
G DATA
TRUST IN
GERMAN
SICHERHEIT

Seguridad en la Nube

TRUST IN GERMAN SICHERHEIT

Ingeniero Javier. Asís
Especialista en Redes
Javier.asis@softnetcorp.net

DEFINICIÓN DE LA NUBE

La nube en la actualidad es lo mas utilizado en el día a día, es una metáfora empleada para hacer referencia al servicio que se utiliza a través de internet.

CARACTERÍSTICAS

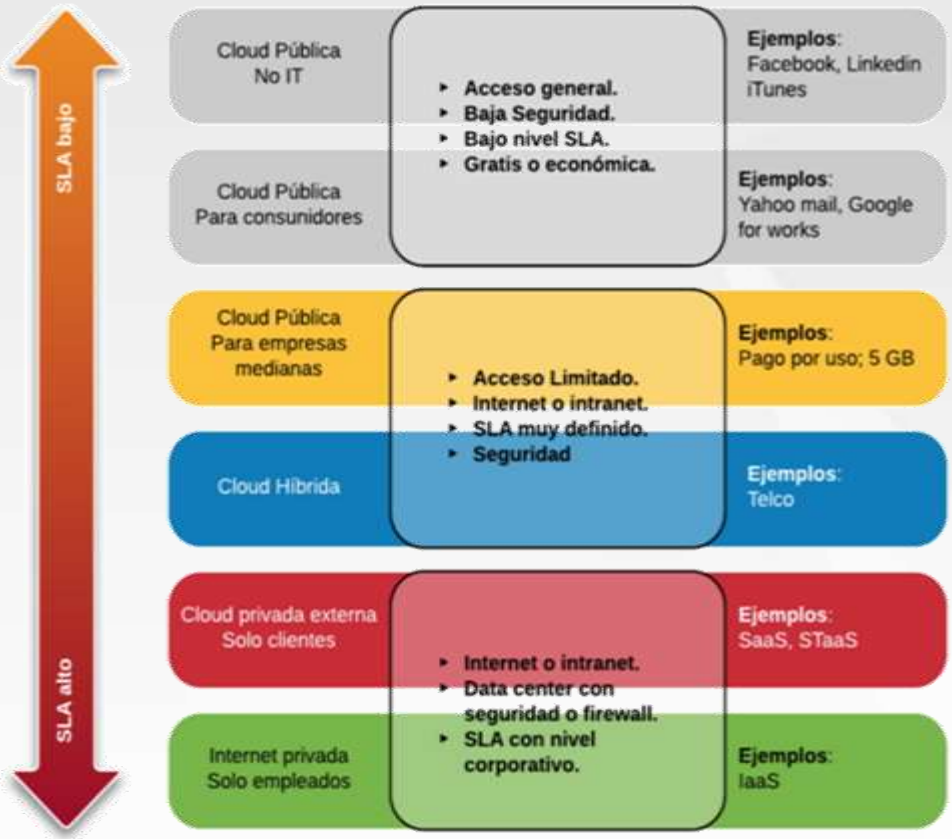
- Autoservicio Bajo demanda.
- Conjunto de recursos multicliente.
- Rapidez y elasticidad (flexibilidad, escabilidad).
- Servicio medido(pago por uso)
- Amplio acceso a la red ("cualquier momento, cualquier lugar, cualquier dispositivo).

Modelo de despliegue en la Nube

Nube privada (private cloud).– Infraestructura en la nube la cual atiende exclusivamente a una organización. Este modelo de nube puede ser administrada por un tercero o por la misma organización.

Nube pública (public cloud).– Infraestructura en la nube abierta al público en general, ya sea mediante una suscripción o de forma gratuita.

Nube híbrida (hybrid cloud).– infraestructura en la nube compuesta de una combinación de privada y pública.



Tipo de servicio de la Nube

Software como un Servicio: (del inglés: Software as a Service, **SaaS**) es un modelo de distribución de software donde el soporte lógico y los datos que maneja se alojan en servidores de una compañía de tecnologías de información y comunicación (TIC), a los que se accede vía Internet desde un cliente. Este modelo de servicio lo prestan aplicaciones web como GMail, Office 365, Dropbox o Google Docs.

Plataforma como Servicio (en inglés *platform as a service*, **PaaS**) En este modelo de servicio al usuario se le ofrece la plataforma de desarrollo y las herramientas de programación por lo que puede desarrollar aplicaciones propias y controlar la aplicación, pero no controla la infraestructura. Ejemplos comerciales son Google App Engine, que sirve aplicaciones de la Infraestructura Google; Microsoft Azure, una plataforma en la nube que permite el desarrollo y ejecución de aplicaciones codificadas en varios lenguajes y tecnología.

