TIC

Lineamientos de seguridad de la información para el uso de servicios en la nube

Ministerio de tecnologías de la información y las comunicaciones

MSPI

Julián Molina Gómez – Ministro de Tecnologías de la Información y las Comunicaciones
Yeimi Carina Murcia Yela - Viceministra de Transformación Digital
Lucy Elena Urón Rincón - Directora de Gobierno Digital
Luis Clímaco Córdoba Gómez - Subdirector de Estándares y Arquitectura de TI
Danny Alejandro Garzón Aristizábal – Contratista Subdirección de Estándares y Arquitectura de TI
German García Filoth – Contratista Subdirección de Estándares y Arquitectura de TI
Johanna Marcela Forero Varela - Profesional Especializado Subdirección de Estándares y Arquitectura de TI
Julio Andrés Sánchez Sánchez - Contratista Subdirección de Estándares y Arquitectura de TI
Lourdes María Acuña Acuña - Contratista de la Dirección de Gobierno Digital
Tairo Elías Mendoza Piedrahita - Profesional Especializado Dirección de Gobierno Digital
Andrés Díaz Molina- Jefe de la Oficina de Tecnologías de la Información
Nelson Barrios Perdomo – Contratista Equipo de Respuesta a Emergencias Cibernéticas de Colombia – COLCERT
Adriana María Pedraza - Contratista Equipo de Respuesta a Emergencias Cibernéticas de Colombia – COLCERT
Camilo Andrés Jiménez - Contratista Equipo de Respuesta a Emergencias Cibernéticas de Colombia – COLCERT
Emanuel Elberto Ortiz - Contratista Equipo de Respuesta a Emergencias Cibernéticas de Colombia – COLCERT
Angela Janeth Cortés Hernández - Oficial de Seguridad y Privacidad de la Información GIT de Seguridad y Privacidad de la Información.

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

Versión	**Observaciones**
Versión 5 21/04/2025	Lineamientos de seguridad de la información para el uso de servicios en la nube Dirigida a las entidades del Estado

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

Lineamientos de seguridad de la información para el uso de servicios en la nube V 5.0

Tabla de contenido

Listado de Tablas

Tabla de ilustraciones

Lineamientos de seguridad de la información para el uso de servicios en la nube

1. Derechos de autor

Para el desarrollo de este documento, se recogieron aspectos importantes de mejores prácticas y documentos de uso libre por parte del NIST (National Institute of Standards and Technology – (Computer Security Incident Handling Guide), tomando como base los lineamientos recomendados en las Normas ISO/IEC 27017 e ISO IEC 27001 –2022.

2. Alcance

El presente documento, además de presentar definiciones sobre el modelo de computación en la nube, busca que las entidades del sector público puedan identificarse o clasificarse dentro de los actores y modelos de servicios de esta tendencia. Además, proporciona criterios y consideraciones que deben evaluarse y contemplarse al adquirir este tipo de servicios.

3. Introducción

3.1. Conceptos previos

En la actualidad el acceso a servicios a través de Internet se ha incrementado exponencialmente aunado a esto la pandemia del COVID-19 acelero el uso excesivo del internet como medio para apalancar sus negocios y obligando a la gran mayoría de las organizaciones a depender casi que un 100% de ella teniendo en cuenta el artículo publicado por **Data Center Market** (https://www.datacentermarket.es/tendencias-ti/el-90-de-las-empresas-ha-incrementado-el-uso-de-la-nube-por-la-pandemia/). Este hecho, así como la heterogeneidad de los dispositivos que dan acceso a estos servicios, ha supuesto un auge en el uso de las tecnologías web como un estándar.

La migración a entornos web, el uso de aplicaciones móviles y la introducción de dispositivos IoT han sido un catalizador para la externalización de los sistemas de información de un amplio número de organizaciones. Como consecuencia de esta situación surge el modelo de servicios en la nube, como una propuesta tecnológica capaz de ofrecer una gran cantidad de servicios en red de forma ágil y flexible, con grandes posibilidades de escalabilidad y reduciendo al mínimo los tiempos de despliegue.

Los servicios en la nube consisten en la disposición de software, plataformas o infraestructuras por parte de un proveedor (CSP, Cloud Servicie Provider) o por parte de la

propia entidad, accesibles en red, con independencia de donde se encuentren alojados los sistemas de información y de forma transparente para el usuario final.

Los sistemas “on premise” tradicionales ya no están tan aislados como en el pasado, presentando una mayor superficie de exposición y difuminando el perímetro de la red. El uso de la nube permite utilizar tecnologías diseñadas para responder a necesidades de externalización introduciendo arquitecturas y paradigmas de seguridad, por lo que son una alternativa segura para procesar y almacenar datos.

La provisión de servicios en la nube es un modelo que permite acceder por red a recursos de computación configurables (redes, servidores, almacenamiento, aplicaciones y servicios) que pueden suministrar y desplegar.

Este documento establece definiciones y criterios para identificar si una persona, natural o jurídica, pública o privada es proveedor de servicios de computación en la nube y presenta las consideraciones a tener en cuenta al contratar estos servicios. Además, ofrece un anexo para identificarse como actor dentro del ecosistema de computación en la nube y determinar si puede participar como proveedor de estos servicios.

Con el fin de proporcionar criterios y definiciones en referencia a la 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, el Ministerio de Tecnologías de la Información y las comunicaciones (MinTIC) desarrolla este documento y la pone a disposición de los interesados.

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, así ofrecer criterios para determinar la adecuada clasificación de los proveedores de servicios en la nube.

3.2. Características de los servicios en la nube

La característica principal de la nube es la accesibilidad de la información. Este modelo, unido a la capacidad de despliegue automático de servicios en cuestión de segundos a nivel global, facilita el acceso a la información por parte de los usuarios, con independencia del lugar o el tipo de dispositivo que se emplee: basta tener acceso a la red, aunque el uso de este paradigma implica habitualmente la necesidad de disponer de conexiones con una capacidad significativa.

Otra de las características que hacen de la nube un área en expansión es el ahorro económico. Generalmente el modelo de servicios en la nube permite reducir costes a la organización con respecto al modelo de servicio y alojamiento tradicional. Esto es por el ahorro de recursos dedicados internamente a hardware, mantenimiento, personal dedicado, suministros, espacio e instalaciones, y por el uso de economías de escala en los servicios en la nube, donde cuanto mayor es necesario para proporcionar el servicio, menor coste de estos recursos.

Por otro lado, los servicios en la nube se caracterizan por la deslocalización de datos, donde la principal ventaja es que el cliente puede decidir la geolocalización de la información y permite llevar los datos y los procesos al lugar más conveniente para la organización, además de mantener el control de acceso estén donde estén los datos.

De esta forma se pueden mantener copias del servidor repartidas en distintos puntos del planeta tanto para mejorar los tiempos de acceso y reducir la latencia al mínimo, como para evitar pérdidas de datos o servicios por la caída de un centro de proceso, manteniendo alta disponibilidad y durabilidad. Esta deslocalización tiene implicaciones de seguridad que las organizaciones deben evaluar convenientemente antes de hacer uso de los servicios en la nube, como la aplicación de legislaciones regionales sobre los datos o la baja disponibilidad de la infraestructura de red en la región, y deben aplicar medidas de seguridad y configuraciones adecuadas a cada escenario.

Por consiguiente, es pertinente que existan normas regulatorias con orientaciones internacionales sobre el tema en cuestión.

Por ello, la Norma ISO/IEC 27017:2015 es un estándar que proporciona una serie de directrices para los controles de seguridad de la información que se aplican a los servicios en la nube teniendo en cuenta los siguientes puntos:

- Orientación adicional para los controles pertinentes especificados en la ISO/IEC 27002;
- Controles adicionales determinados con directrices que se relacionan específicamente a los servicios en la nube.

Además, esta norma también ofrece controles y orientaciones tanto para los clientes de los servicios como para el CSP, Por ejemplo, la sección 6.1.1, en la que se explican los roles y responsabilidades en la seguridad de la información, se han añadido, además de las indicaciones existentes en la sección 5.2 en la ISO/IEC 27002:2022, los siguientes aspectos:

Para el cliente de los servicios en la nube

El cliente de los servicios en la nube debe estar de acuerdo con el CSP de la asignación adecuada de los roles y responsabilidades en la seguridad de la información, y confirmar que pueda cumplir esa asignación. Los roles y responsabilidades en la seguridad de la información de ambas partes deben ser establecidos bajo un acuerdo común. El cliente de los servicios en la nube debe identificar y gestionar su relación con la parte de soporte del cliente y prestar atención a la función que desempeña el CSP.

Para el CSP En esta línea, recalcando los roles y responsabilidades en seguridad de la información se recoge lo siguiente:

El CSP debe redactar y concertar una adecuada asignación sobre los roles y responsabilidades en la seguridad de la información con su cliente, los otros CSPs y sus proveedores.

Se puede observar, evidentemente que, por un lado, la ISO/IEC 27017 ha completado la ISO/IEC 27002 con aspectos especializados en los asuntos sobre la seguridad de la información almacenada en la nube; por otro lado, aunque las responsabilidades están determinadas entre ambas partes (el cliente y el CSP), en realidad, el cliente es el responsable de la decisión sobre la utilización de los servicios en la nube. Esa decisión se debe tomar atendiendo a los roles y responsabilidades determinados por el CSP

Por otro lado hay que tener cuenta, para los servicios en la nube se identifican cinco (5) características

a) Esenciales según NIST:

- ✓ Autoservicio a demanda. El cliente puede ajustar la capacidad necesaria de forma unilateral, sin necesidad de involucrar al personal del proveedor.

- ✓ Amplio acceso a través de redes. Acceso estándar a través de redes, habilitando todo tipo de dispositivos de acceso: teléfonos, tabletas, portátiles, equipos personales, servidores, etc.

- ✓ Agregación y compartición de recursos. Los recursos del proveedor se agregan y se ponen a disposición de múltiples clientes para su compartición. La agregación incluye equipos físicos y equipos virtuales que se asignan dinámicamente bajo demanda. El cliente se independiza de la ubicación física de los recursos, aunque puede delimitar ubicaciones a un cierto nivel de abstracción (país, estado, etc.) y mantienen el control de acceso a sus recursos.

