Arquitectura TI COLOMBIA
MARCO DE REFERENCIA

vive digital para la gente

G.ST.02 Guía de Computación en la nube

Guía técnica

Versión 0.9

5 de septiembre de 2017

Servicios Tecnológicos

MINTIC

TODOS POR UN NUEVO PAÍS
PAZ EQUIDAD EDUCACIÓN

HISTORIA

VERSIÓN	FECHA	CAMBIOS INTRODUCIDOS
0.9	05/09/2017	Emisión de la guía para consulta pública

DERECHOS DE AUTOR

AUTORES

Versión 0.9

David Luna Sánchez
Ministro de las Tecnologías de la Información y las Comunicaciones

Daniel Quintero Calle
Viceministro de Tecnologías y Sistemas de la Información
Ministerio de Tecnologías de la Información y las Comunicaciones

Juanita Rodríguez Kattah
Directora de Estándares y Arquitectura de TI
Ministerio de Tecnologías de la Información y las Comunicaciones

Asesores del Ministerio de Tecnologías de la Información y las Comunicaciones
Carlos Arturo Merchán Herrera
Claudia Milena Rodríguez Álvarez
Miguel Antonio Roa Bejarano
Paula Andrea Restrepo Suárez
Waldir Ramiro Arteaga Guzmán

TABLA DE CONTENIDO

PÁG.

LISTA DE TABLAS

TABLA DE FIGURAS

INTRODUCCIÓN

Con el fin de proporcionar definiciones y criterios para identificar si un proveedor de servicios de tecnologías de la información y las comunicaciones es un proveedor de servicios de computación en la nube (del inglés, cloud computing) y presentar consideraciones a tener en cuenta a la hora de contratar este tipo de servicios, el Ministerio de Tecnologías de la Información y las comunicaciones (MinTIC) desarrolla esta guía y la pone a disposición de los interesados.

En Colombia, los servicios de computación en la nube a partir de la reforma tributaria definida en la Ley 1819 de 2016, poseen un beneficio tributario y de acuerdo al Marco de Referencia de Arquitectura Empresarial de estado Colombiano, las entidades públicas deben evaluar como primera opción la posibilidad de prestar o adquirir servicios tecnológicos haciendo uso de la nube (pública, privada o hibrida), para atender las necesidades de los grupos de interés, por lo que resulta clave entender los conceptos que giran alrededor de la computación en la nube y el papel que juega en cada una de nuestras organizaciones.

Este documento contribuye a establecer la definición de referencia de computación en la nube para Colombia, sus características, los modelos de servicios e implementación, beneficios y aspectos a considerar para proveer o adquirir servicios en la nube. Así mismo ofrece un anexo que le permitirá identificarse como un actor dentro del ecosistema de computación en la nube y determinar si puede considerarse un proveedor de este tipo de servicios.

Es oportuno aclarar que este documento no es una norma o especificación técnica, es solo una orientación para facilitar la contratación de servicios de computación en la nube por parte de las entidades públicas y demás actores y ofrecer criterios para determinar si un proveedor puede considerarse proveedor de servicios en la nube.

1.1 OBJETIVOS DE LA GUÍA

- Proveer a los interesados una orientación para entender el modelo de computación en la nube.
- Ofrecer una definición formal de computación en la nube alineado con lo definido en los Acuerdos Marco de TI relacionados con nube pública y privada.
- Presentar aspectos y criterios a tener en cuenta al momento de adquirir servicios en la nube.

1.2 ALCANCE DE LA GUÍA

La presente guía, además de presentar definiciones sobre el modelo de computación en la nube, busca que las organizaciones puedan identificarse o clasificarse dentro de los actores y modelos de servicios de esta tendencia. Así mismo proporciona un conjunto de criterios y consideraciones que deben ser evaluadas y tenidas en cuenta a la hora de adquirir este tipo de servicios.

1.3 LINEAMIENTOS DEL MARCO DE REFERENCIA ASOCIADOS CON ESTA GUÍA

La presente guía apoya el cumplimiento y adopción del siguiente lineamiento del dominio de Servicios Tecnológicos, del Marco de Referencia de AE para la Gestión de TI [1]:

LI.ST.04 Acceso a servicios de la Nube: La Dirección de Tecnologías y Sistemas de la Información o quien haga de sus veces debe evaluar como primera opción la posibilidad de prestar o adquirir los Servicios Tecnológicos haciendo uso de la Nube (pública, privada o hibrida), para atender las necesidades de los grupos de interés.

1.4 TÉRMINOS Y DEFINICIONES

Aprovisionamiento: Capacidad de los servicios de computación en la nube para proporcionar nuevos servicios o modificar características del servicio dispuestos a los consumidores.

