etapas iniciales, pero los proveedores de nube ya están ofreciendo acceso a entornos cuánticos. En los próximos 5 años, veremos avances en la integración de la computación cuántica en la nube para resolver problemas de optimización, simulación molecular y desarrollo de nuevos materiales. La Computación Cuántica (QC) utiliza principios de la mecánica cuántica para realizar cálculos a velocidades inalcanzables para los superordenadores clásicos actuales. Si bien la QC se encuentra en una fase inicial, la única forma en que el gobierno accederá a esta tecnología será a través de la nube.

4.6.2.1. Acceso a Infraestructura Cuántica como Servicio (QCaaS)

La construcción, el mantenimiento y la operación de un ordenador cuántico requieren recursos y entornos especializados (criotemperaturas) que están fuera del alcance de la mayoría de las instituciones gubernamentales. Los proveedores de nube (AWS, Azure, Google Cloud) ofrecen QCaaS, permitiendo a las agencias gubernamentales experimentar con el cómputo cuántico en la nube mediante un modelo de pago por uso. Esto democratiza la investigación cuántica, que de otro modo sería prohibitivamente cara.



4.6.2.2. Casos de Uso Potenciales de la QC para el Gobierno

En los próximos 5 a 10 años, la QC se aplicará a problemas de optimización de gran escala que son críticos para la misión gubernamental:

- **Optimización Logística a Nivel Nacional:** Resolver problemas complejos de enrutamiento y logística, como la optimización de las rutas de distribución de ayuda humanitaria durante desastres, la planificación del transporte público o la cadena de suministro de vacunas a nivel nacional.
- **Desarrollo de Nuevos Materiales:** Simulación precisa de moléculas para la investigación de nuevos fármacos, el desarrollo de materiales más ligeros para el sector de defensa o la creación de catalizadores más eficientes para la producción de energía limpia.
- **Ciberseguridad Poscuántica:** La QC tiene la capacidad teórica de romper los algoritmos de cifrado clásicos (como RSA) utilizados actualmente. Por ello, los gobiernos están utilizando la nube para investigar y desarrollar nuevos algoritmos de cifrado resistentes a la computación cuántica (post-quantum cryptography), una tarea que requiere una capacidad de cómputo masiva.

4.7. Edge, Ética y Transformación

El futuro de la IA en la nube se enfocará en la distribución de la inteligencia, la integración de tecnologías aún más avanzadas y la gestión de los desafíos éticos y de sostenibilidad.

4.7.1. Edge AI y la Inteligencia Distribuida

A medida que más dispositivos se conectan (IoT, 5G), la IA debe moverse de los grandes centros de datos a los puntos de interacción.

- **Inteligencia en el Borde:** El entrenamiento de los modelos de IA se lleva a cabo en la nube centralizada, pero la inferencia (la ejecución del modelo para hacer una predicción) se mueve al borde de la red. Esto reduce la latencia, ya que los datos no necesitan viajar hasta el centro de datos y viceversa.
- **Casos de Uso Críticos:** Es fundamental para aplicaciones donde el tiempo de respuesta es vital: vehículos autónomos, robótica, análisis de video en tiempo real y sistemas de vigilancia industrial. La nube proporciona la orquestación central de miles de dispositivos Edge.

4.7.2. La IA y las Tecnologías Emergentes

El matrimonio de la IA con otras tecnologías disruptivas se gestará en la nube.



- **Computación Cuántica en la Nube:** Los proveedores están ofreciendo acceso a hardware cuántico y herramientas de simulación a través de la nube. Si bien la computación cuántica es incipiente, la IA jugará un papel crucial al optimizar los algoritmos cuánticos y gestionar la complejidad de estos sistemas en el futuro.
- **Integración de Blockchain y Confianza:** La IA puede combinarse con tecnologías de registro distribuido para mejorar la transparencia y la trazabilidad de las decisiones de los modelos (IA Explicable), lo cual es crucial para el cumplimiento normativo.

4.7.3. Desafíos Éticos, de Gobernanza y Sostenibilidad

La potencia de la IA en la nube viene con responsabilidades significativas que deben abordarse en los próximos cinco años.