- ✓ Adaptación inmediata. La capacidad requerida puede provisionarse rápida y elásticamente para seguir las variaciones de la demanda. Desde el punto de vista del consumidor, los recursos parecen ilimitados, pudiendo disponer de cualquier volumen en cualquier momento.

- ✓ Servicio consumido. El proveedor puede controlar el servicio prestado efectivo en cada momento, al nivel de abstracción que se especifique por contrato; por ejemplo, capacidad de almacenamiento, capacidad de procesamiento, ancho de banda, cuentas de usuario, etc. El uso de recursos puede ser monitorizado, controlado y auditado, proporcionando una gran transparencia tanto para el proveedor como para el consumidor del servicio utilizado.

Cabe destacar la posible dependencia de terceros en los servicios en la nube. La tendencia mayoritaria apunta hacia externalizar los servicios en la nube a terceros delegando en ellos todas las tareas de mantenimiento, adquisición de sistemas, gestión de la capacidad, etc.

Aunque se considera una ventaja, debe considerar que esta característica de externalización no debe conllevar una pérdida del control de la información o una despreocupación por la seguridad, ya que la responsabilidad final recae en el organismo contratante.

A la hora de contratar servicios en la nube es fundamental estudiar adecuadamente las condiciones del servicio y las medidas de seguridad aplicadas para confirmar que son adecuadas para los requisitos exigidos a la organización cliente, además de establecer medidas adecuadas de monitorización y vigilancia

b) 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.

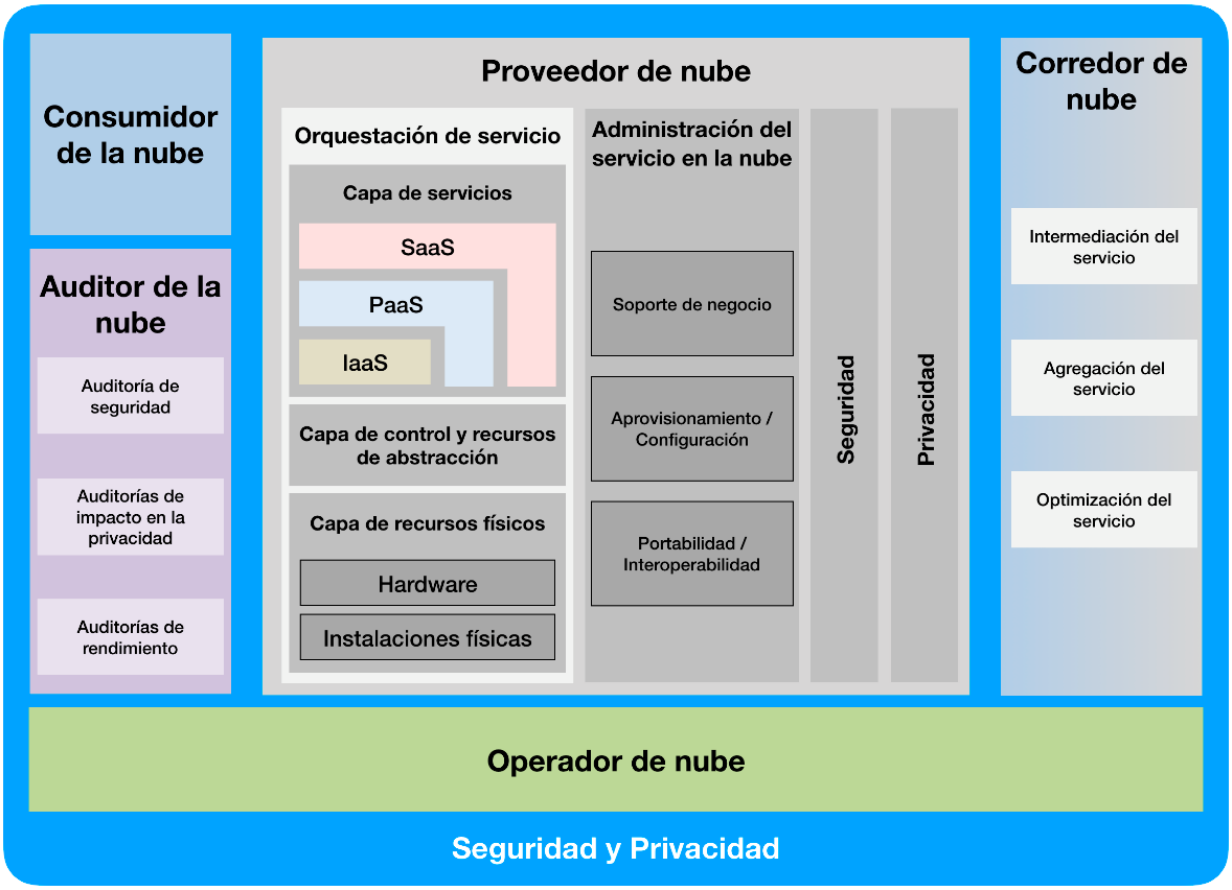


Ilustración 1 Modelo de referencia Conceptual – NIST

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.

- ✓ Consumidor Una persona u organización que mantiene una relación comercial con un proveedor de servicios Cloud y utiliza el servicio. Los consumidores de la nube necesitan un SLA, es decir un acuerdo de nivel de servicio, para especificar los requerimientos de desempeño técnicos cumplidos por el proveedor de la nube. Un SLA puede cubrir términos relativos a la calidad del servicio, seguridad y soluciones por fallas. El proveedor de la nube también puede enumerar en los SLAs un conjunto de premisas explícitamente no hechas por los consumidores (por ejemplo, limitaciones y obligaciones que los consumidores de la nube deben aceptar).

La Ilustración 2 presenta algunos ejemplos de servicios disponibles para los consumidores de la nube.

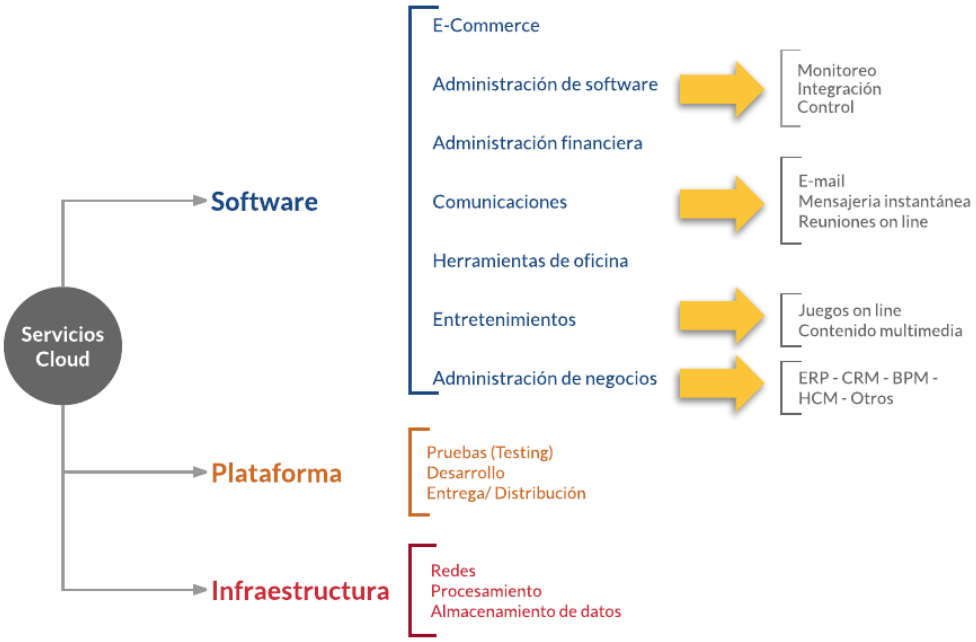


Ilustración 2 Servicios disponibles para los consumidores

Fuente: http://i.imgur.com/ItozCV2.png

- ✓ Proveedor Una persona, organización o entidad responsable de disponibilidad el servicio a las partes interesadas.

- ✓ Auditor Una parte que puede realizar una evaluación independiente de los servicios en la nube, de las operaciones del sistema de información, el rendimiento y la seguridad de las implementaciones en Cloud.

- ✓ Intermediario Una entidad que administra el uso, vela por el desempeño, por la entrega de servicios e intermedia en la relación entre los proveedores de servicios en Cloud y los consumidores finales.

- ✓ Operador Un intermediario que provee conectividad y transporte desde los proveedores de servicio hacia los consumidores.

- ✓ Operador Un intermediario que provee conectividad y transporte desde los proveedores de servicio hacia los consumidores.

La Tabla 1 enumera brevemente los actores definidos en la arquitectura de referencia de computación en la nube propuesta por el NIST [4][5].

Modelos de servicio	Actividades del Consumidor	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
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 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

Tabla 1 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 Ias 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.

c) 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 plataforma como servicio 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 Infraestructura como servicio 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 9, 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.

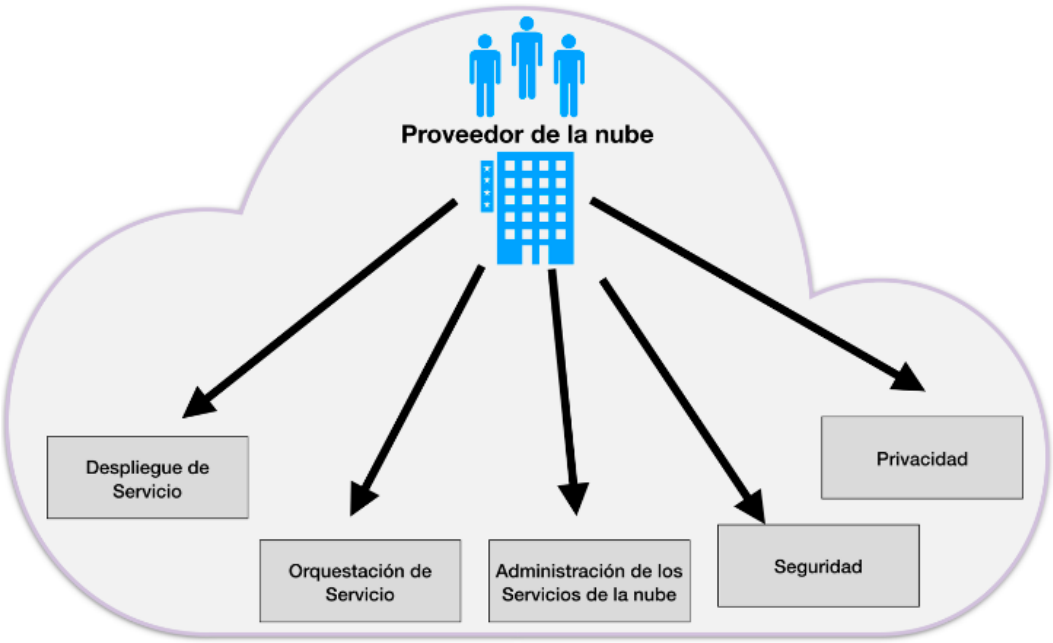


Ilustración 3 Actividades principales de un Proveedor de la nube

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.

