Fundamentos de la nube

Las tecnologías basadas en la nube permiten a las organizaciones acceder a la informática, el almacenamiento, el software y los servidores a través de internet. Trasladó el componente tecnológico de la organización a un proveedor de nube como puede ser: AWS, Azure o Google Cloud.

Servicios de la nube

Software como servicio (SaaS)

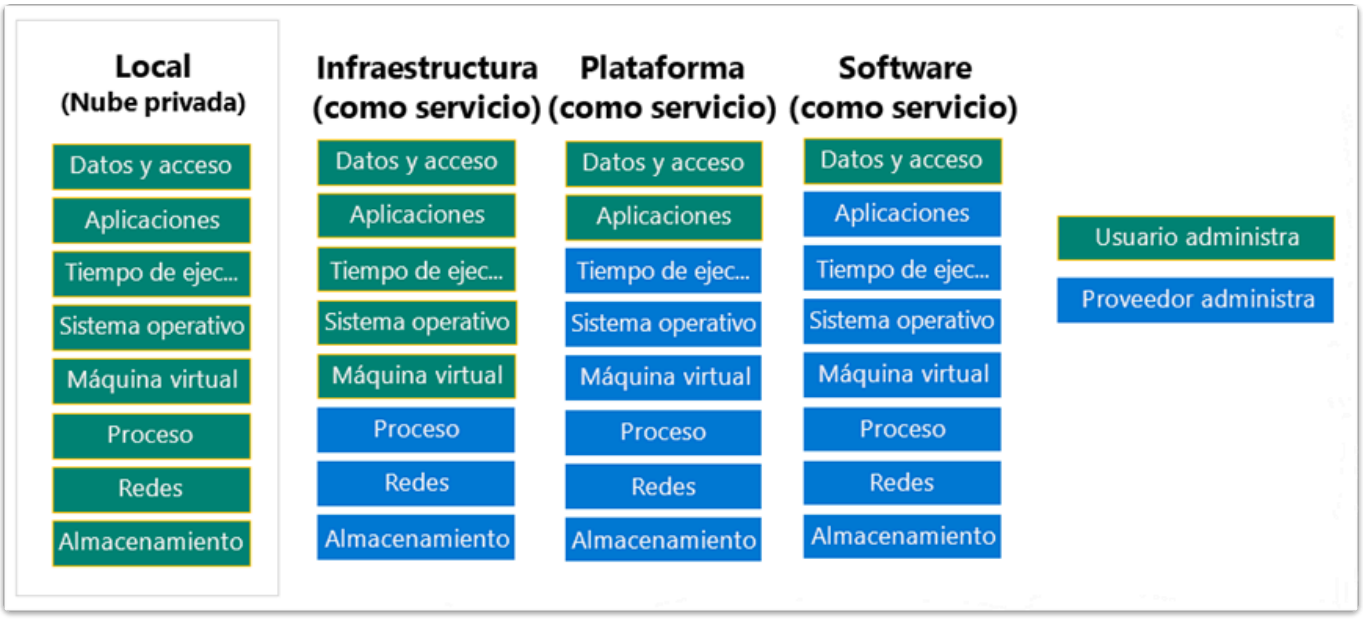
SaaS, permite a los usuarios acceder a las aplicaciones y bases de datos. Los proveedores de la nube administran la infraestructura mientras que los usuarios almacenan datos en los servidores del proveedor de la nube.
Ejemplo: Un usuario utiliza Google Workspace para acceder a Gmail, Google Drive y Google Docs sin la necesidad de instalar ningún software.

Plataforma como servicios (PaaS)

Permite a una organización acceder de forma remota a las herramientas y servicios de desarrollo utilizados para ofrecer dichas aplicaciones mediante una suscripción.
Ejemplo: Un desarrollador crea una aplicación en Heroku. No necesita preocuparse por configurar servidores ni bases de datos, ya que Heroku proporciona las herramientas y servicios necesarios para el desarrollo.

Infraestructura como servicio (IaaS)

Proporciona recursos informáticos virtualizados a través de Internet. El proveedor aloja el hardware, software y componentes de almacenamiento, el usuario paga por el uso de estos recursos, generalmente de forma flexible según demanda.
Ejemplo: Una empresa contrata instancias virtuales de AWS EC2 para alojar sus servidores. La empresa es responsable de instalar el S.O y las aplicaciones, mientras que AWS proporciona el hardware virtualizado.



Tipos de nube

La computación en la nube posee diferentes clasificaciones, las cuales se basan en el método de implementación de los modelos de servicio.

Nube privada

También conocida como nube interna, corporativa o empresarial, una nube privada está alojada en una plataforma privada. Esta le ofrece a la organización, más control sobre sus datos, pero puede ser más costosa que otros servicios de nube debido a los costos de infraestructura, mantenimiento y administración.
Ejemplo: Un banco utiliza su propia infraestructura para alojar sistemas críticos como bases de datos de clientes, garantizando el control total sobre los datos.

Nube pública

Está alojada por un proveedor de servicios en una instalación externa. Los usuarios pagan una suscripción de manera mensual o anual para poder acceder a sus servicios. Esta opción le cuesta a la organización menos infraestructura, mantenimiento y administración, sin embargo, la organización tiene menos control sobre sus datos.
Ejemplo: Una startup utiliza los servicios de Google Cloud para almacenar datos y ejecutar sus aplicaciones, reduciendo costos de infraestructura y mantenimiento.

Nube híbrida

Es una nube que combina tanto a la nube privada como la pública ofreciendo el control de los datos de la organización y combinando el control de datos de una nube privada con la escalabilidad de una nube pública.
Ejemplo: Una tienda en línea almacena información confidencial de clientes en su propia nube, pero usa Microsoft Azure para escalar durante promociones o temporadas de alta demanda.