- **IA Responsable y Explicabilidad (XAI):** La necesidad de comprender por qué un modelo de IA tomó una decisión específica (especialmente en finanzas o salud) será una prioridad. Los servicios en la nube integrarán herramientas de XAI para garantizar la equidad, transparencia y auditabilidad de los modelos.
- **Regulación y Soberanía de Datos:** A medida que la IA se vuelve crítica, las regulaciones de soberanía de datos se endurecerán. Las nubes deberán ofrecer soluciones de residencia de datos hiperlocalizadas y herramientas de compliance asistidas por IA para ayudar a las empresas a cumplir con leyes como GDPR o sus equivalentes locales.
- **Sostenibilidad como Servicio (Green Cloud):** La inmensa demanda de cómputo de la IA impulsa la necesidad de eficiencia energética. La IA se utilizará para optimizar la carga de los centros de datos, enfriamiento y distribución de energía, haciendo que el consumo de la nube sea inherentemente más ecológico y sostenible.

5. MITOS Y REALIDADES DE LA COMPUTACIÓN EN LA NUBE

La adopción de la nube en el sector público suele estar rodeada de percepciones que no siempre reflejan la realidad tecnológica y regulatoria actual. Alinear estos conceptos es crucial para una estrategia exitosa bajo el MRAE 3.0 y el NIST CSF 2.0. [19] [20] [21]

Aspecto	Mito	Realidad
Costo y Ahorro	Ir a la nube es intrínsecamente más barato que mantener un Centro de Datos propio (CPD).	La nube solo es más barata si se implementa una disciplina FinOps.



Aspecto	Mito	Realidad
Rendimiento	Los sistemas legados funcionarán peor o más lentos en la nube.	La elasticidad y el cómputo de alto rendimiento (HPC) de la nube ofrecen un rendimiento superior. Sin embargo, para los sistemas Lift & Shift, se requiere una Conectividad Dedicada y una arquitectura de red bien diseñada para evitar problemas de latencia entre la nube y el CPD local.
Seguridad	La nube pública es inherentemente menos segura que mi infraestructura local (<i>on-premise</i>).	Los proveedores hiperescalares invierten miles de millones en seguridad física y lógica, ofreciendo capacidades (como cifrado masivo, IA para detección de amenazas y Zero Trust) que superan la capacidad de la mayoría de los CPD gubernamentales.
Soberanía y Datos	Si mis datos están en la nube, pierdo la Soberanía sobre ellos.	El proveedor garantiza la Residencia de Datos en la región geográfica acordada (dentro del país, si se contrata una región local). La soberanía (regulación, acceso legal) se mantiene a través de contratos y Acuerdos Marco que cumplen con la legislación nacional y regulan el acceso a los datos por parte de terceros.
Control Tecnológico	Al usar la nube, pierdo el control sobre mi infraestructura de TI.	El control se transforma. En IaaS, la entidad mantiene control total del SO en adelante. En PaaS/SaaS, la entidad delega el mantenimiento y se enfoca en el control de la Aplicación, los Datos, y la Identidad (IAM), concentrando los recursos internos en la misión pública (MRAE 3.0).
Adopción y Bloqueo	Si elijo un proveedor, quedo "bloqueado" (Vendor Lock-in) y es imposible migrar	La estrategia moderna del Estado es Multi-Cloud e Híbrida. La entidad debe usar tecnologías abiertas como Contenedores (Kubernetes) para hacer que las aplicaciones sean portables y minimizar la dependencia de las herramientas específicas de un solo proveedor, cumpliendo el principio de Neutralidad Tecnológica.
Innovación	La nube es solo para el almacenamiento de archivos y backups.	La nube es la plataforma para la Innovación Digital. Habilita el uso de servicios avanzados como IA/ML, Serverless y Edge Computing, permitiendo a la entidad crear nuevos servicios al



Aspecto	Mito	Realidad
		ciudadano de manera ágil y rápida (time to market).