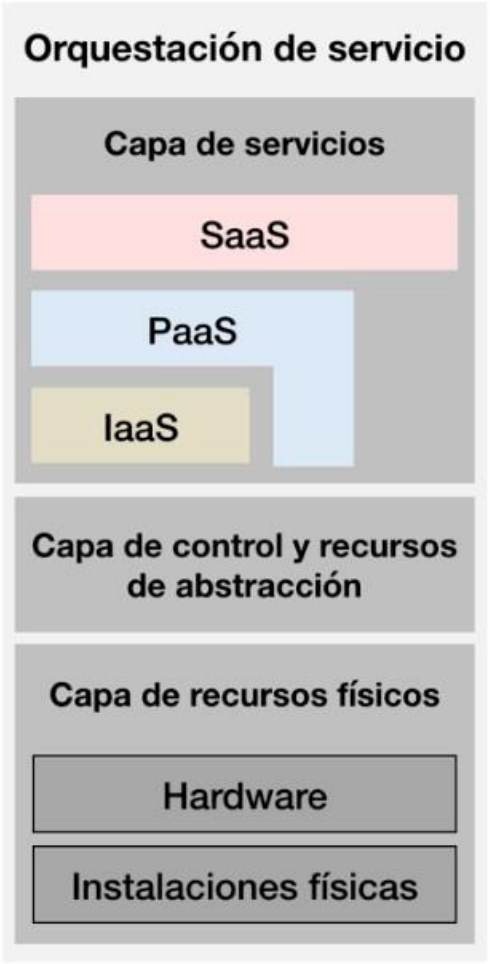


Ilustración 4 Proveedor de nube – Orquestación del Servicio

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.

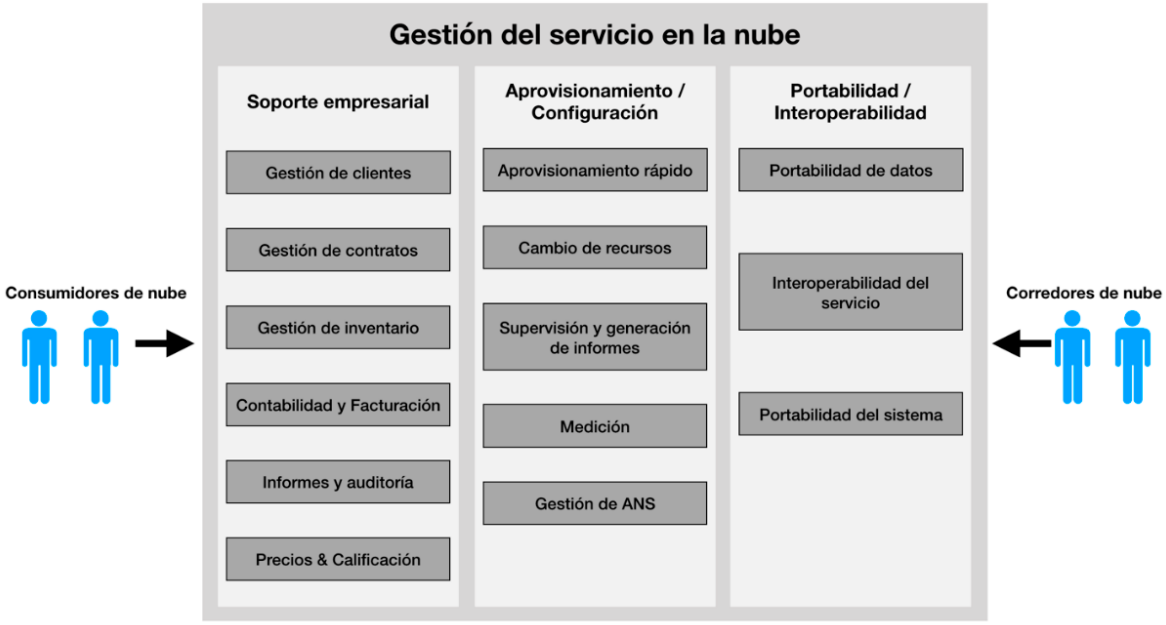


Ilustración 5 Proveedor de nube – Administración del servicio en la nube

- ✓ **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.

d) 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 auditoria sin dejar excluidos los ANS respectivos, las características esenciales de un modelo de computación en la nube.

e) 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.

f) 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].

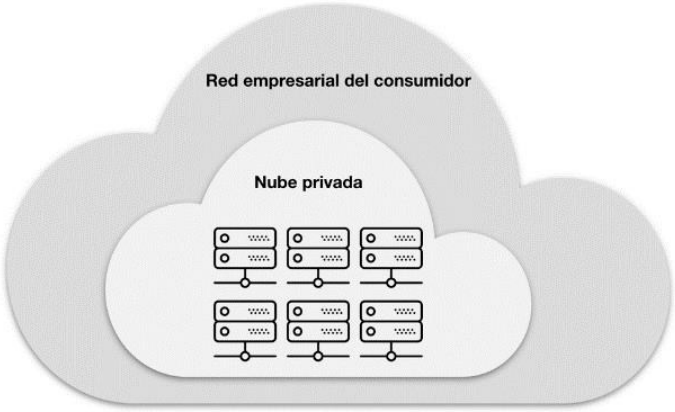
Hay que tener en cuenta que un proveedor de la nube establecerá ANS con un operador de nube para proporcionar servicios consistentes con el nivel de ANS ofrecidos a los consumidores de nube y puede requerir que el proveedor de nube proporcione conexiones seguras y dedicadas entre los consumidores de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

3.3. Modelos de despliegues

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:

3.3.1. 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 8 y 9 representan una nube privada en el sitio y una nube privada subcontratada, respectivamente.



lustración 6 Nube privada en sitio

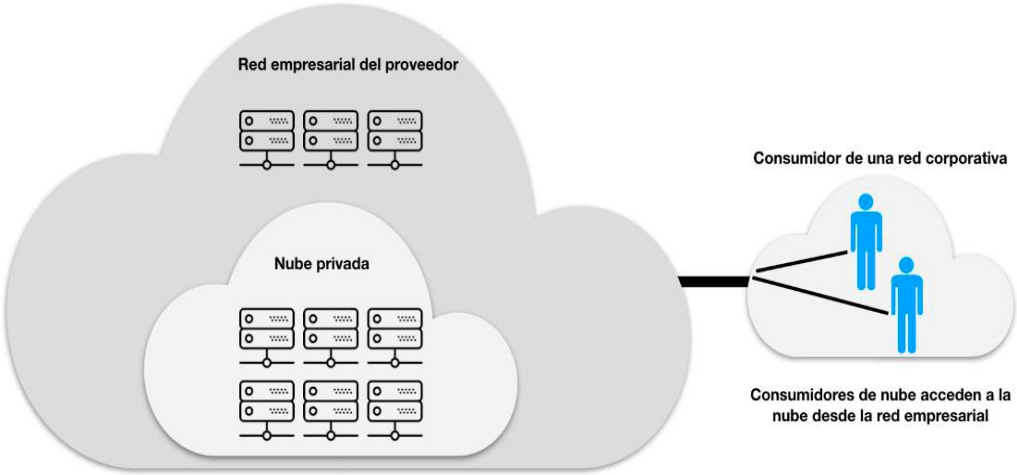


Ilustración 7 Nube privada subcontratada

3.3.2. 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 10 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.

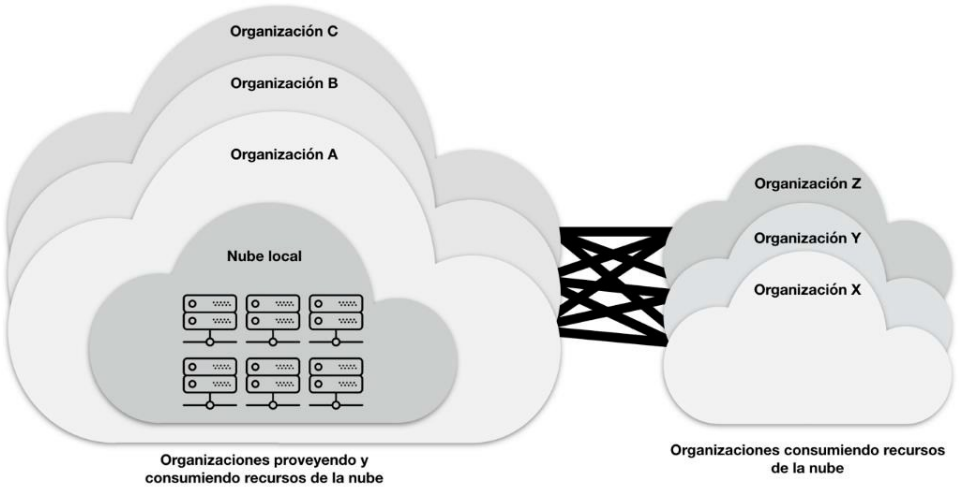


Ilustración 8 Nube comunitaria en sitio

3.3.3. 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.