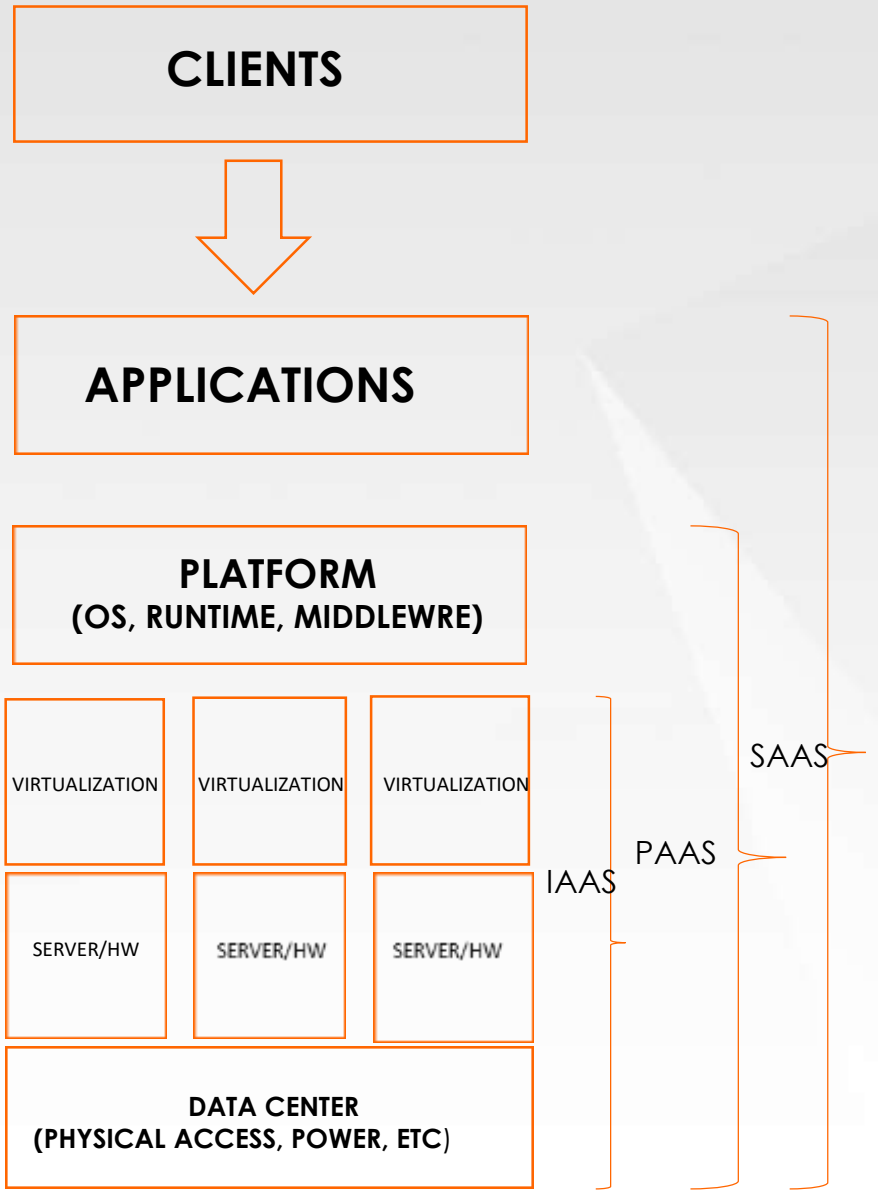
Infraestructura como servicio (*infrastructure as a service*, **IaaS**) -también llamada en algunos casos *hardware as a service*, HaaS) está orientado a administradores de sistemas. Con este modelo, el proveedor ofrece el acceso a recursos de cómputo y de almacenamiento mediante un modelo de pago por uso. El ejemplo comercial mejor conocido es Amazon Web Services, cuyos servicios EC2 y S3 ofrecen cómputo y servicios de almacenamiento esenciales.

Tipo de servicio de la Nube

Responsabilidades del proveedor del servicio de nube

Las responsabilidades del proveedor del servicio de nube se inician con la seguridad física y ambiental. Después de todo, el proveedor del servicio de la nube está operando un conjunto de centros de datos.

Las principales cosas que deberá buscar son el acceso físico de los empleados, la detección y supresión de incendios, la continuidad de la energía eléctrica, el control del clima y la temperatura para los servidores y otros dispositivos de hardware así como el saneamiento para los dispositivos de almacenamiento desmantelado.



Responsabilidades del cliente

- comprender y calificar el perfil del riesgo de las cargas de trabajo que intentan mover a la nube.

- considerar las responsabilidades de que sus controles técnicos cumplan con los requerimientos de seguridad, privacidad y de cumplimiento.

- Para cumplir con los requerimientos de seguridad, privacidad y cumplimiento, los clientes podrían emplear los controles técnicos que brindan a la nube o podrían consumir esos servicios desde la nube.

Ventajas de la informática en la nube:

- Es probable que los estándares de seguridad de datos sean más altos en el entorno de su proveedor que en su empresa, especialmente si el proveedor de la nube cuenta con las normas ISO y otros estándares clave de la industria.