Arquitectura de Referencia: Es un diseño de alto nivel, sin detalles tecnológicos o de productos, que se utiliza como una plantilla para guiar el bosquejo de otras arquitecturas más específicas. Esta plantilla incluye los principios de diseño que la guían, las decisiones de alto nivel que se deben respetar, los componentes que hacen parte de la solución, sus relaciones tanto estáticas como dinámicas, las recomendaciones tecnológicas y de desarrollo, las herramientas específicas de apoyo a la construcción y los componentes existentes reutilizables. El concepto de Arquitectura de Referencia se puede utilizar como base del diseño detallado de arquitecturas de solución, de software, de información o de plataforma tecnológica. [1]

Capa media: Funciona como una capa de abstracción de software distribuida, que se sitúa entre la capa de aplicaciones y las capas inferiores (sistema operativo y red). Es un software que asiste a una aplicación para interactuar o comunicarse con otras aplicaciones, o paquetes de programas, redes, hardware y/o sistemas operativos. Éste simplifica la tarea de generar las conexiones y sincronizaciones que son necesarias en los sistemas distribuidos. [2]

Conexión dedicada: Es una conexión permanente en internet las 24 horas, que no requiere el uso de líneas telefónicas y garantiza siempre el ancho de banda contratado (misma velocidad y

ancho de banda de bajada tanto como de subida "síncrono") asegurando un alto nivel de confiabilidad, estabilidad, seguridad y desempeño de sus aplicaciones web publicadas.

Entorno de desarrollo integrados (IDE): Es un entorno de programación que ha sido empaquetado como un programa de aplicación y consiste en un editor de código, un compilador, un depurador y un constructor de interfaz gráfica. Los IDE pueden ser aplicaciones por sí solas o pueden ser parte de aplicaciones existentes. Por ejemplo Net Beans, Visual Studio, Eclipse, entre otros.

Implementación del servicio: Todas las actividades necesarias para hacer disponible un servicio en la nube.

Incidente: Es cualquier evento que no forma parte del desarrollo habitual del servicio y que causa, o puede causar una interrupción del mismo o una reducción de la calidad de dicho servicio.

Interfaz: Se utiliza para nombrar a la conexión funcional o física entre dos sistemas, programas, dispositivos o componentes de cualquier tipo, que permite una comunicación de distintos niveles permitiendo el intercambio de información.

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 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. Al analizar y detallar la definición es importante tener claridad de los siguientes conceptos:

Nube: El término nube viene del uso común del símbolo de una nube para referirse usualmente a Internet. No todo lo que está en internet es computación en la nube.

Acceso ubicuo: Hace referencia a que desde diferentes dispositivos, desde cualquier lugar y en cualquier momento, es posible acceder a los servicios.

Acceso adaptable: Hace referencia a que es conveniente y práctico. Se adapta a las necesidades o propósitos específicos.

Acceso por demanda: Hace referencia a que se encuentra disponible cuando el cliente requiere el servicio, lo que implica que el proveedor debe ofrecer una rápida capacidad de respuesta. Es decir, acceso bajo pedido.

Aprovisionar: En el ámbito de computación en la nube el aprovisionamiento es la acción de contratar, abastecer o adquirir recursos computacionales durante un periodo de tiempo determinado. De igual manera estos recursos pueden ser liberados de acuerdo a la necesidad del usuario.

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:

1. **Autoservicio bajo demanda (On-demand self-service):** Un consumidor puede unilateralmente aprovisionar capacidades o recursos de computación, tales como tiempo de servidor y almacenamiento en red, según sea necesario y de manera automática sin necesidad de interacción humana con cada proveedor de servicios.
2. **Acceso amplio a la red (Broad network access):** Los servicios proporcionados deben poder ser accesibles sobre la red y a través de mecanismos estándares que promuevan el uso desde plataformas heterogéneas del cliente (por ejemplo: computadores, teléfonos móviles o tabletas).
3. **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. Hay un sentido de independencia de la localización en la que el usuario no tiene un estricto control del lugar exacto en el que se encuentra su información o de los servicios contratados, aunque sí debe poder especificar un ámbito mínimo de actuación (por ejemplo: un país, una región o un centro de proceso de datos concreto). Ejemplos de recursos incluyen almacenamiento, procesamiento, memoria y ancho de banda.
4. **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
5. **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 tanto al proveedor del servicio como al consumidor del mismo.

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].

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.