Tabla 9 Mitos y realidades de la nube

Para el sector público, FinOps es la materialización del beneficio de "Servicio Medible" (característica esencial NIST) y un imperativo de gobernanza del MRAE 3.0.

5.1. LA TRANSFORMACIÓN DEL GASTO

La nube introduce el modelo de Gasto Operativo (OpEx), donde el pago es variable y por consumo, a diferencia del Gasto de Capital (CapEx) tradicional (compra de servidores).

Aspecto	Infraestructura Tradicional (CapEx)	Nube (OpEx)
Gasto	Fijo, grande, anticipado.	Variable, granular, posconsumo.
Control	Bajo. Una vez se compra el <i>hardware</i> (TCO), el costo no se puede reducir.	Alto. El costo se controla a diario mediante la Optimización y el Ajuste elástico.
Gobernanza	Presupuesto anual y lento.	Presupuesto dinámico y rápido (FinOps).

Tabla 10 Aspectos financieros para tener en cuenta para migrar a la nube

5.2. LOS TRES PILARES DE FINOPS PARA EL SECTOR PÚBLICO

La práctica FinOps sigue un ciclo de vida continuo que requiere la colaboración entre las áreas de Finanzas, Tecnología (TI/Ingeniería) y los Líderes del Negocio o la misionalidad. [22]

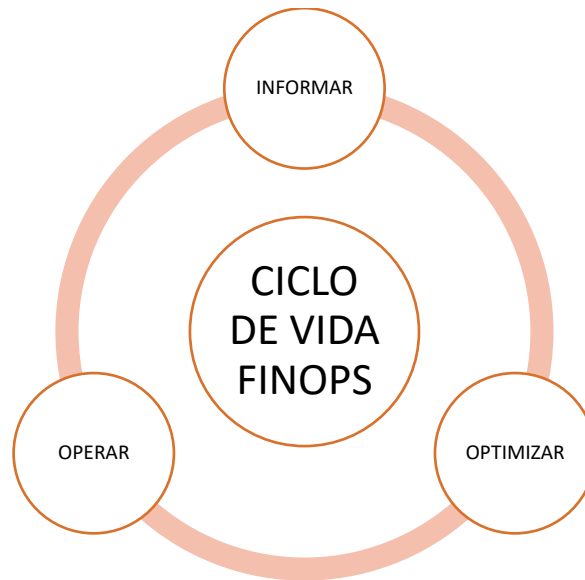


Figura 13 Ciclo de vida para FINOPS en la nube

5.2.1. Informar

La viabilidad y responsabilidad como primer paso lograr la transparencia total sobre dónde se gasta el dinero de la nube. [22]

- **Asignación de Costos (Tagging):** Es crucial etiquetar (tagging) obligatoriamente cada recurso de nube (VM, bases de datos, almacenamiento) con identificadores claros como código de proyecto, unidad ejecutora, responsable de presupuesto. Esto permite asignar el costo exacto a la función o servicio público que lo consume.
- **Medición Granular:** Aprovechar la capacidad de Servicio Medible del proveedor para obtener datos detallados de uso y gasto en tiempo real.
- **Presupuesto y Forecasting:** Crear presupuestos dinámicos basados en la demanda real y usar herramientas de forecasting para predecir el gasto futuro, evitando sorpresas presupuestales.

5.2.2. Optimizar

Una vez que se conoce el gasto, se busca el ahorro proactivo y el equipo de TI implementa acciones de ahorro. [22]



- **Eliminación de Residuos:** Identificar y apagar recursos infrautilizados o inactivos (ej. ambientes de staging o prueba que se dejan encendidos durante la noche o los fines de semana).
- **Elasticidad y Serverless:** Migrar cargas de trabajo que fluctúan a modelos Serverless o utilizar la Elasticidad Rápida para pagar solo por el tiempo de ejecución exacto, en lugar de mantener servidores fijos encendidos.
- **Compromisos de Uso:** Utilizar las Instancias Reservadas o los Planes de Ahorro que ofrecen los proveedores a cambio de un compromiso de uso (generalmente de 1 o 3 años), reduciendo significativamente la tarifa horaria para cargas de trabajo estables.