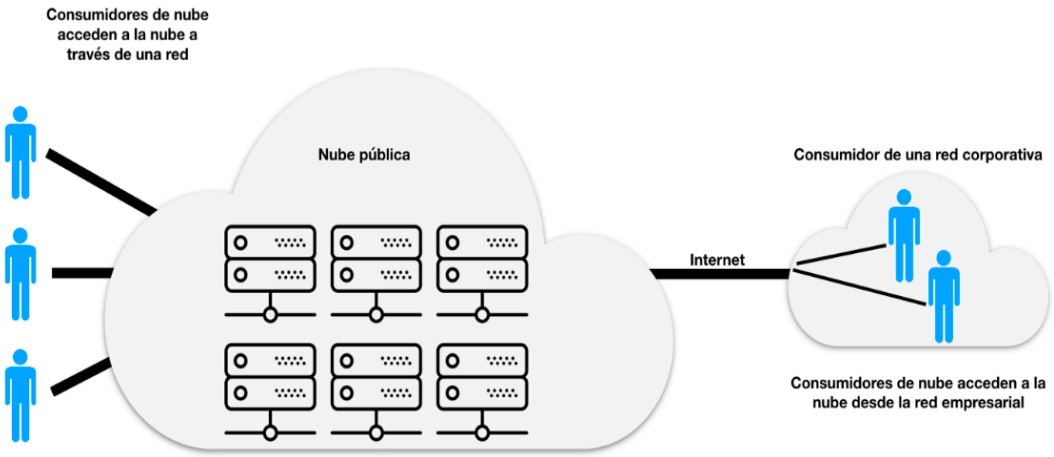


Ilustración 9 Nube pública

3.3.4. 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.

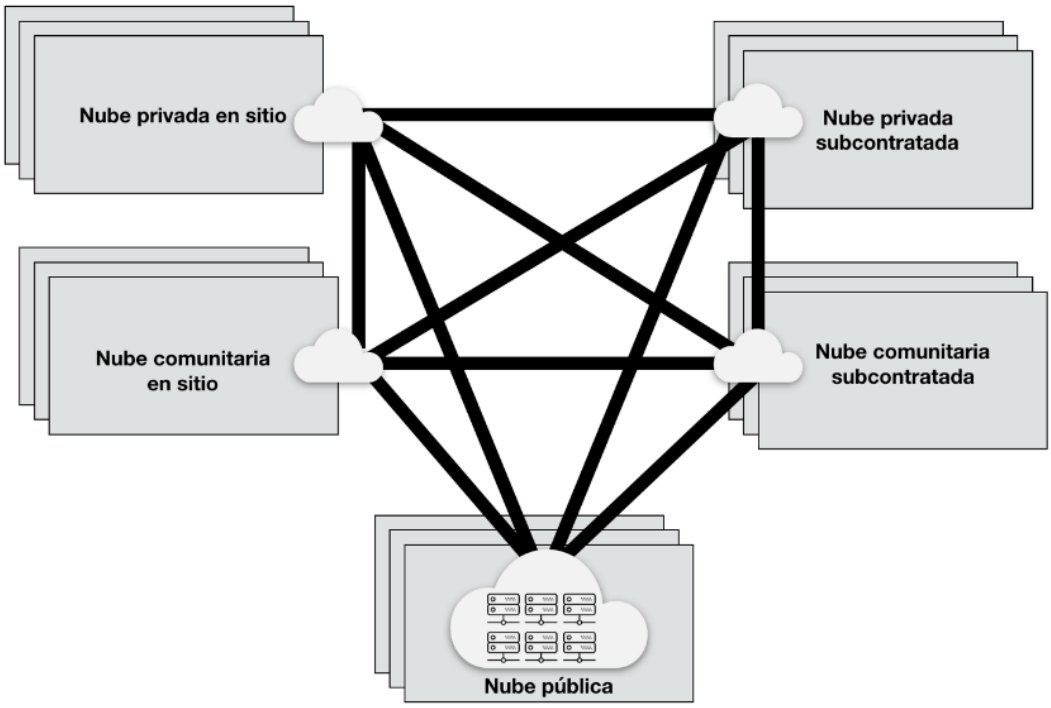


Ilustración 10 Nube híbrida

3.4. Categorías o modelos de servicios

La computación en la nube basa su arquitectura haciendo una separación entre infraestructura, plataforma y aplicaciones, como se ilustra en la figura 17 [5]:

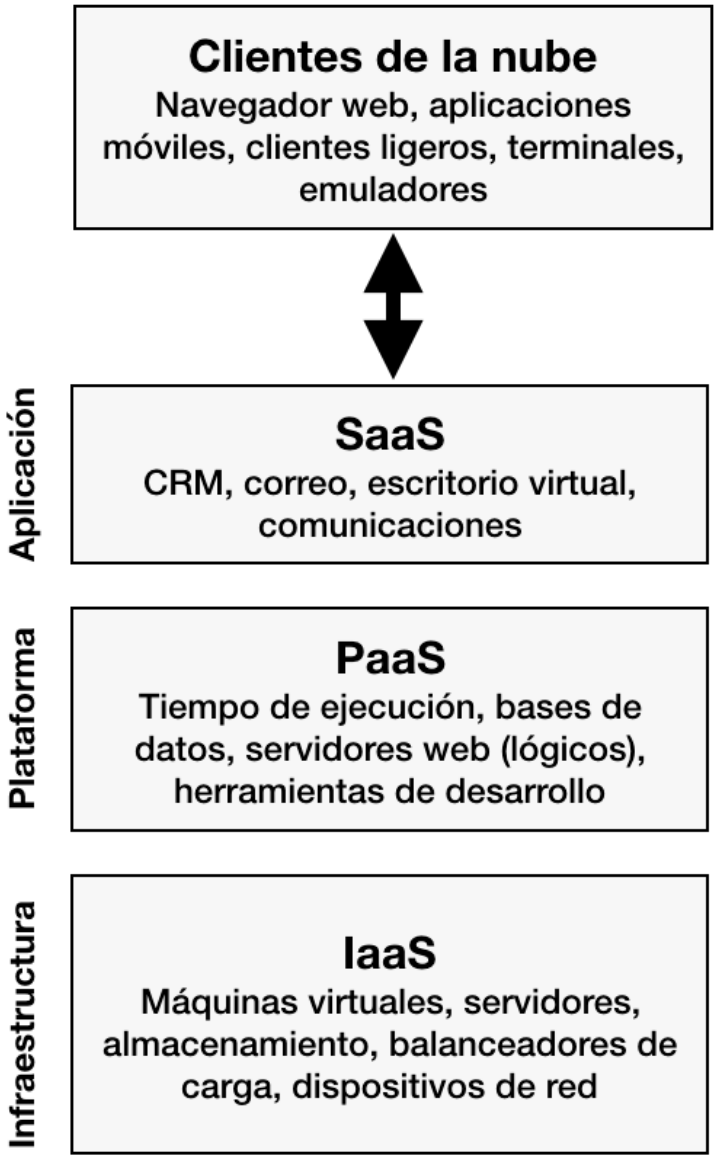


Ilustración 11 Modelos de servicios Cloud

3.4.1. 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 (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.

3.4.2. 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.

3.4.3. 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 autoaprovisionamiento 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 autoaprovisionamiento 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.

3.5. Beneficios 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:

a) 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 optimizar costos en 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. Los usos de estas alternativas hacen 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]

b) 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]

c) 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].

d) 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].

e) 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].

f) 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.

g) 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].

h) 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].

4. Seguridad y privacidad en la nube

En los últimos años, el uso de servicios en la nube por parte de entidades públicas ha aumentado significativamente debido a su flexibilidad, escalabilidad y eficiencia. Sin embargo, este crecimiento ha estado acompañado de nuevos desafíos en materia de seguridad y privacidad de la información. Los entornos de nube, por su naturaleza distribuida y altamente interconectada, introducen riesgos adicionales como la pérdida de control directo sobre los activos, la dependencia del proveedor, la exposición a legislaciones extranjeras, y la dificultad para auditar el cumplimiento de controles de seguridad.

En respuesta a estos desafíos, estándares internacionales como la **ISO/IEC 27017** (controles de seguridad en la nube) y la **ISO/IEC 27018** (protección de datos personales en entornos cloud) han establecido buenas prácticas específicas para mitigar los riesgos asociados al uso de la nube. Estas normas recomiendan, entre otros aspectos, garantizar la transparencia del proveedor, definir responsabilidades compartidas, asegurar el cifrado de la información y controlar la ubicación geográfica donde los datos son almacenados o tratados.

Por lo anterior, las entidades públicas deben exigir a sus proveedores de servicios en la nube **la declaración explícita de la ubicación física de los centros de datos donde se almacenará o procesará la información**, así como el cumplimiento de los **requisitos legales vigentes en Colombia en materia de protección de datos y soberanía digital**.

En lo posible, se deberá priorizar el uso de infraestructuras cuya geolocalización ya haya sido verificada en implementaciones anteriores dentro del país, o que se encuentren en jurisdicciones con marcos normativos equivalentes o convenios de cooperación en protección de datos personales.

Esta información deberá ser documentada como parte de la evaluación de riesgos, los contratos y los mecanismos de supervisión a proveedores, conforme a los principios de seguridad, privacidad, legalidad y responsabilidad institucional

4.1. Seguridad digtal y riesgos específicos del cloud

La seguridad en entornos cloud tiene exactamente el mismo objetivo que la seguridad digital en general: proteger nuestra infraestructura ante posibles ataques o interrupciones del servicio (ya sean accidentales o provocados). La principal diferencia la encontramos en la base de su diseño. En el caso del cloud, detrás de toda nuestra infraestructura tenemos un proveedor de servicios el cual también tiene su propia responsabilidad sobre los "assets" o "elementos" que nos ofrece como cliente de su nube. Todos conocemos las grandes ventajas de la computación en la nube o cloud computing. El principal de ellos es el considerable ahorro al no tener una infraestructura física, tanto en energía como en recursos para su configuración mantenimiento. También factores como la alta disponibilidad y las copias de seguridad de los elementos que componen la infraestructura son responsabilidades del proveedor, por lo que no tendremos que preocuparnos (al menos en principio) de ellas.