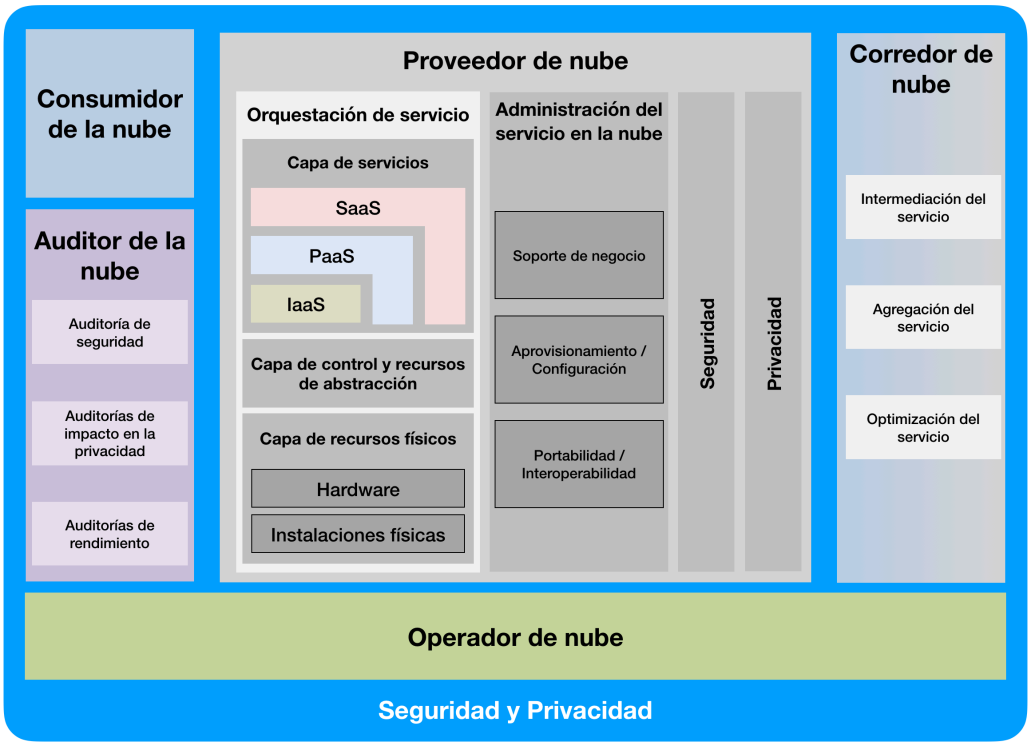

Figura 1 Modelo de referencia Conceptual – NIST

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.

Actor	Definición
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 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

La Figura 2 ilustra las interacciones entre los actores. Un Consumidor de nube puede solicitar servicios en la nube a un proveedor de nube directamente o a través de un corredor u agente de nube. Un auditor de nube lleva a cabo auditorías independientes y puede contactar a los otros para recopilar la información necesaria. Un operador de nube soporta los canales físicos de comunicación entre todos los actores de la nube.

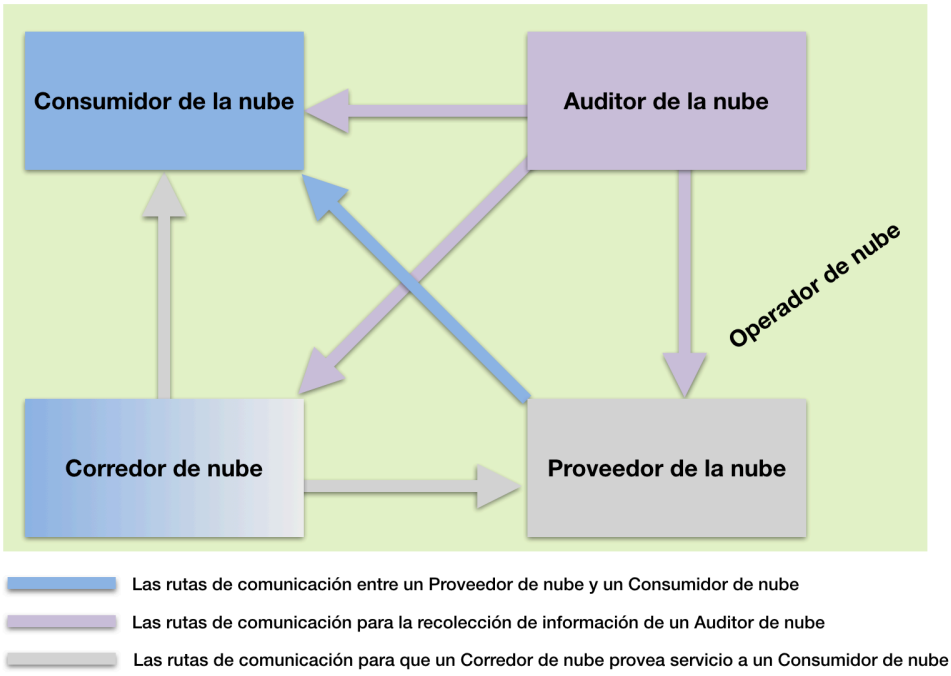

Figura 2 Interacción entre los actores de la computación en la nube

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	Actividades del Proveedor
SaaS (Software como servicio)	Usa la aplicación o los servicios para operaciones de proceso de negocio.	Instala, administra, mantiene y soporta la aplicación de software en una infraestructura de nube.
PaaS (Plataforma como servicio)	Desarrolla, testea, 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 lo 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 IaaS a través de un conjunto de interfaces de servicios y abstracciones de

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

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.

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.

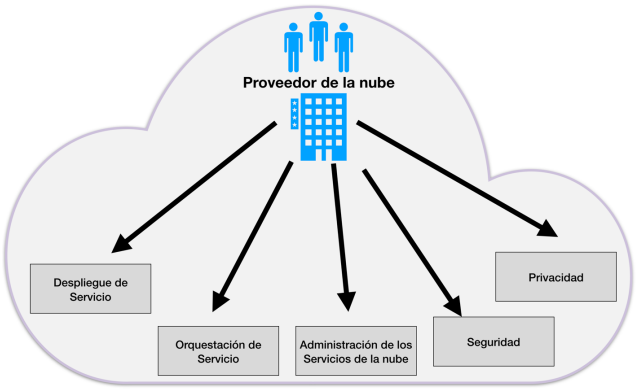

Figura 3 Actividades principales de un Proveedor de la nube.

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. Para mayor detalle, remítase al numeral 2.5 Modelos de implementación.

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.

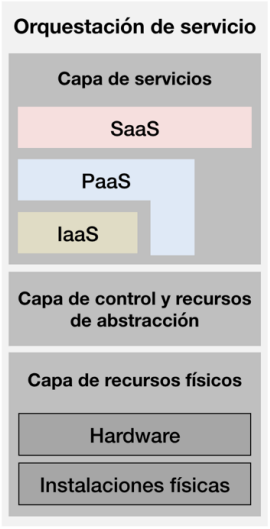

Figura 4 Proveedor de nube – Orquestación del Servicio

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.