- Posiblemente, su proveedor de la nube tenga mejores recursos físicos y financieros que usted, para contrarrestar las amenazas a la seguridad de los datos a las que se enfrenta su infraestructura.

- Sus datos aún estarán disponibles, incluso si pierde una laptop.

- Puede concentrar más recursos y esfuerzos hacia un aspecto más estratégico y trascendente, que tenga un impacto directo sobre los procesos de negocio de la organización, transfiriendo al proveedor la responsabilidad de la implementación, configuración y mantenimiento de la infraestructura necesaria para que se ejecute la aplicación.

desventajas de la informática en la nube:

- Sus datos estarán almacenados fuera de la red empresarial, y posiblemente en el exterior, lo que puede infringir las leyes y las normas de protección de datos.

- Falta de control sobre recursos. Al tener toda la infraestructura e incluso la aplicación corriendo sobre servidores que se encuentran en la nube, es decir, del lado del proveedor, el cliente carece por completo de control sobre los recursos e incluso sobre su información, una vez que ésta es subida a la nube.

- Dependencia. En una solución basada en cómputo en la nube, el cliente se vuelve dependiente no sólo del proveedor del servicio, sino también de su conexión a Internet, debido a que el usuario debe estar permanentemente conectado para poder alcanzar al sistema que se encuentra en la nube.

Estrategias de seguridad en la nube - Gartner

- **La Estrategia de seguridad en la nube no es diferente a una estrategia de seguridad actual.**

Lo único que cambia es el ambiente en donde estamos desarrollando la estrategia. Es importante identificar qué controles de seguridad diferentes a los tradicionales se deben implementar. Para esto, es necesario apegarse a las regulaciones existentes, revisar las modificaciones a las normas ISO, así como otros controles en diferentes instancias.

- **Establecer una estrategia de administración del cambio.**

Es importante ayudar a la gente del negocio a entender que, al irnos a la nube no estamos poniendo en riesgo nuestra información. Si bien es cierto que si existe un nivel de riesgo, este puede ser mitigado a través de la primera recomendación, que es la implementación de los controles.

- **Una estrategia de seguridad no son solo controles y políticas.**

Una estrategia de seguridad inicia con la contratación del servicio. Es necesario identificar los puntos que deben establecerse dentro de un contrato. ¿Cómo puedo hacer las auditorías? ¿Con qué periodicidad? ¿Dónde van a estar almacenados los datos? ¿Tengo acceso o no a las instalaciones? ¿Tienen los proveedores una certificación? Una estrategia es, precisamente, prepararnos para iniciar un camino.

- **Establecer un equipo de Cloud Computing.**

Este no es un equipo de tecnología. Es un equipo en que se integra gente de Legal y de recursos humanos, para que trabaje sobre temas regulatorios de acuerdo al país, que tome acciones en caso de algún fraude perpetrado por un empleado, verificar las leyes y normativa existente. El equipo deberá velar porque el proveedor cumpla todas estas normativas y regulaciones, y porque las transacciones se mantengan seguras al amparo de las mismas.

Aspectos a considerar

- Uno de los aspectos fundamentales cuando se vaya a tercerizar es velar por que realmente el proveedor haga las cosas como se deben de hacer desde el punto de vista de seguridad y privacidad.
- la seguridad de la nube es una responsabilidad compartida entre el proveedor del servicio de la nube y el cliente.
- Utiliza doble Autenticación, cuando vayas a estar en la red.
- Invierta en un software de seguridad que optimice el uso de una red de protección contra amenazas basada en la nube
- Cifre los datos siempre que sea posible para minimizar los riesgos asociados con la pérdida de datos usando contraseñas complejas, difíciles de adivinar y que por otro lado puedas recordar

Gdata y la seguridad en la Nube

Protección online:

- Contra Virus y gusanos que destruyen o roban sus archivos.
- Contra Programas espía, rootkits, troyanos y adware que toman el control de los clientes o incluso espían datos Personales.
- Protección contra keyloggers. En tiempo real e independiente de firmas de virus.

Incluye:

- PolicyManager para establecer las directrices de uso de Internet y uso del software dentro de la red de la empresa.
- Filtro de navegación para bloquear los sitios web que no pertenezcan al trabajo cotidiano.
- Copias de seguridad, tanto en dispositivos externos -discos duros o memorias USB- como en los servicios en la nube (tipo Dropbox o Google Drive) cifrando la información y protegiéndola con una contraseña.
- Integración de G DATA Managed Endpoint Security en la plataforma Azure de Microsoft

G DATA fue la primera empresa que consideró la computación en la nube para sus productos. En el **2005, Cloud Security,.**

Teléfono Master: (+58) 212.627.05.00 E-mail: info@softnetcorp.net Web Site: www.softnetcorp.net