5.2.3. Operar

Realizar gobernanza continua e integrar las decisiones de costo en el flujo de trabajo diario de los ingenieros. [22]

- **Automatización de Políticas:** Usar la Infraestructura como Código (IaC) para establecer políticas de aprovisionamiento que incluyan límites de gasto.
- **Alertas:** Configurar alertas automáticas que notifiquen al equipo de Ingeniería cuando el gasto de un proyecto excede un umbral predefinido.
- **Toma de Decisiones Conjunta:** Crear un Comité FinOps donde los líderes de Negocio, Finanzas y TI revisen conjuntamente los informes de gasto y tomen decisiones sobre la mejor manera de invertir los recursos de la nube para el bien público.

5.3. ALINEACIÓN CON EL MRAE 3.0

FinOps es una herramienta que permite a la entidad gubernamental ser ágil y financieramente responsable: [18]

- **Eficiencia:** Cumple con la necesidad de eficiencia y optimización del gasto público.
- **Transparencia:** Asegura la transparencia y la rendición de cuentas sobre el uso de los fondos asignados a la transformación digital.
- **Neutralidad Tecnológica:** Permite evaluar objetivamente qué proveedor ofrece el mejor valor económico para una carga de trabajo específica, reforzando la capacidad de tomar decisiones Multi-Cloud basadas en datos.

6. ASPECTOS LEGALES Y JURÍDICOS VIGENTES

6.1. PRIORIZACIÓN DE LA NUBE (LEY 1955 DE 2019)

Este artículo establece que las entidades del orden nacional deben priorizar el uso de servicios de nube y tecnologías emergentes antes de considerar inversiones en infraestructura física propia. Esta "priorización de la nube" busca no solo la eficiencia



en el gasto público (pasar de CapEx a OpEx), sino también garantizar la agilidad en la prestación de servicios al ciudadano.

6.2. DIRECTRICES PRESIDENCIALES Y ESTÁNDARES DEL MINTIC (DIRECTIVA PRESIDENCIAL 03 DE 2021)

Se dan lineamientos claros sobre la gestión de datos, seguridad digital y el uso de servicios de nube. Complementariamente, el Decreto 1263 de 2022 (que adiciona el Decreto Único 1078 de 2015) formaliza los estándares para la Transformación Digital Pública, obligando a las instituciones a realizar una evaluación técnica previa que justifique la adopción de nubes públicas, privadas o híbridas, siempre bajo principios de interoperabilidad y neutralidad tecnológica.

6.3. EL MODELO DE RESPONSABILIDAD COMPARTIDA Y SEGURIDAD

Desde el punto de vista jurídico-técnico, la seguridad no se delega totalmente al proveedor. Bajo el NIST CSF 2.0 y los lineamientos de la Resolución 2239 de 2024 del MinTIC, rige el modelo de responsabilidad compartida. Mientras el proveedor asegura la infraestructura base, la entidad pública es legalmente responsable por la integridad, confidencialidad y disponibilidad de los datos, así como por la gestión de identidades y accesos (IAM).

6.4. PROTECCIÓN DE DATOS PERSONALES (LEY 1581 DE 2012)

Cualquier despliegue en la nube debe cumplir estrictamente con la Ley 1581 de 2012. Esto implica que, aunque los servidores puedan estar en el extranjero, la entidad debe asegurar que el país receptor cuente con niveles adecuados de protección de datos o que existan contratos de transmisión que garanticen los derechos de los titulares. La soberanía de la información se mantiene mediante el control contractual sobre la residencia y el acceso a la data.

6.5. CONTRATACIÓN MEDIANTE AGREGACIÓN DE DEMANDA

Para cumplir con los principios de transparencia y economía, la normativa colombiana impulsa la adquisición de estos servicios a través de la Agencia Nacional de Contratación Pública - Colombia Compra Eficiente. El uso de los Acuerdos Marco de Precios (AMP) es la vía jurídica para evitar la atomización de contratos y asegurar precios competitivos y condiciones legales estandarizadas que protejan los intereses del Estado.