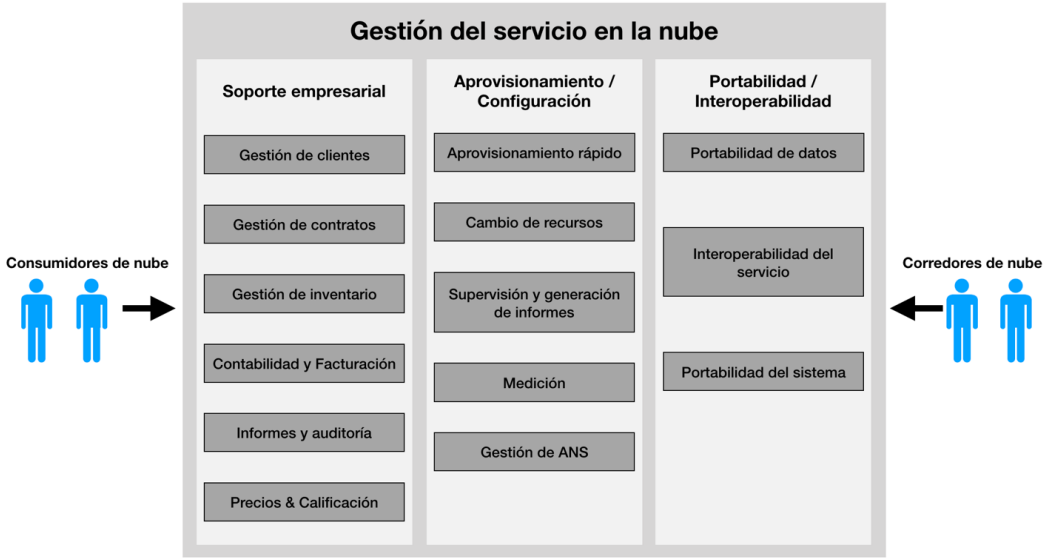

Figura 5 Proveedor de nube – Administración del servicio en la nube

- 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. Cuando 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.

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 de seguridad, impacto sobre la privacidad, rendimiento, etc [4][5].

Actividades del corredor u agente (Intermediario) de nube

Un corredor de nube puede proporcionar 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 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.

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]:

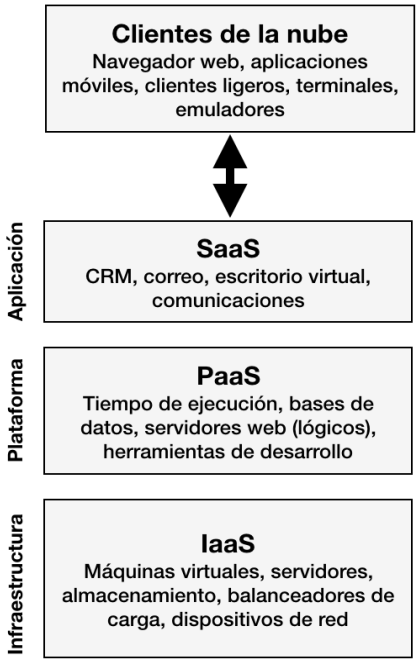

Figura 6 Modelos de servicio

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

La capacidad proporcionada al consumidor es 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 (por ejemplo, correo electrónico basado en web) o una interfaz de programa. El consumidor no gestiona ni controla la infraestructura subyacente de la nube, como la red, los servidores, los sistemas operativos, el almacenamiento o incluso las capacidades de las aplicaciones individuales, con la posible excepción de los ajustes de configuración específicos de la aplicación específicos del usuario. El proveedor de SaaS, es responsable del mantenimiento, operación y soporte del SaaS.

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

- ***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.
- ***Sistemas de Gestión y manejo de relaciones con clientes (Customer Relationship Management-CRM):*** Aplicaciones de CRM dispuestas en la nube, que van desde las aplicaciones de centro de llamadas hasta la automatización de la fuerza de ventas y con facturación por demanda.
- ***Herramientas de Colaboración:*** Aplicaciones de software dispuestas en la nube, que permiten a los usuarios colaborar en grupos de trabajo, dentro de las empresas y entre empresas.
- ***Aplicaciones de gestión de contenidos:*** Servicio que permite el acceso a herramientas dispuestas en la nube para gestionar la producción y el acceso a contenidos de aplicaciones basadas en la web.
- ***Herramientas de gestión de documentos:*** Aplicaciones dispuestas en la nube para gestionar documentos, hacer cumplir los flujos de trabajo de producción de documentos y proporcionar espacios de trabajo para grupos o empresas para consultar y acceder a documentos.
- ***Finanzas:*** Aplicaciones para la gestión de procesos financieros que van desde el procesamiento de gastos y la facturación a la gestión tributaria.
- ***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.
- ***Redes de colaboración:*** software que permite la administración y seguimiento de diferentes tipos de plataformas de manera unificada, ya sean plataformas de redes sociales o plataformas de servicios.
- ***Planificación de Recursos Empresariales (ERP):*** Sistema integrado web, dispuesto en la nube para administrar recursos internos y externos, incluyendo activos tangibles, recursos

financieros, materiales y recursos humanos. Para que sea un SaaS, debe ser facturado por demanda y cumplir con las características definidas por el NIST, detalladas en este documento.