En los entornos cloud, los datos son la información más importante por proteger. Para mantener los datos lo más seguro posible es necesario cumplir tres requisitos básicos en el cloud:

1. Confidencialidad: garantizar que sólo los usuarios definidos dentro del sistema tienen acceso a la infraestructura y la información contenida en ella.

2. Integridad: los datos deben de mantenerse en su formato original, sin ningún tipo de alteración o modificación sin autorización.

3. Disponibilidad: debe de estar accesible y garantizar su acceso a todos los usuarios que necesiten acceder a la información. [21]

Ilustración 12 Capas de protección en el cloud para asegurar la información (datos)

En cambio, por otro lado, el estar en la nube implica tenerlo todo en internet, lo cual, sumado a las nuevas características del servicio ofrecido y la responsabilidad del proveedor, se abre una nueva ventana a vectores de ataques los cuales pueden ser totalmente nuevos aprovechando estas características o simplemente ser variaciones de los clásicos. Trabajar con un proveedor en el cloud, además de securizar todos los elementos que componen nuestra infraestructura (como máquinas virtuales, etc.) también debemos tener en consideración una correcta configuración y control de los servicios ofrecidos por el proveedor.

Todo lo que hemos aprendido sobre seguridad hasta ahora es aplicable al mundo del cloud, pero sin perder de vista algunos riesgos y amenazas que, aunque también sean similares en la informática en general, en el caso del cloud difieren debido a su naturaleza. Vamos a verlos en detalle para comprender mejor algunos de los riesgos específicos del cloud:

Accesos: es fundamental tener una buena política de control de accesos a nuestro sistema cloud, así como un acceso seguro y control a los servidores que componen nuestra infraestructura virtual. Una vez el usuario se ha validado correctamente es necesario controlar los diferentes recursos a los que puede acceder y evitar que tenga acceso o visibilidad a aquellos que no necesite (no sólo por seguridad, también por eficiencia del servicio). Los sistemas de doble factor de autenticación o 2FA así como las contraseñas seguras son elementos clave para evitar accesos no autorizados a nuestro entorno cloud. IAM (Identity and Access Management) es un framework que nos facilita la implementación de estos controles de accesos y gestión de la identidad presente en todos los servicios cloud.

Vulnerabilidades: el self-provisioning (autoaprovisionamiento) permite que un usuario pueda ejecutar o acceder a aplicaciones y servicios sin ser administrador del sistema o incluso sin ser parte del equipo técnico de IT. Está compuesta de una herramienta de gestión la cual controla los servicios o aplicaciones (backend). Cualquier vulnerabilidad en uno de estos servicios self-provisioning podría poner en riesgo toda la plataforma cloud. Las APIs creadas para gestionar este tipo de servicios también

tienen que estar completamente aseguradas y bien diseñadas desde el punto de vista de la seguridad.

Virtualización: todos los recursos ofrecidos por el proveedor son virtualizados y estos pertenecen a diferentes organizaciones, empresas o particulares. Por lo tanto, deben de estar aislados a nivel lógico (e incluso físico) entre ellos. Pero a pesar de este aislamiento, aparece una nueva amenaza la cual podría hacer que un potencial atacante explotara alguna vulnerabilidad, por ejemplo, del Hypervisor principal que almacena todas las máquinas virtuales de los diferentes entornos, y de esta forma tener acceso a toda la infraestructura cloud.

Tráfico de red cliente - proveedor: en el caso del cloud todas las peticiones al sistema se realizan entre cliente y proveedor del servicio cloud. Si un posible atacante puede interceptar o "esnifar" la información en tránsito nuestro servicio podría estar en peligro. Este riesgo se denomina Traffic Eavesdropping.

4.1.1. CSP y Algunos ejemplos

Vulnerabilidades: CVE y CVSS

Existen una gran variedad de proveedores de servicios cloud o CSP (Cloud Service Providers). Los más conocidos están Amazon con AWS (Amazon Web Services), Microsoft (Azure) y Google (Google Cloud), entre otros. Aunque los términos y las herramientas difieran entre los diferentes proveedores de servicios de computación en la nube, en general todos tienen un funcionamiento interno más o menos similar. El modelo de facturación es importante tenerlo claro debido a los altos costes por uso (se suelen tarificar por tiempo de utilización normalmente en fracciones de segundo).

4.1.2. Vulnerabilidades: CVE y CVSS

El mayor vector de ataque contra una infraestructura cloud se basa en aprovechar vulnerabilidades en todo tipo de software, desde aplicaciones hasta incluso el sistema operativo. Por lo tanto, es importante saber identificarlas teniendo claro qué significan las siglas CVE o Common Vulneratilities and Exposures. El etiquetado CVE tiene el siguiente formato general: CVE-AAAA-NNNN, AAAA es el año de descubrimiento de la vulnerabilidad y NNNN su número único asignado. Cuando una nueva vulnerabilidad solicita un código CVE, durante proceso de aceptación comenzarán con CAN-AAAA-NNNN.

Por otro lado, CVSS o Common Vulneratility Scoring System en la versión 3.0, ofrece una puntuación final indicando el nivel de amenaza de la vulnerabilidad con un valor entre 0 (menos importante) y 10 (crítica).

Ejemplo de etiquetado CVE y puntuación CVSS de la vulnerabilidad “Meltdown”: CVE-2017-5754. AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:N/A:N

Puntuación CVSS: 5.6 Medium

Fuente: https://nvd.nist.gov/vuln/detail/CVE-2017-5754

4.1.3. Responsabilidad compartida (CSP y Cliente)

A la hora de contratar un servicio con un CSP es necesario tener perfectamente atados y claros los límites de la responsabilidad, tanto por parte del CSP como por parte del cliente, en los recursos y el servicio ofrecido. Es importante resaltar que contratar este tipo de servicios implica que todos nuestros datos, así como la infraestructura, pasa a manos de una empresa externa o un tercero y, por lo tanto, tener claro que el CSP no se hará cargo de todos los problemas de seguridad que puedan aparecer. Es decir, el CSP sólo será responsable de los servicios asociados directamente a su diseño, como por ejemplo ofrecer acceso seguro a bases de datos, almacenamiento, aislamiento, interrupción de energía, etc.

Nosotros como clientes, seremos responsables de cumplir e implementar lo que sea necesario para proteger nuestra infraestructura. El cliente es el responsable de toda la seguridad de sus activos en la nube. Pero no sólo eso, también es responsable de la correcta configuración y seguridad de la configuración de los servicios ofrecidos por el CSP como son por ejemplo los accesos, monitorización, gestión de logs, etc. La gestión de accesos es crítica ya que afecta no sólo a nuestra infraestructura ubicada en la nube, sino también a la gestión de la misma.

Haciendo un resumen estas son las responsabilidades clave de cada uno:

CSP:

- Accesos de administrador de los clientes.
- Actualizaciones y seguridad del Hypervisor que sustenta la infraestructura.
- Seguridad de los servicios.
- Aislamiento respecto a otros clientes del CSP.
- Protección ante ataques DDoS o similares.
- Almacenamiento, computación, bases de datos, red perimetral y cualquier otro servicio ofrecido por el CSP están bajo su responsabilidad

Cliente:

- Gestión, monitorización y securización de la red interna.
- Configuración, mantenimiento, monitorización y actualizaciones de las aplicaciones ubicadas en el servicio.
- Creación de políticas de seguridad para la red y todos los elementos que conforman la infraestructura.

- Cifrado.
- Fortificación de los servidores virtuales

4.1.4. Autenticación y autorización (IAM)

Antes, se ha mencionado el concepto de IAM o Identity and Access Management. Este servicio es realmente importante ya que es el portal principal que da acceso a todos nuestros servicios, así como su control, dentro de la nube. Por lo tanto, será necesario crear unas políticas responsables las cuales incluyan una asignación correcta de los usuarios y sus accesos mediante la creación de grupos y roles varios. Todos los proveedores de servicios cloud ofrecen utilidades o incluso un panel de control a los diferentes clientes del cloud. Cuando nos damos de alta por primera vez en uno de estos servicios, siempre lo haremos con una cuenta principal, a veces denominada también root.

La primera de las medidas de seguridad está asociada a esta cuenta: nunca utilizarla en tareas cotidianas, esta cuenta se debe de utilizar las tareas concretas de administración de cuentas y algunos servicios críticos. La segunda está orientada más a los accesos, es decir, será necesario tener un control con la máxima información detallada de los accesos a nuestro sistema por parte de clientes o trabajadores.

No debemos olvidar por otro lado, que los accesos no se realizan sólo por personas y contra el frontend del CSP los cuales tienen una estructura similar a esta en la cual tenemos que introducir nuestro usuario y contraseña:

También es posible que programas accedan a nuestros servicios utilizando APIs. Por lo tanto, será necesario también una serie de políticas y controles de seguridad a la hora de la creación de código.

4.1.5. MFA o Multi Factor Authentication

Es una capa adicional de seguridad además del usuario y la contraseña. En otras palabras, no es más que un 2FA o Doble Factor de Autenticación. Es decir, cuando el usuario acceda a la cuenta de del CSP, si tiene activada esta opción será necesario introducir también una respuesta adicional (suele ser un token) generada por un dispositivo externo o una aplicación. Dicho dispositivo (un Smartphone es el más extendido, aunque existen muchos otros) nos genera una nueva contraseña o token la cual introduciremos junto a nuestras credenciales normales.

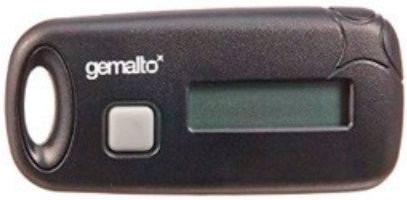


Ilustración 13 Ejemplo de MFA físico modelo SafeNet IDProve 100 6-digit OTP Token.

Fuente: https://aws.amazon.com/es/iam/features/mfa/?audit=2019q1

Las aplicaciones virtuales son las más extendidas ya que pueden instalarse en un teléfono móvil. Las principales opciones son: Google Authenticator y Authy 2FA.

