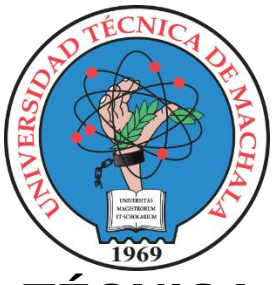

UNIVERSIDAD TÉCNICA DE MACHALA

Maestría en Software

Asignatura:

Gestión de la seguridad del software

Tema:

Caracterizar la situación de la seguridad informática y marco legal de esta en computación en la nube

Docente: Ing. Félix Oscar Fernández Peña

Estudiantes:
Ing. Fernando Castillo
Ing. Carlos Quezada
Ing. Esteban Gonzabay
Ing. Jorge Miranda
Ing. Leonardo Caraguay

2021-2022

Contenido

Situación de la seguridad informática en computación en la nube

La seguridad en la nube es similar a la seguridad de los centros de datos en las instalaciones, solo que sin los costos de mantener instalaciones y hardware. En la nube, no hay que administrar servidores físicos ni dispositivos de almacenamiento. En la nube se usan herramientas de seguridad basadas en software para monitorizar y proteger el flujo de información que entra y sale de los recursos en la nube. Por este motivo, la seguridad en la nube es una responsabilidad compartida entre el cliente y la plataforma nube (Google, AWS etc) (AWS, 2021) .

Ejemplo de modelo de seguridad compartida

Figura 1: Modelo de responsabilidad compartida de AWS

Amenazas de seguridad en la computación en la nube

La Cloud Security Alliance identifica 12 amenazas relacionadas con la seguridad en la nube. Se clasifican de acuerdo al orden de gravedad:

- Incumplimiento de datos.
- Identidad, credencial y gestión de acceso débiles.
- APIs inseguras.
- Vulnerabilidades de sistema y aplicación.
- Secuestro de cuenta.
- Inicio de sesión malintencionado.
- Amenazas persistentes avanzadas.
- Pérdida de datos.
- Evaluación Insuficiente.
- Abuso de los servicios en la nube.
- Denegación de Servicio.
- Vulnerabilidades de tecnología compartida.

Responsabilidades

Un análisis detallado sobre la seguridad de los datos y los controles de privacidad provistos en la nube por destacados proveedores de servicios, revela la siguiente matriz de diferentes tipos de controles de seguridad. Esto tendría que implementarse en los diferentes modelos de servicios en la nube (Amazon, Microsoft, IBM, Techtalk).

Asignación de la responsabilidad de los requisitos de privacidad y seguridad de datos al modelo de servicio en la nube

Responsabilidad	On Premise	SaaS		Paas		Iaas	
Gobierno de datos	C		C		C		C
Protección de puntos finales	C		C		C		C
Gestión de acceso a usuarios	C		C		C		C
Identidad	C		C		C		C
Aplicación	C	CSP		CSP			C
Control de red	C	CSP		CSP			C
Seguridad de sistema operativo	C	CSP		CSP			C
Host	C	CSP		CSP		CSP	
Red	C	CSP		CSP		CSP	
Data Center	C	CSP		CSP		CSP	

C= Cliente / CSP= Proveedor de servicios cloud

Figura 2: Asignación de responsabilidades según Cloud Security Alliance

Marco legal en computación en la nube

Los objetivos de seguridad incluyen tanto aspectos más técnicos como otros más relacionados con el gobierno de seguridad de la información; entre estos últimos se pueden destacar las políticas de seguridad, la organización y gestión de la seguridad, la gestión de activos, la gestión de incidencias y continuidad del negocio, y el cumplimientos de normas y legislación vigente.

ISO/IEC 27002

El estándar ISO/IEC 27002 constituye una valiosa referencia para asegurar que se están defendiendo medidas de seguridad para todos los ámbitos existentes, y que no se deja ningún tema sin abordar. Por ello, generalmente las organizaciones optan por usar ambos estándares conjuntamente dada su integración.
Dentro de la familia de estándares, la ISO ha publicado el estándar ISO/IEC 27014 (ISO/IEC 2013) con el objeto de abordar específicamente el ámbito del gobierno de seguridad de la información. Este estándar está desarrollado para garantizar eficiencia, eficacia, agilidad y visibilidad del gobierno de seguridad, de forma que se propicie un

alineamiento entre la seguridad y las estrategias y objetivos de negocio. Para lograr su cometido, la norma se basa en seis principios de gobierno de seguridad, entre los que se encuentra el extender la seguridad de la información a toda la organización o el adoptar una postura basada en riesgos.

CSA

CLOUD SECURITY ALLIANCE 2011B, entre las recomendaciones para llevar un buen sistema de servicio cloud, menciona que:

- Para que las organizaciones puedan continuar midiendo y comunicando su conformidad con regulaciones y estándares, se requiere una adaptación de los procesos y prácticas de auditoría existentes. Este tipo de servicios permite delegar los esfuerzos de conformidad en el proveedor, y que se ofrezcan soluciones conjuntas que garanticen esta conformidad de forma contractual sin que el cliente deba preocuparse por ello. Sin embargo, la responsabilidad del servicio sigue estando en el lado del cliente, por lo que este debe poder realizar auditorías que justifiquen la conformidad del servicio.
- Los métodos tradicionales de gestión de la información deben adaptarse en la transición a arquitecturas Cloud Computing. Puesto que la información en este nuevo escenario muchas veces sale fuera de los controles de la organización propietaria, surge el desafío de su gestión y seguridad mediante nuevas estrategias. La guía recomienda definir un ciclo de vida de la seguridad de la información, soportado por herramientas de encriptación y monitorización. Ello requiere un adecuado gobierno de la información, de forma que se desarrollen políticas para su gestión, clasificación, autorización y control de responsabilidades.
- En aplicaciones tradicionales, donde todo es almacenado en un centro de datos controlado por la organización, normalmente solo se cifran los contenidos que así lo requieren disposiciones legales. Sin embargo, en los entornos Cloud Computing donde la organización puede no confiar plenamente en el proveedor que aloja sus datos, parece más necesaria la implementación de soluciones de cifrado de forma genérica. Eso añade complejidad en la gestión de estos datos, y requiere el establecimiento de procedimientos de gestión de claves para su adecuada custodia.

Bibliografía

AWS. (2021). *Seguridad en la nube.* Recuperado el 2021, de https://aws.amazon.com/es/security/security-learning/?whitepapers-main.sort-by=item.additionalFields.sortDate&whitepapers-main.sort-order=desc&awsf.whitepapers-content-type=*all