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

Este modelo de servicio, proporciona al consumidor la posibilidad de desplegar 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 no gestiona ni controla la infraestructura subyacente de la nube, servidores, sistemas operativos o almacenamiento, pero tiene control sobre las aplicaciones desplegadas y posiblemente configuraciones para el entorno de hospedaje de aplicaciones. El proveedor de PaaS, es responsable del mantenimiento, soporte y operación de las plataformas dispuestas como servicio. Esta capacidad no excluye necesariamente el uso de lenguajes de programación compatibles, bibliotecas, servicios y herramientas de otras fuentes.

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. Estos servicios proporcionan bases de datos, entornos de ejecución de aplicaciones web, entre otros.

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

Este modelo de servicio proporciona al consumidor de nube, capacidades de procesamiento, almacenamiento, redes y otros recursos de computación fundamentales donde el consumidor es capaz de desplegar y ejecutar software arbitrario, que puede incluir sistemas operativos y aplicaciones. El consumidor no gestiona ni controla la infraestructura subyacente de la nube, sino que tiene control sobre los sistemas operativos, el almacenamiento y las aplicaciones implementadas y posiblemente un control limitado de componentes de red selectos (por ejemplo, firewalls de host).

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

- ***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 auto-aprovisionamiento y las demás características esenciales de la computación en las nubes antes mencionadas.
- ***Cómputo:*** recursos de servidor para ejecutar sistemas basados en la nube que se pueden aprovisionar dinámicamente y configurar según sea necesario, por ejemplo, memoria, procesador, entre otros.
- ***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. Son ejemplos de uso de estos servicios los periódicos y emisoras de noticias cuando ocurren hechos como el ataque a las torres gemelas, que deben distribuir su contenido para soportar los altos volúmenes de concurrencia. También son muy usadas para la distribución de audio y video por internet en tiempo real.
- ***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.
- ***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 el auto-aprovisionamiento y las demás características esenciales de la computación en las nubes antes mencionadas.
- ***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.
- ***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.

2.5 MODELOS DE IMPLEMENTACIÓN

Existen diferentes tipos de nubes [4] de acuerdo a 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.

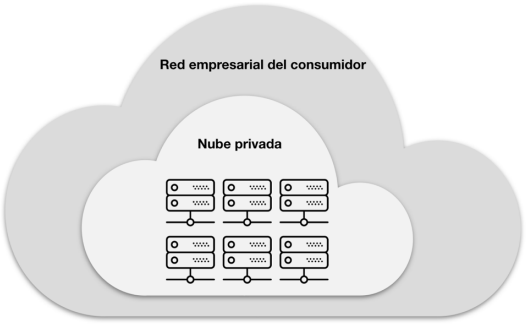

Figura 7 Nube privada en sitio

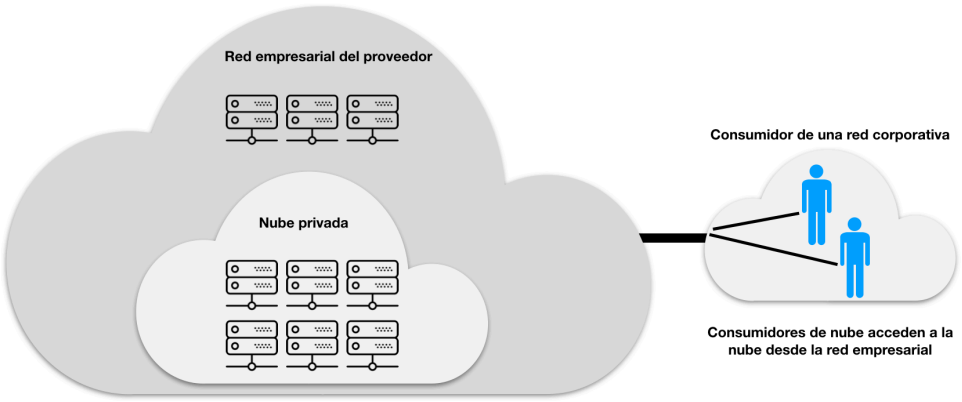

Figura 8 Nube privada subcontratada

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 9 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.