Es importante destacar que la pérdida de nuestro elemento 2FA, ya sea físico o virtual (es decir, el dispositivo donde se encuentra almacenada la aplicación, un Smartphone, por ejemplo) implica perder el acceso a nuestros sistemas. Para poder volver a acceder será necesario hablar con nuestro proveedor CSP para dar de baja el dispositivo y volver a dar de alta otro nuevo.

4.1.6. AK/SK, Access Key y Secret Key

Aparte de los accesos habituales por parte de usuarios a nuestro cloud o los servicios que tengamos alojados en ella, también hay que tener en cuenta otro tipo de acceso: el realizado automáticamente por un programa desde una API. Si nuestro servicio ofrece una API para acceder a él o ejecutar algún servicio dentro de una aplicación diseñada a medida, debemos tener en cuenta y controlar su seguridad.

Una Access Key (AK) es un token alfanumérico de cierta longitud (más de 10 caracteres) la cual permite el acceso de la API desde un programa. Este token a su vez lleva asociada una Secret Key (SK) única para el usuario/programador la cual no se debe compartir ni poner visible en el código fuente. El CSP entrega estas contraseñas una vez solicitadas mediante una única descarga por lo tanto es necesario almacenarlas en un lugar seguro. Todos estos accesos mediante API se pueden controlar y gestionar desde el panel de control IAM.

4.1.7. Políticas (policies)

Antes incluso de empezar a crear los usuarios, grupos y roles, será necesario revisar y crear las políticas necesarias de las cuales definirán a qué recurso del sistema podrán acceder. Las políticas prácticamente en todos los proveedores están siempre relacionadas con dos factores: la identidad (el usuario o grupo) y un recurso concreto (por ejemplo, una instancia). Estas políticas son ficheros con formato JSON y el siguiente ejemplo muestra Script o líneas de códigos para configurar una política de un CSP de sólo lectura, es decir, si se aplica a un usuario este sólo podrá consultar los recursos, pero no podrá realizar ninguna acción sobre ellos:

{

“Version”: “2012-10-17”,

“Statement”: [{

“Effect”: “Allow”,

“Action”: “ec2:Describe*”,

“Resource”: “*”

}

]

}

El campo “Versión” como su nombre indica la versión de esta política. Por otro lado “Statement” se compone a su vez de las siguientes acciones: “Effect” (permite o deniega la acción que ahora tendrá definida), “Action” es la acción a realizar y “Resource” define el recurso sobre el cual estamos aplicando la política.

4.1.8. Usuarios, grupos y roles

La autorización de los diferentes usuarios es una tarea básica que a su vez necesita de una buena planificación y control para asignar correctamente desde sus privilegios de acceso como las tareas que puede ejecutar dentro del cloud. Como es lógico, esta será la primera de las tareas después de contratar nuestro servicio cloud pero no debe limitarse exclusivamente a crear los usuarios y sus accesos. Una vez creado el usuario y su perfil será imprescindible clasificarlo y es aquí donde entran los grupos. Aunque el primer paso después de crear un usuario será siempre aplicarle una política, el siguiente será asignado a un grupo concreto.

Un grupo en un CSP funciona igual que los grupos Linux, Windows, AD, etc. Un grupo tiene asociado una lista de elementos, en este caso usuarios, que se agrupan en un nombre (nombre del grupo). Esto nos permite manipular a dichos usuarios sin tener que hacerlo de forma individual ya que el nombre de grupo se asocia a todos ellos. Por ejemplo, el siguiente árbol muestra una organización donde podemos observar, entre otros detalles, que un usuario puede pertenecer a más de un grupo:

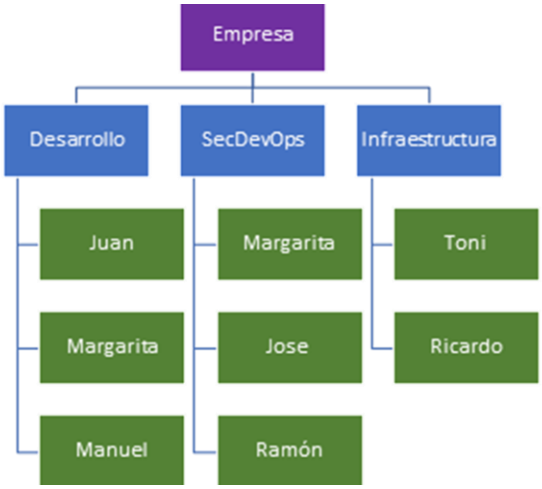


Ilustración 14 Ejemplo Usuarios, grupos y roles

Podemos observar tres grupos llamados "Desarrollo", "SecDevOps" e "Infraestructura". La usuaria Margarita está presente en dos ellos, "Desarrollo" y "SevDevOps" por lo tanto tendrá aplicadas todas las políticas asignadas dichos grupos.

El paso final una vez tenemos los grupos y los usuarios son los roles o conjunto de permiso que permiten realizar acciones sobre los recursos del CSP. Aquí tenemos que destacar el término cross-role, el cual permite que un mismo usuario pueda acceder a las cuentas de todo el sistema. Los permisos de los roles también se gestionan con las correspondientes políticas asignadas. Algunos de los usos prácticos de los roles son:

- **Role de servicio**. Se aplica a un servicio de CSP para realizar acciones como crear instancias, etc.
- **Role de servicio asociado a una instancia**. Permite que la instancia pueda por ejemplo ampliar el espacio de disco, etc.
- **Role vinculado a un servicio**. Son roles de servicio, pero vinculados exclusivamente a uno en concreto, como por ejemplo Elasticsearch el cual sirve para gestionar clúster.
- **Delegación de roles**. Necesario para que una cuenta maestra pueda controlar y por ejemplo ejecutar un servicio en otra cuenta. Federación, por ejemplo, para hacer login en la consola de CSP mediante el login de Facebook, Google, etc.
- **Encadenamiento de roles**. Concatenación entre diferentes roles entre ellos.

4.1.9. IDP o Identity Providers

Si nuestra organización ya tiene por defecto una estructura de usuarios, como por ejemplo puede ser un LDAP, con esta función tendremos la opción de administrarlas desde la cuenta de un CSP que la entidad halla contratado. De esta forma no será necesario dar de alta a dichos usuarios directamente en el CSP, ya que su

configuración, función y datos se heredan directamente del directorio de uso corporativo que estemos utilizando.

Para poder utilizar un IDP en un CSP es necesario siempre crear una relación de confianza entre el CSP y el IDP. Una vez creada la relación de confianza obtendremos algunas ventajas como por ejemplo utilizar un mismo usuario que pueda acceder al entorno cloud y también al resto de servicios corporativos fuera del cloud, facilidad a la hora de gestionar contraseñas (podemos hacerlo directamente desde nuestro servicio de directorio), reflejo inmediato en el cloud de cualquier cambio realizado en la estructura del directorio (altas de usuarios, bajas, cambio de contraseñas, etc.) Es necesario que el servicio de directorio que tengamos en nuestra organización sea compatible con OpenID Connect (OIDC) o SAML 2.0.

4.1.10. Criptografía

El mantener oculta la información que está almacenada o recorre nuestra infraestructura es una tarea fundamental y clave en nuestros sistemas, además de ser obligatoria como indica la GDPR. La criptografía se encarga de estudiar las diferentes técnicas o métodos de protección de la información. Para ello utiliza diferentes algoritmos de cifrado para de esa forma, conseguir ocultar la información real almacenada. Para poder obtener de nuevo la información original será necesario disponer de una clave secreta (o clave de descifrado).

Centrándose en los tipos de cifrado según sus claves:

Simétrico: la misma clave es utilizada tanto para cifrar como para descifrar la información. Los más conocidos son el DES, Triple DES, AES, etc.

Asimétrico (o clave pública): en este caso se utilizan claves distintas, en concreto dos: una pública y otra privada. La clave privada sirve para descifrar la información y la pública se utiliza sólo para el cifrado. RSA y PGP son los más conocidos.

Según la naturaleza de la arquitectura, debemos tener en cuenta de los datos están en reposo (por ejemplo, almacenados en alguna ubicación) o en tránsito (cuando se desplazan de un sistema o servicio a otro). El siguiente listado muestra algunos de los conceptos de criptografía y su definición utilizados en la gran mayoría de los CSP:

Datos autenticados adicionales (AAD): integridad y autenticidad de datos mediante el uso de datos autenticados adicionales durante el proceso de cifrado (datos autenticados, pero no cifrados).

Autenticación: Determina si una entidad es quien afirma ser, o que no la han manipulado entidades no autorizadas.

Autorización: Acceso legítimo autorizado de una entidad a un recurso.

Cifrado de bloque: se utiliza para cifrar información con una longitud aleatoria, es decir, la longitud (por ejemplo, en caracteres) del texto sin cifrar no es la misma que el texto cifrado.

Clave de datos: clave simétrica que genera el CSP, utilizada para cifrar o descifrar información.

Descifrado: proceso de convertir la información cifrada en el formato que tenía antes del cifrado.

Cifrado: aplicar un algoritmo que oculte la información real ofreciendo confidencialidad de datos a un mensaje o datos no cifrados.

Contexto de cifrado: AAD específicos de los KMS con el formato de par “clave“: “valor”. Aunque no está cifrado, está vinculado al texto cifrado durante el cifrado y se debe pasar de nuevo durante el descifrado.

Clave maestra: Una clave creada por los KMS que solo se pueden utilizar en el servicio de estos KMS. La clave principal se utiliza habitualmente para cifrar claves de datos para que el servicio pueda almacenar la clave cifrada de forma segura. [21]

4.1.11. Secrets Manager

Los CSP ofrecen esta herramienta para gestionar los datos confidenciales (también llamados habitualmente “secretos”) relacionados con el acceso a los servicios. Es decir, es un gestor de credenciales (también tiene su propia API) el cual ayuda al administrador del sitio a ampliar la seguridad sobre sus diferentes elementos de la infraestructura. Por ejemplo, permite administrar el acceso a los datos confidenciales basándose en políticas creadas previamente con el IAM.