Nube comunitaria

Es un esfuerzo de colaboración en el que más de una organización comparte y utiliza la misma plataforma. Este tipo de nube está dirigida a las necesidades de un sector como el de servicios de salud o energía.
Ejemplo: Varias universidades comparten una nube comunitaria para almacenar investigaciones científicas, optimizando recursos y garantizando acceso colaborativo

Principales amenazas

La computación en la nube es susceptible a recibir muchas amenazas que afectan a las redes físicas de cualquier empresa. Sin embargo, existen amenazas únicas, entre las cuales están:

Violación de datos

Esto ocurre cuando una entidad no autorizada accede a los datos confidenciales protegidos.

Configuración errónea de la nube

Ocurre cuando el recurso de la computación en la nube está configurado incorrectamente, haciéndolo vulnerable a ataques. Ejemplos comunes incluyen: permisos de almacenamiento abiertos, bases de datos expuestas sin cifrado y la falta de políticas adecuadas de control de acceso.

Estrategia deficiente de la arquitectura de seguridad en la nube

Ya que los distintos modelos de nube poseen diferentes responsables detrás de la seguridad de los sistemas, esto puede generar vulnerabilidades si la arquitectura de seguridad en la nube no se comprende completamente o se implementa de manera incorrecta.

Credenciales de cuentas compartidas

Ocurre cuando las cuentas de usuario o los privilegios de acceso no están bien protegidos y son secuestrados por los atacantes. Esto genera una importante amenaza a la seguridad si la cuenta tiene altos privilegios.

Amenaza interna

Se produce cuando un empleado, contratista o socio comercial pone en peligro el servicio en la nube de forma maliciosa o involuntaria.

Seguridad de la infraestructura en la nube

Políticas de seguridad de la compañía

Las políticas de seguridad establecidas y bien definidas por la empresa y la formación de los usuarios son formas eficaces de gestionar las aplicaciones desconocidas.

Microsegmentación

Aprovecha las topologías de red virtuales para ejecutar redes múltiples, más pequeñas y aisladas, sin incurrir en costos adicionales de hardware. Esta técnica permite un control más granular de la seguridad del tráfico y los flujos de trabajo dentro de la nube.

Seguridad en capas

Cada recurso en la nube se puede proteger en múltiples niveles, como por ejemplo:

- **Capa de hardware**: Uso de dispositivos seguros en los data centers.
- **Capa de infraestructura:** Configuración adecuada de redes virtuales, firewalls y VPNs.
- **Capa de plataforma:** Implementación de controles de acceso a servicios de base de datos y entornos de ejecución.
- **Capa de aplicación:** Uso de mecanismos como el control de versiones y pruebas de seguridad del software.

Seguridad de aplicaciones en la nube

Firma de código

Ayuda a demostrar que una pieza de software es auténtica. Los ejecutables diseñados para instalarse y ejecutarse en un dispositivo se firman digitalmente para validar la identidad del autor y garantiza que el código del software no ha cambiado desde que se firmó.

Cookies seguras

El uso de cookies seguras protege la información almacenada contra accesos no autorizados. Los desarrolladores web deberían de utilizar cookies con HTTPS para asegurar las cookies y evitar que se transmitan a través de HTTP sin cifrar.

Control de versiones

El control de versiones se utiliza para evitar cambios accidentales realizados por usuarios autorizados. Esto significa que 2 usuarios no pueden actualizar el mismo objeto, ya sea: archivos, registros de base de datos o una transacción, exactamente al mismo tiempo.

Seguridad de datos en la nube

Criptografía

La encriptación es el proceso de codificar los datos de modo que las personas no autorizadas no pueden leerlos fácilmente. Cuando los datos están sin cifrar, se denominan texto plano; la versión cifrada es el texto cifrado o ciphertext.
Existen 2 clases de cifrado:

- **Algoritmos de cifrado simétricos**: Utilizan la misma clave precompartida para cifrar y descifrar datos. Tienen un tamaño de bloque fijo de 128 bits con un tamaño de clave de 128, 192 o 256 bits.

- **Algoritmo de cifrado asimétrico**: Utiliza una clave para el cifrado que es diferente de la clave utilizada para descifrar. Este algoritmo incluye Rivest-Shamir-Adleman (RSA), Diffie-Hellman, ElGamal y la criptografía de curva elíptica (ECC).

Hashing

Hash es una herramienta que garantiza la integridad de los datos tomando datos binarios y produciendo una representación de longitud fija llamada valor hash. Estas funciones son funciones unidireccionales utilizadas para verificar y garantizar la integridad de los datos. Una herramienta de este tipo también puede verificar la autenticación.
Las funciones de hash criptográfica tienen las siguientes propiedades:

- La entrada puede ser de cualquier longitud.
- La salida tiene una longitud fija.
- La función de hash es unidireccional y es irreversible.
- Dos valores de entrada diferentes casi nunca darán como resultado el mismo hash.
  Hash se compone de la familia SHA:
- SHA-224 (224 bits)
- SHA-256 (256 bits)
- SHA-384 (384 bits)
- SHA-512 (512 bits)

Implementación de cifrado en la nube

- **En tránsito**: Uso de TLS 1.2 o 1.3 para asegurar la comunicación entre cliente y servidor.
- **En reposo**: Cifrado automático de bases de datos y almacenamiento mediante claves administradas por el proveedor de nube.
- **En uso**: Técnicas emergentes como el cifrado homomórfico (Realiza cálculos directamente sobre datos cifrados sin la necesidad de descifrarlos, lo que asegura la privacidad de la información incluso mientras está siendo procesada. Aunque ofrece un potencial significativo para proteger datos sensibles, su implementación todavía enfrenta desafíos relacionados con el rendimiento.) para proteger datos durante el procesamiento