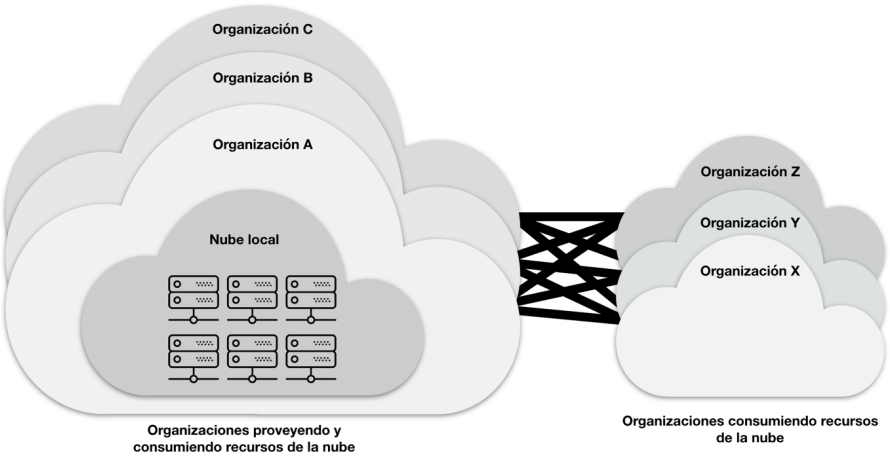

Figura 9 Nube comunitaria en sitio

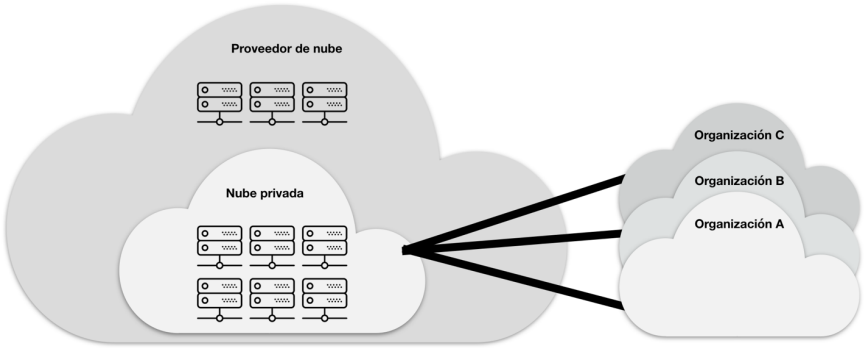

Figura 10 Nube comunitaria subcontratada

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 11 presenta una vista simple de una nube pública y sus clientes.

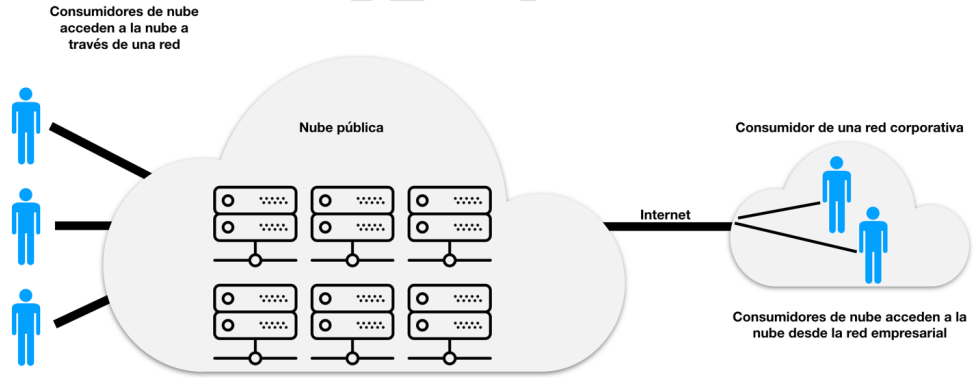

Figura 11 Nube pública

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. La Figura 12 presenta una vista

simple de una nube híbrida que podría ser construida con un conjunto de nubes en las cinco variantes del modelo de implementación.

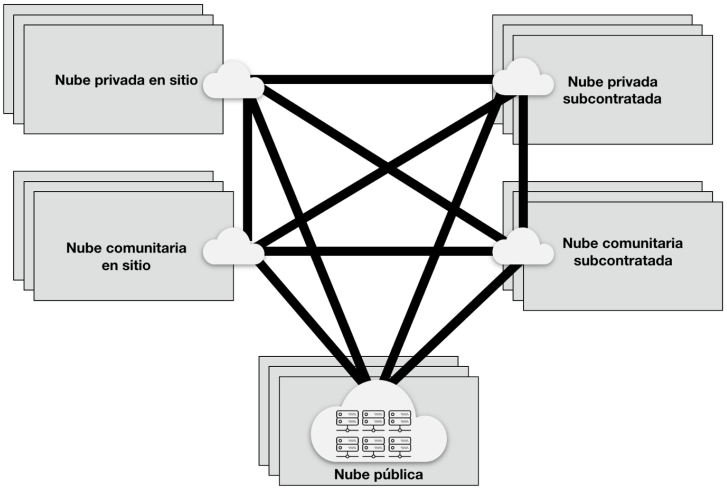

Figura 12 Nube híbrida

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, sin embargo, hay otros beneficios que provee el modelo de computación en la nube como los siguientes:

Reducción de costos de operación.

La adquisición de servicios de computación en la nube ofrece la posibilidad de pagar por la capacidad o servicio utilizado efectivamente, así como no pagar licencias de software, ni ocuparse de actualizaciones, compatibilidad con sistemas operativos, instalación, mantenimiento y soporte de equipos y servidores. Del mismo modo, se pueden reducir costos de personal y pago de servicios públicos, dado que el contratar servicios en la nube, puede disminuir el número de servidores y equipo de cómputo y por ende la reducción de servicios públicos en especial la energía eléctrica. Todos estos costos son conocidos como los costos de propiedad (TCO por sus siglas en ingles Total Cost Ownership) y en el sector público hacen parte del presupuesto de operación, donde el presupuesto de un área de TI, que está destinado en su mayoría o se emplea en cubrir los costos de operación y el presupuesto de inversión es cada vez más reducido. El uso de estas alternativas hace que una entidad pueda emplear o destinar estos recursos a inversiones de TI más estratégicas. En febrero de 2016, un estudio Gartner con recomendaciones e ideas para optimizar los costos de TI a través de soluciones

computación en la nube, muestra que la reducción de costos en hardware y mantenimiento de TI, varia y depende del nivel de optimización y que cuando se utilizan soluciones y servicio de computación en la nube, se pueden alcanzar ahorros de hasta el 30% en costos TCO. [7][8][9]

Escalabilidad.