Un secreto puede ser cualquier tipo de información que ofrezca algún dato confidencial o sensible. Por ejemplo, el nombre de un servidor, un puerto, una dirección IP, nombre de usuario, contraseña, etc. Cifra esta información utilizando los KMS el cual se encarga de generar claves para el cifrado o descifrado. El transporte de este tipo de información también es importante y por lo tanto los Secrets Manager sólo lo hace utilizando el estándar TLS y PFS (Perfect Forward Secrecy). Una característica a tener en cuenta que aumenta también la seguridad es la rotación. La rotación permite crear de forma automática nuevas versiones del tipo de cifrado del secreto. En general estas herramientas, Secrets Manager cuentan con una interfaz web de control y un CLI. [21]

4.1.12. Certificate Manager (CM)

Esta herramienta permite gestionar los certificados SSL/TLS, los cuales se utilizan para proteger las comunicaciones. En definitiva, los Certificate Manager es un gestor de certificados que permite la compra, carga, renovación o cualquier otra gestión asociada a un certificado (ya sea público o privado), todo de forma automática. Esta herramienta, se integra con el resto de los servicios de la nube del CSP. CM también genera sus propios certificados públicos basados en el dominio (DV) y tienen una validez por lo general de 13 meses. [21]

5. Computación en la nube en Colombia

5.1. 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 Digital . 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 deben 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, teniendo en cuenta a sección abreviada de la Ley 80 de 1993 y la Ley 1150 de 2007 para acceder a los Acuerdo Marco de Precios.

Así mismo, los diferentes conceptos, cartillas y demás que la Superintendencia de Industria y Comercio publicó para aplicarlo en cuanto a los datos y computación en la nube [12] [18].

6. Pasos fundamentales para dar el salto a la nube

6.1. Identificación y análisis de riesgos de migrar a la nube.

Con el análisis de Riesgo, los objetivos misionales y funcionales de la Entidad, así como la estrategia de TI para apoyar dichas actividades, es de vital importancia para la toma de decisiones de lo que se debe o puede migrar a la Nube. Teniendo en cuenta lo anterior estos pueden ser:

- Datos.
- Servicios.
- Aplicaciones.
- Funcionalidades o Procesos.

Una de las actividades más importante es la evaluación de riesgo de los activos que se van a mover a la nube, en esta la entidad identifica los datos y funcionalidades a mover. También debe tener presente el aumento de tráfico, operaciones y datos; los cuales pueden ser mayores de lo planeado.

Identificar que tan importantes son las operaciones y/o datos para la entidad; donde se determine qué tan confidencial es la información, el proceso, la operación o función a migrar. La entidad puede realizar una autoevaluación a través de preguntas sencillas donde identifique el valor de los activos en términos de confidencialidad, disponibilidad, integridad y su riesgo asociado al llevar los datos a la nube parcial o totalmente.

Por ejemplo: Que impacto tendría en la entidad si:

- El activo estuviera expuesto públicamente
- Un funcionario del tercero o proveedor accediera al activo
- Un proceso fuera modificado por un externo
- Un proceso o alguna de sus funciones entregaran resultados erróneos
- La información o datos fueran modificados de manera inesperada
- Se presentarán fallas de disponibilidad

6.2. 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 momento de adquirir servicios de Nube Pública y Nube Privada a través de los AM de TI.

6.3. 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 cotice 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 [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, 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.

6.4. 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: 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 se considere adecuado mantener alojadas en centros de datos propios

6.5. Definición De La 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 puede generar accesos no autorizados a datos confidenciales, sin embargo, cabe aclarar que los esquemas de computación en la nube cuentan con las herramientas necesarias que garantizan un ambiente seguro entre usuarios. 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]. Además, es importante aclarar que, al ser un modelo de seguridad compartido, la responsabilidad de la seguridad recae en ambas partes y se debe verificar: que el proveedor cuente con las herramientas y condiciones requeridas y que la entidad las usa bien.

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), Ley de Protección de datos personales 1581 de 2012 y demás normatividad 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].

Una estrategia que implique usar los servicios en la nube en empresas tiene sentido en primera instancia, solo si los aspectos de seguridad sean garantizados en su totalidad. [20].

6.6. 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: 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, entre otros que defina el proveedor de nube. [13]

6.7. Gestión de Cambios

Las entidades deberán establecer contractualmente la obligación de mantener actualizados los sistemas para garantizar su funcionamiento, así como eliminar las 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. [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

6.8. 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].

Adicionalmente la entidad debe asegurarse que la residencia física de los datos se encuentre en uno de los países que ofrecen un nivel adecuado de protección de datos de acuerdo con los estándares fijados por la Superintendencia de Industria y Comercio sobre la materia, garantizando el cumplimiento del artículo 26 de la Ley Estatutaria 1581 de 2012

6.9. 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, hibridas o comunitarias, el servicio se puede prestar a través de redes MPLS, Metroethernet entre otras.

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

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. [9]

6.11. Acuerdos de Nivel de servicio (ANS).

Para todos los servicios de informática en la nube se deben establecer acuerdos de nivel de servicio donde se detallen aspectos como: controles, reglamentación, medidas de protección y seguridad, plazos de recuperación del servicio, indicadores y forma de medición de indicadores de calidad del servicio, valores mínimos aceptables, tiempos de respuesta ante una eventual falta de disponibilidad, penalizaciones y el régimen de responsabilidad por daños y perjuicios ocasionados por un incumplimiento del proveedor, limitaciones al servicio o a sus garantías, solicitudes de cambio, gestión de incidentes, regulación de la seguridad y el tratamiento de datos y terminación del servicio/contrato. 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]

6.12. 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

6.13. 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. [12] [13].

6.14. 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 que el aislamiento de la carga de trabajo es menos un problema de seguridad que en una nube

pública (se debe considerar que los protocolos de seguridad de estas nubes se encuentran definidos 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 red de la organización de consumidor de nube, mientras que una nube privada externalizada tiende a requerir tal protección perimetral en el límite [13] [14] [15].

Hay que hablar de seguridad compartida, ya 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. El proveedor suele realizar controles de administración de cuenta para usuarios privilegiados del sistema inicial en escenarios IaaS, mientras que la administración de cuentas de usuarios de aplicaciones para la aplicación desplegada en un entorno IaaS no es responsabilidad del proveedor [13] [14] [15].

6.15. 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 [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.

7. Gobernanza de la Nube

La gobernanza de la nube es un conjunto de reglas y políticas adoptadas por las empresas que ofrecen servicios en la nube. El objetivo de la gobernanza de la nube es mejorar la seguridad de los datos, gestionar los riesgos y permitir el funcionamiento sin problemas de los sistemas en la nube.

La nube facilita más que nunca que los equipos de las entidades desarrollen sus propios sistemas e implementen activos con un solo clic. Si bien esto promueve la innovación y la productividad, también puede causar problemas como:

- Mala integración entre sistemas en la nube, incluso dentro de la misma organización
- Duplicación de esfuerzos o datos entre diferentes partes de la organización
- Falta de alineación entre los sistemas de nube y los objetivos comerciales
- Nuevos problemas de seguridad, por ejemplo, el riesgo de implementar sistemas en la nube con un control de acceso débil o inexistente

La gobernanza de la nube garantiza que la implementación de activos, la integración de sistemas, la seguridad de los datos y otros aspectos de la computación en la nube se planifiquen, consideren y gestionen adecuadamente. Es muy dinámica, porque los sistemas en la nube pueden ser creados y mantenidos por diferentes grupos de la organización, involucrar a proveedores externos y pueden cambiar a diario.

Las iniciativas de gobernanza de la nube garantizan que este entorno complejo cumpla con las políticas organizacionales, las mejores prácticas de seguridad y las obligaciones de cumplimiento.

7.1. Importancia de la gobernanza en la nube

A continuación, se presentan algunas formas en las que la gobernanza de la nube puede beneficiar a una organización que ejecuta servicios críticos en la nube.

- Mejora la gestión de recursos en la nube

La gobernanza de la nube puede ayudar a dividir los sistemas de la nube en cuentas individuales que representan departamentos, proyectos o centros de costos dentro de la organización. Esta es una práctica recomendada por muchos proveedores de servicios en la nube. Separar las cargas de trabajo de la nube en cuentas separadas puede mejorar el control de costos y la visibilidad, y limitar el impacto comercial de los problemas de seguridad.

- Reduce la TI en la sombra

Los riesgos y los costos de los sistemas en la nube aumentan significativamente si la organización no sabe qué sistemas y datos se implementan y dónde. Hoy en día, es muy común que los empleados recurran a sistemas de TI ocultos cuando no obtienen una respuesta rápida de los servicios de TI tradicionales. La gobernanza de la nube permite a los empleados solicitar recursos en la nube de una manera cómoda, pero que aplica los controles y la visibilidad pertinentes para la organización. En lugar de recurrir a TI en la sombra, los empleados pueden recibir acceso a los sistemas en la nube, dentro de las limitaciones presupuestarias y de cumplimiento de la organización.

- Reduce los gastos administrativos

Sin un programa de gobernanza de la nube y soluciones tecnológicas que lo respalden, las organizaciones tienden a utilizar hojas de cálculo u otros procesos manuales para realizar un seguimiento de las cuentas de la nube, los costos y los problemas de cumplimiento, o para controlar el acceso y los presupuestos de los recursos de la nube. Esto es ineficiente, propenso a errores y falla a gran escala. Una solución completa de gobernanza de la nube permite a las organizaciones definir políticas de forma centralizada y aplicarlas a toda la

infraestructura de la nube. Centraliza el control sobre el acceso y los costos, genera alertas y facilita la respuesta ante infracciones. Esto ahorra tiempo y esfuerzo, reduce el riesgo de actividades no conformes y costos inesperados en la nube.

Mejora los problemas de seguridad en la nube

Un modelo de gobernanza de la nube establece una estrategia de autenticación para proteger la confidencialidad, integridad y disponibilidad de la información. Permite a la organización que, sin importar dónde se encuentren los datos o se implementen los sistemas críticos, haya visibilidad de la información confidencial y garantías de que se implementen los controles de seguridad adecuados.

