UNIVERSIDAD FRANSCISO GAVIDIA

Facultad de Ingeniería y Sistemas

Trabajo de Investigación

Seguridad en la Nube

Asignatura: *Estructura de Datos*

Grupo clase: *V01*

Catedrático: *Ing. Wilfredo Alemán*

Alumno:

Carné	***Apellidos***	***Nombres***
AR100816	*Alfaro Reales*	*David Alejandro*

San Salvador, 7 de noviembre del 2021.

TABLA DE CONTENIDO

PROPÓSITO

Hoy en día, muchas empresas están optando por proveedores en la nube, donde puedan alojar archivos clasificados, datos de clientes, aplicaciones, servicios, etc. Migrar a la nube se ha convertido la solución tanto para evitar problemas causados por el error humano, como para aprovechar la oportunidad de escalabilidad que brinda.

Sin embargo, a pesar de los muchos beneficios que tener todo alojado en la nube pueda traer, también hay que considerar los riesgos que se corren si no se toman las medidas necesarias para proteger la información.

El propósito de este trabajo es explorar más en esta área, para poder entender claramente qué es la seguridad en la nube y sus beneficios y riesgos.

RESULTADOS

Es un término muy amplio que abarca la tecnología y las prácticas recomendadas para proteger los datos y la información importante dentro de una arquitectura de nube. En pocas palabras, son controles, normas, tecnologías y procedimientos que se utilizan para proteger los datos de clientes y de la misma empresa.

La seguridad en la nube es toda la tecnología, los protocolos y las buenas prácticas que protegen los entornos informáticos en la nube, las aplicaciones que se ejecutan en la nube y los datos almacenados en ella. La seguridad de los servicios en la nube comienza por comprender qué se está asegurando exactamente, así como los aspectos del sistema que se deben administrar.

Este tipo de seguridad está diseñada para proteger las siguientes áreas:

- Redes físicas.
- Servidores de datos.
- Sistemas Operativos.
- Middlewares.
- Datos.
- Aplicaciones.
- Hardware de usuario final.
- Almacenamiento de datos.

Para poder entender un poco sobre la seguridad en la nube, primero es importante conocer los diferentes tipos de servicios que existen:

- **Infrastructure as a Service (IaaS):** permite que una empresa construya su propio data center virtual.
- **Platform as a Service (PaaS):** permite que el cliente despliegue o cree software.
- **Software as a Service (SaaS):** permite que el cliente tenga el uso del software sin la necesidad de una computadora o servidor donde construirlo.

Ahora bien, existen 4 entornos que sirven como modelos de implementación en los que uno o más servicios en la nube crean un sistema para los usuarios finales o empresas. Estos son:

- Entornos de nubes públicas, en los que un cliente comparte los servidores de un proveedor con otros clientes, como un edificio de oficinas o un espacio de trabajo.
- Entornos de nubes privadas, tipo de servicio que proporciona al cliente el uso exclusivo de su propia nube.
- Entorno de varias nubes, que incluyen el uso de dos o más servicios en la nube de proveedores independientes.
- Entorno de nubes híbridas, una combinación de nube privada de terceros o centro de datos de nubes privadas con una o más nubes públicas.

Las medidas de seguridad que se toman en la nube tienen objetivos claros como permitir la recuperación de datos en caso de pérdida de los mismos, proteger el almacenamiento y las redes contra el robo de datos malicioso, reducir el impacto de cualquier compromiso de datos y evitar los errores humanos que causan la fuga de datos.

¿Por qué usar medidas de seguridad?

Una de las principales razones es que tienen **menores costos por adelantado.** Las empresas pagan menos por la seguridad en la nube que por la seguridad en sus instalaciones. Otras razones son porque tiene **mayor escalabilidad** y **menos tiempo de llegada al mercado**, las aplicaciones o sistemas en la nube pueden ampliarse rápidamente. Igualmente, al usar un proveedor en la nube, las empresas pueden pagar por la seguridad que efectivamente utilicen, **lo que resulta en menores costos permanentes.**

A pesar de mencionar solo cosas positivas de tener un proveedor en la nube donde podamos alojar nuestra información vital, también existen riesgos que se puedan presentar, como:

- Riesgos de la infraestructura basada en la nube.
- Amenazas internas debido a errores humanos.
- Amenazas externas causas por actores maliciosos como malwares, phishing y ataques de DDoS.

REFERENCIAS

- Kaspersky. (2021, 16 marzo). ¿Qué es la seguridad en la nube? www.kaspersky.es. https://www.kaspersky.es/resource-center/definitions/what-is-cloud-security

- ¿Qué es la seguridad en la nube? (2020). Rackspace Technology. https://www.rackspace.com/es/library/what-is-cloud-security

- CyberArk Software. (2020, 28 abril). ¿Qué es la seguridad en la nube y cómo se puede proteger la nube con PAM? CyberArk. https://www.cyberark.com/es/what-is/cloud-security/

- VMWare (2021, 6 abril). ¿Qué es la seguridad de la nube? WMWare. https://www.vmware.com/latam/topics/glossary/content/cloud-security.html