Las alternativas y servicios de computación en la nube ofrecen agilidad para desplegar nuevos servicios o trámites, flexibilidad y escalabilidad para responder a las demandas de capacidad y/o procesamiento que se requieran. Esto es especialmente útil en la prestación de servicios que tienen picos con gran número de solicitudes durante un periodo de tiempo que luego bajan y suben drásticamente [9]

Reducción de costos de obsolescencia tecnológica

La tecnología avanza todos los días y a una gran velocidad, por lo cual las inversiones o compra de bienes relacionados con TI tienen un mayor riesgo de presentar obsolescencia tecnológica. La obsolescencia se presenta como resultado del surgimiento de bienes de mejor calidad o con mejores características técnicas. Cuando se adquieren servicios de computación en la nube, ese riesgo se traslada al proveedor de servicios, dado que las entidades no invierten o compran tecnología (servidores, licenciamiento, aplicaciones de software) sino que pagan únicamente por su uso [7].

Acceso a tecnología de punta.

Gracias a que los proveedores de servicios de computación en la nube siempre están actualizando sus plataformas de software e infraestructura, las organizaciones de todos los tamaños pueden tener acceso a la misma tecnología y a los mismos avances tecnológicos [9].

Rápida recuperación ante desastres y fallos.

Las capacidades de respaldo y recuperación ante fallos o eventualidades y las características de alta disponibilidad y continuidad del negocio son propios de la computación en la nube. Es conveniente revisar los contratos y acuerdos de niveles de servicio que cada proveedor ofrece [7][9].

Transferencia y reducción de riesgos técnicos

La implementación de nuevos servicios y sistemas de información para las entidades representan un menor riesgo técnico debido al respaldo del proveedor de servicios de computación en la nube, que a su vez posee y da soporte a otros clientes probando el mismo sistema y en procesos de mejora continua.

Entrega rápida y flexible

La adquisición de soluciones y servicios de computación en la nube, reducen el tiempo de salida y despliegue de nuevos servicios o trámites (reducción del time to market). Así mismo, permite aumentar o disminuir las capacidades y/o funcionalidades (ancho de banda, capacidad de procesamiento, capacidad de almacenamiento, entre otros) en algunos casos de forma automática (basado en reglas predefinidas). Las capacidades se pueden comprar prácticamente en cualquier cantidad y en cualquier momento [7][9].

Permite concentrar esfuerzos en la misión y objetivos de la entidad

Los directores y líderes de Tecnología de las entidades públicas - CIO, pueden concentrar más recursos y esfuerzos hacia aspectos más estratégicos y de planeación que tengan impacto directo sobre los procesos de negocio de la organización, transfiriendo al proveedor la responsabilidad de la implementación, configuración y mantenimiento de la infraestructura requerida [9].

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 articulo 2.2. 9.1.1.1 de la estrategia de Gobierno en Línea (GEL). 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 para la gestión de TI, adopta entre sus principios el principio de Neutralidad Tecnológica, el cual plantea que el Estado no debe privilegiar tecnologías, ni proveedores y por lo tanto las entidades del Estado debe hacer una evaluación de las alternativas de inversión, aplicando criterios y evaluando todas las posibilidades para obtener una buena relación costo/beneficio. Por lo anterior las entidades públicas, especialmente al adquirir servicios de computación en la nube deben evaluar y justificar la selección de servicios y tecnología de manera objetiva, siendo deseable las alternativas de computación en la nube.

De otro lado, la Agencia Nacional de Contratación Pública - Colombia Compra Eficiente, con el apoyo técnico del Ministerio de TIC, puso a disposición de las entidades estatales los siguientes Acuerdos Marco de TI relacionados con los servicios de computación en la nube: (i) Servicios de Centro de Datos/Nube Privada, I y II generación, y (ii) Servicios de Nube Pública (actualmente en estructuración la II generación). Estos Acuerdos Marco de TI le permiten 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

A la fecha, más de 70 Entidades Estatales han adquirido servicios de nube a través de la Tienda Virtual del Estado Colombiano (TVEC) por más de $ 7.976 millones de pesos.

Así mismo, los diferentes conceptos, cartillas y demás que la Superintendencia de Industria y Comercio haya hecho públicos para su aplicación en cuanto a todo lo referente en materia de datos y computación en la nube [12][18].

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

3.2.1 Aprovisionamiento 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. [16]

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 auto- aprovisionamiento 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 adquirir servicios de Nube Pública y Nube Privada a través de los AM de TI.

3.2.2 Migración y portabilidad.

Las organizaciones que revisan como alternativa la computación en la nube, deben ser conscientes que pueden tener que cambiar de proveedores en el futuro, en especial si se utilizan servicio de computación en la nube a través de los Acuerdos Marco de TI, en donde el proceso de adjudicación se da al proveedor que cotice el menor valor por los servicios de nube solicitados y cotizados a través de la Tienda virtual del Estado Colombiano (TVEC).

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 [13][14].

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, sin contratiempos. La migración y la portabilidad suelen ser parte del plan de continuidad de las entidades.

3.2.3 Escalonamiento

Tenga 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 realice un análisis de: 1) Qué vale la pena migrar a la nube de manera inmediata. 2) Qué puede esperar, 3) 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, considere.

3.2.4 Seguridad y Privacidad

La mayoría de las infraestructuras en esquemas de computación en la nube son compartidas por múltiples empresas o usuarios y una mala definición de los niveles de seguridad pueden generar accesos no autorizados a datos confidenciales. La definición de una buena política de identidad y control de acceso, basado en el mínimo privilegio, es esencial en entornos Cloud [13][14][15].