7.2. Principios del modelo de gobernanza de la nube

Los siguientes cinco principios son un buen punto de partida para construir su modelo de gobernanza de la nube:

1. Cumplimiento de políticas y estándares: los estándares de uso de la nube deben ser coherentes con las regulaciones y los estándares de cumplimiento utilizados por su organización y otros en su industria.

2. Alineación con los objetivos empresariales: la estrategia de la nube debe ser parte integral de la estrategia empresarial y de TI general. Todos los sistemas y políticas de la nube deben respaldar de manera demostrable los objetivos empresariales.

3. Colaboración: debe haber acuerdos claros entre los propietarios y usuarios de la infraestructura de la nube y otras partes interesadas en las unidades organizativas pertinentes, para garantizar que hagan un uso apropiado y mutuamente beneficioso de los recursos de la nube.

4. Gestión de cambios: todos los cambios en un entorno de nube deben implementarse de manera consistente y estandarizada, sujetos a los controles adecuados.

5. Respuesta dinámica: la gobernanza de la nube debe basarse en la supervisión y la automatización de la nube para responder dinámicamente a los eventos en el entorno de la nube.

7.3. Como se diseña e implementa un marco de gobernanza en la nube

Los siguientes son los componentes principales de un marco de gobernanza de la nube.

Ilustración 15 Componentes de un marco de gobernanza de la nube

Gestión financiera en la nube

En muchas organizaciones, los costos de la nube se salen rápidamente de control. Los servicios en la nube a menudo prometen reducir los costos de TI, pero esto solo es cierto si los costos se gestionan adecuadamente. Hay tres elementos de la gestión financiera de la nube:

- Políticas financieras que aclaren cómo la organización planea utilizar la nube. Por ejemplo, las políticas pueden definir en qué casos se deben utilizar servicios gestionados para reducir los costos operativos internos o especificar una lista de verificación de gestión de costos que se debe seguir antes de implementar nuevos servicios en la nube.
- Los presupuestos definen la asignación específica para diferentes partes de la organización o diferentes categorías de servicios en la nube.
- Es difícil lograr informes de costos de manera consistente. Algunos servicios en la nube tienen cargos impredecibles que pueden aparecer en diferentes lugares de la infraestructura en la nube; por ejemplo, las instantáneas de la nube que se usan para realizar copias de seguridad se pueden almacenar en diferentes regiones y cuentas. Puede usar herramientas de informes de costos proporcionadas por el proveedor de la nube o adoptar herramientas de terceros que cubran varias nubes.

Gestión de operaciones en la nube

La gestión de operaciones implica definir procesos para la implementación de servicios. Estos procesos deben incluir:

- Una definición clara de los recursos asignados al servicio a lo largo del tiempo
- Acuerdos de nivel de servicio (ANS) para definir el rendimiento esperado
- Monitoreo continuo para garantizar que se cumplan los ANS
- Proceso y comprobaciones necesarias antes de implementar el código en producción

- Requisitos de control de acceso

Una gestión eficaz de las operaciones en la nube es una forma excelente de evitar la TI en la sombra. Puede ahorrar costes al evitar el uso innecesario de recursos en la nube y puede mejorar drásticamente el retorno de la inversión en la nube a largo plazo.

Gestión de datos en la nube

La nube facilita la recopilación y el análisis de grandes cantidades de datos, pero esto hace que la gestión de datos sea un desafío mucho mayor. La gobernanza de la nube debe especificar cómo gestionar todo el ciclo de vida de los datos en la nube. Esto incluye:

- Elaborar un esquema de clasificación de datos y establecer políticas para los datos en diferentes niveles de sensibilidad
- Garantizar que todos los datos estén cifrados, en reposo y en tránsito
- Establecer controles de acceso adecuados para cada tipo de datos
- Uso del enmascaramiento de datos para reducir el riesgo de datos confidenciales cuando se utilizan para escenarios como desarrollo, pruebas o capacitación
- Desarrollar una estrategia de niveles, moviendo datos a lo largo del tiempo desde sistemas de acceso rápido de alto costo a sistemas de archivo de menor costo
- Garantizar que la gestión del ciclo de vida de los datos esté automatizada: esto es fundamental para aplicar políticas en implementaciones de nube a gran escala.

Gestión de la seguridad y el cumplimiento normativo en la nube

La gobernanza de la nube asume la responsabilidad de todos los temas clave de la seguridad empresarial. Determina cuáles son los requisitos de seguridad y cumplimiento de la organización y garantiza su cumplimiento en el entorno de la nube:

- Evaluación de riesgos
- Gestión de identidad y acceso
- Gestión de datos y cifrado
- Seguridad de la aplicación
- Recuperación de desastres

La gobernanza de la nube debe lograr un equilibrio entre los impulsores y requisitos del negocio, los riesgos de seguridad reales y los requisitos de las normas de cumplimiento. Debe utilizar las políticas y prácticas de seguridad existentes, extendiéndolas a la nube y traduciéndolas al entorno de la nube. [22]

8. 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 este documento. Según esto, es necesario que este formato sea diligenciado por los responsables TI de la organización y anexe la documentación necesaria para probar que el 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).

Hay que aclarar que cualquier servicio de computación en la nube 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 de implementación. Por lo anterior, si se evita la falta de alguno de estos mediante el formato en cuestión, se entiende que dicho servicio está incompleto y necesita la implementación de soluciones que completen los requisitos para diagnosticarlo satisfactoriamente. 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 [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 porque, aunque sus actividades forman parte del modelo de referencia de NIST en una etapa avanzada y madura de la computación en la nube, tampoco se consideran modelos de servicio. En la ruta de definición e implementación de la computación en la nube en Colombia liderada por el Ministerio TIC, se considerarán las normas técnicas y las posibilidades tecnológicas

(incluyendo todos los actores y actividades, estándares, entre otros) de un entorno de alto nivel que aseguren la madurez esperada 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.

9. Lineamientos específicos para la gestión de seguridad en la nube

Para fortalecer la gestión de seguridad en servicios en la nube, se sugiere que las entidades públicas adopten los siguientes lineamientos alineados al control A.5.23 de la norma ISO/IEC 27001:2022:

- Definir controles de seguridad compartida con el proveedor, incluyendo las responsabilidades de cada parte (cliente y proveedor) mediante cláusulas contractuales explícitas.

- Solicitar evidencias técnicas o certificaciones (como ISO/IEC 27001:2022 o 27017) que permitan validar la madurez en seguridad del proveedor sin limitar la pluralidad de oferentes. En caso de no contar con la certificación, se aceptará documentación robusta de políticas y prácticas internas.

- Incluir en el contrato cláusulas sobre la notificación de incidentes, tiempos máximos de respuesta, canales oficiales y niveles de severidad.

- Realizar auditorías o revisiones periódicas al cumplimiento de los controles de seguridad aplicados por el proveedor, incluyendo los servicios en nube bajo el modelo SaaS, PaaS o IaaS.

- Establecer mecanismos de control para la residencia y ubicación de los datos, de forma que se garantice el cumplimiento normativo nacional e internacional sobre protección de datos.

- Implementar políticas para la clasificación de la información previa a su migración a la nube, que definan qué categorías de información pueden o no ser tratadas en entornos externos.

10. Implementación y monitoreo de controles de seguridad en servicios en la nube

Con base en el control A.5.23 de la norma ISO/IEC 27001:2022, las entidades públicas deben establecer una relación clara y controlada con sus proveedores de servicios en la nube, que permita garantizar la seguridad de la información procesada o almacenada en dichos entornos. Para ello, se deberán tener en cuenta las siguientes acciones:

Controles exigidos al proveedor

Definir en los contratos los controles mínimos de seguridad exigibles, tales como: cifrado de datos en tránsito y en reposo, autenticación multifactor, control de accesos privilegiados, trazabilidad, respaldo y recuperación, así como la ubicación geográfica de los datos.

Exigir la presentación de certificaciones vigentes (como ISO/IEC 27001, 27017 o 27018) o documentación equivalente que evidencie un sistema de gestión de seguridad de la información implementado.

Incluir cláusulas sobre la notificación obligatoria de incidentes de seguridad, con tiempos de respuesta establecidos y mecanismos de comunicación definidos.

En concordancia con las mejores prácticas definidas por la ISO/IEC 27017 y los controles de la norma ISO/IEC 27001:2022, toda cuenta con privilegios administrativos o acceso a servicios críticos en la nube deberá contar con mecanismos de autenticación multifactor (MFA). Este requisito aplica tanto a cuentas internas como a las utilizadas por proveedores o terceros autorizados.

Cada entidad definirá el mecanismo técnico más adecuado según sus condiciones, siempre que garantice la validación en dos o más factores independientes (algo que se sabe, algo que se tiene, algo que se es), sin restringir tecnologías o marcas específicas.

Acciones de monitoreo por parte de la entidad

Realizar revisiones periódicas (documentales o técnicas) sobre el cumplimiento de los controles contractuales establecidos.

Solicitar reportes de auditoría externa, resultados de pruebas de seguridad (pentesting o escaneo de vulnerabilidades), y evidencia de implementación de medidas correctivas.

Monitorear continuamente los niveles de servicio relacionados con la disponibilidad, integridad y confidencialidad de la información en la nube, conforme a los SLA definidos.

Establecer mecanismos internos de verificación de seguridad para los servicios cloud críticos, incluyendo herramientas de monitoreo de actividad y acceso.

Este enfoque permite a las entidades mantener el control sobre los riesgos inherentes al uso de servicios en la nube, asegurar el cumplimiento de sus políticas institucionales de seguridad y responder adecuadamente a incidentes, auditorías o requerimientos legales.

11. 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://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=909024 .

[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: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication500-292.pdf

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

[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 Digital (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

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

[19] Gartner. Gartner IT Glossary > Data Center [Online]. Disponible: https://www.gartner.com/it-glossary/data-center/

[20] Peter Mell. Computación en la Nube – Perspectiva de NIST. Semana de Gobierno Digital. 2017.

[21] Centro Europeo de Postgrados – Fundamentos de Seguridad Cloud e Infraestructuras Industriales. 2023.

[22] Articulo Cloud Governance**,** **https://www.imperva.com/learn/data-security/cloud-governance/**