6.6. ALINEACIÓN CON EL MRAE 3.0

Finalmente, el uso de la nube debe enmarcarse en el Modelo de Referencia de Arquitectura Empresarial (MRAE 3.0). Este marco exige que la tecnología no sea un



silo independiente, sino un habilitador de la misión institucional, donde la gobernanza de TI asegure que la nube sea elástica, escalable y auditable para los entes de control.

7. BIBLIOGRAFÍA

1. Ministerio de Tecnologías de la Información. Colombia. Marco de Referencia de Arquitectura Empresarial. <https://www.mintic.gov.co/arquitecturati>
2. Microsoft. Azure. ¿Qué es el Middleware?. <https://azure.microsoft.com/eses/overview/what-is-middleware/>
3. P. Mell, T. Grance (2011, Sep.), "The NIST Definition of Cloud Computing", Special Publication 800-145, p.2. <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf>
4. Working Group members (2013, Jul.), "NIST Cloud Computing Standards Roadmap", Special Publication 500 - 291v2, p. 12-24. https://www.nist.gov/sites/default/files/documents/itl/cloud/NIST_SP-500-291_Version-2_2013_June18_FINAL.pdf
5. F. Liu, J. Tong, J. Mao, R. Bohn, J. Messina, L. Badger, D. Leaf (2011, Sep.), "NIST Cloud Computing Reference Architecture", Special Publication 500-292, Appendix B: Examples of Cloud Services p. 24-25. http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=909505
6. Colombia compra eficiente. Acuerdos Marco de TI. <https://www.colombiacompra.gov.co/tienda-virtual-del-estado-colombiano/tecnologia>.
7. Junta de Andalucía. Consejería de economía, Innovación, ciencia y empleo. Cloud Computing. Aplicado a los sectores de agroindustria, eficiencia energética, industrias culturales y turismo. 2012.
8. Congreso de Colombia. Ley de TIC, 1341 del 30 de Julio de 2009.
9. Ministerio de Tecnologías de la Información y las comunicaciones. Decreto 1078 de 2017 artículo 2.2.9.1.1.1. Estrategia de Gobierno Digital (GD).
10. Guía para clientes que contraten servicios de Cloud Computing (2013), Agencia Española de Protección de datos.
11. Cloud Security Alliance (2011). Guía de seguridad de áreas críticas en Cloud Computing. 3.0
12. Luis Joyanes Aguilar. Computación en la nube. Notas para una estrategia española en Cloud Computing.



13. V. Hernández (2010, Feb.), "El papel del aprovisionamiento de la gestión en la nube".
<https://www.ibm.com/developerworks/community/blogs/b35561d9-e0ef-48e0-b455-001f4a64b4da/entry/cloudcomputing?lang=en>
14. Guía 12 (2016, Mar.), Seguridad en la nube, Seguridad y privacidad de la información, Ministerio de Tecnologías de la Información y las comunicaciones.
https://www.mintic.gov.co/gestionti/615/articles-5482_G12_Seguridad_Nube.pdf
15. Gartner. Gartner IT Glossary > Data Center.
<https://www.gartner.com/itglossary/data-center/>
16. Mell P. Grance T. The NIST Definition of Cloud Computing. 2011.
<https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf>
17. El Marco de Seguridad Cibernética (CSF) 2.0 del NIST. 2024.
<https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.spa.pdf>
18. Marco de referencia de arquitectura empresarial 3.0. 2022.
https://www.mintic.gov.co/portal/715/articles-273207_recurso_2.pdf
19. 5 mitos sobre Cloud Computing.
<https://ozein.es/5-mitos-sobre-cloud-computing/>
20. Diez mitos que existen sobre computación en la nube
<https://www.bbva.com/es/innovacion/diez-mitos-que-existen-sobre-computacion-en-la-nube/>
21. Computación en la nube: mitos que debemos derribar
<https://www.claro.com.co/empresas/noticias-interes/mitos-de-la-computacion-en-la-nube/>
22. ¿Qué es FinOps? Microsoft.
<https://learn.microsoft.com/es-es/cloud-computing/finops/overview>