Así mismo, las entidades deben a partir de la clasificación de la información de la ley de transparencia y acceso a la información pública (ley 1712 de 2014) y demás aplicable y vigente, determinar qué información puede o debe llevarse a la nube.

De otro lado, la entidad contratante debe asegurarse de cumplir con la reglamentación que para tal efecto prevé la legislación colombiana sobre protección de datos personales, dentro y fuera de país y para ello debe exigir al proveedor los mecanismos que garanticen el borrado seguro de los datos al finalizar el contrato. (Un mecanismo apropiado es requerir una certificación de la destrucción emitido por el proveedor del servicio) [13] [14] [15].

3.2.5 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 por lo menos: a) acciones y secuencia de las acciones a seguir durante el procedimiento, b) responsables e interlocutores, c) tipología de incidentes incluidos en el servicio, d) procedimientos específicos ante incidentes de seguridad, e) tiempos de respuesta y resolución de incidentes y f) gestión y resolución de incidentes. [13]

3.2.6 Gestión de cambios

Las entidades deberán establecer contractualmente la obligación de mantener actualizados los sistemas para garantizar el correcto funcionamiento de los mismos, así como eliminar las posibles vulnerabilidades que puede afectar los servicios de computación en la nube prestados. Para ello se deberá definir un procedimiento de coordinación en el mantenimiento de la infraestructura que soporta los servicios entre ambas partes para prevenir paradas 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. [9]

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.

3.2.7 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 dado por las entidades competentes como la superintendencia de industria y comercio (SIC), el Ministerio de TIC.[13].

3.2.8 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.

3.2.9 Planes de continuidad del negocio (BCP) y recuperación de desastres (DR).

Dependiendo la criticidad del servicio, los clientes o entidades contratantes deben inspeccionar y hacer parte de las pruebas de los planes de recuperación de catástrofes y de continuidad del negocio del proveedor en la nube. 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 [9]

3.2.10 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]

3.2.11 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.

3.2.12 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 clausulas no impiden la contratación de servicios en la nube. [13].

3.2.13 Seguridad

Es fundamental reconocer que la seguridad es un aspecto transversal de la arquitectura que abarca todas las capas del modelo de nube [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 [13][14][15].

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. 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 [13][14][15].

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 [17]. 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 [13][14][15].

3.2.14 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 [17].

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.

3.3 FORMATO DE AUTO DIAGNÓSTICO 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 (auditorias, 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 auto-diagnostico 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 [17]. 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.

REFERENCIAS

[1] Ministerio de Tecnologías de la Información. Colombia. Marco de Referencia de Arquitectura Empresarial para la gestión de TI [Online]. Disponible: www.mintic.gov.co/arquitecturati.

[2] Microsoft. Azure. ¿Que és el Middleware? [Online]. Disponible: https://azure.microsoft.com/es-es/overview/what-is-middleware/

[3] P. Mell, T. Grance (2011, Sep.), "The NIST Definition of Cloud Computing", Special Publication 800-145, p. 2 [Online]. Disponible: 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[Online]. Disponible: 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 [Online]. Disponible: http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=909505

[6] Colombia compra eficiente. Acuerdos Marco de TI [Online]. Disponible: https://www.colombiacompra.gov.co/tienda-virtual-del-estado-colombiano/acuerdos-marco.

[7] Mesa Sectorial Cloud Computing (2010), Cloud Computing una perspectiva para Colombia.

[8] Jim Mc Gittigan, Sanil Solanki. The Gartner Top 10 Recommended IT Cost Optimization Ideas, 2016.

[9] 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.

[10] Congreso de Colombia. Ley de TIC, 1341 del 30 de Julio de 2009.

[11]Ministerio de Tecnologías de la Información y las comunicaciones. Decreto 1078 de 2017 articulo 2.2. 9.1.1.1. Estrategia de Gobierno en Línea (GEL).

[12] SIC (2015), "Protección de los datos personales en los servicios de computación en la nube (Cloud Computing)", [Online]. Disponible: http://www.sic.gov.co/sites/default/files/files/Nuestra_Entidad/Publicaciones/Cartilla_Proteccion_datos.pdf.

[13] Guía para clientes que contraten servicios de Cloud Computing (2013), Agencia Española de Protección de datos.

[14] Cloud Security Alliance (2011). Guía de seguridad de áreas críticas en Cloud Computing. 3.0

[15] Luis Joyanes Agilar. Computación en la nube. Notas para una estrategia española en Cloud Computing.

[16] V. Hernández (2010, Feb.), "El papel del aprovisionamiento de la gestión en la nube", [Online]. Disponible:https://www.ibm.com/developerworks/community/blogs/b35561d9-e0ef-48e0-b455-001f4a64b4da/entry/cloudcomputing?lang=en

[17]Guía 12 (2016, Mar.), Seguridad en la nube, Seguridad y privacidad de la información, Ministerio de Tecnologías de la Información y las comunicaciones [Online]. Disponible: https://www.mintic.gov.co/gestionti/615/articles-5482_G12_Seguridad_Nube.pdf

[18] SIC Concepto 16-263922 (2016, Nov.),[Online]. Disponible: http://www.sic.gov.co/sites/default/files/normatividad/Concepto_16-263922_0.pdf