Ciberseguridad

Grado en Ingeniería Informática

M6 - Seguridad en Entornos Cloud e IoT

Oscar Delgado
oscar.delgado@uam.es

Álvaro Ortigosa (Coord.)
alvaro.ortigosa@uam.es

UAM Universidad Autónoma de Madrid

Contenido

Seguridad en Entornos Cloud

Contexto

Existe una tendencia cada vez mayor en muchas organizaciones a mover todas las operaciones de T.I. (o una parte grande de ellas) al **entorno cloud**.

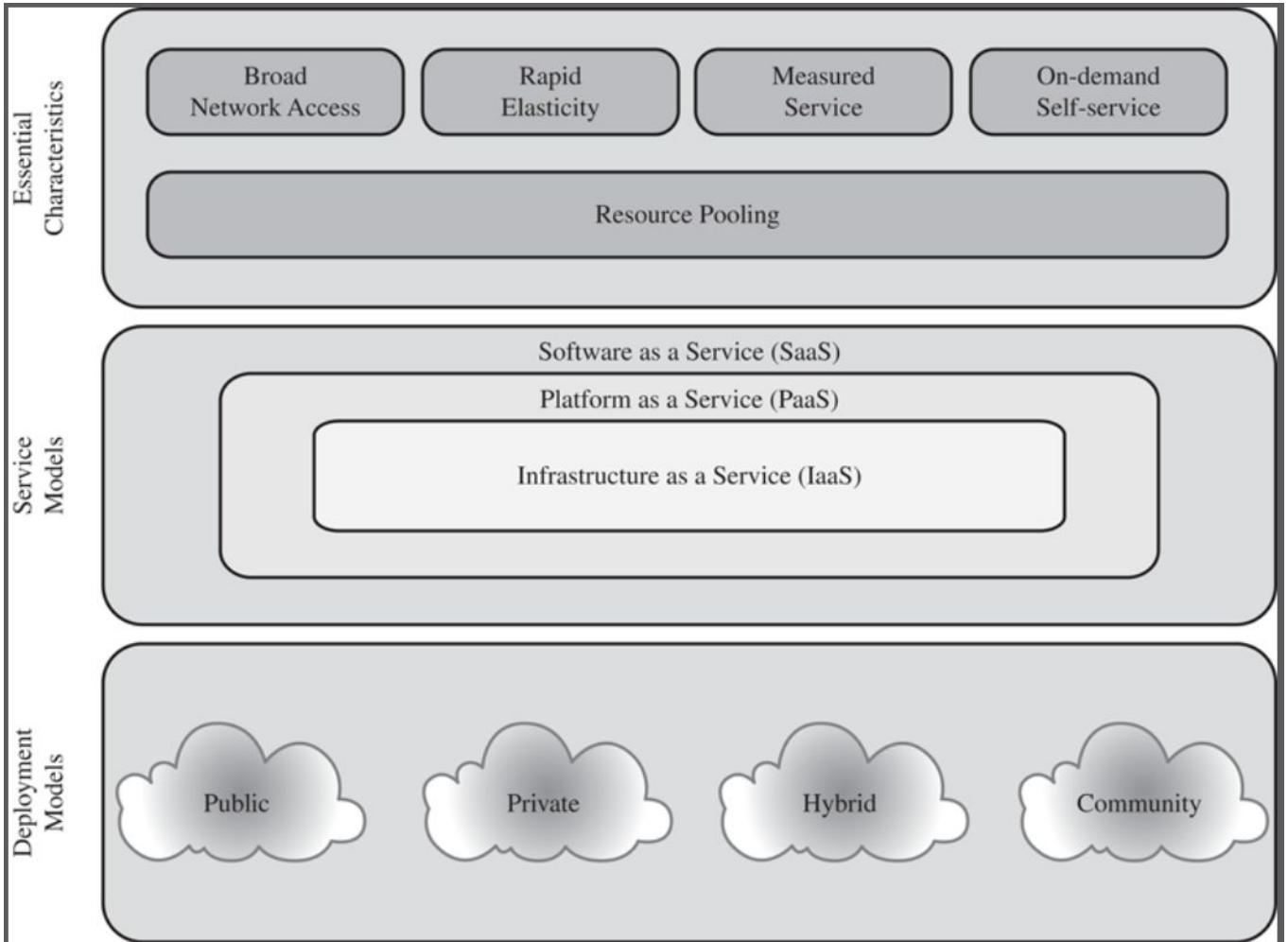
Entorno cloud: infraestructura conectada a Internet → **enterprise cloud computing**.

Definición

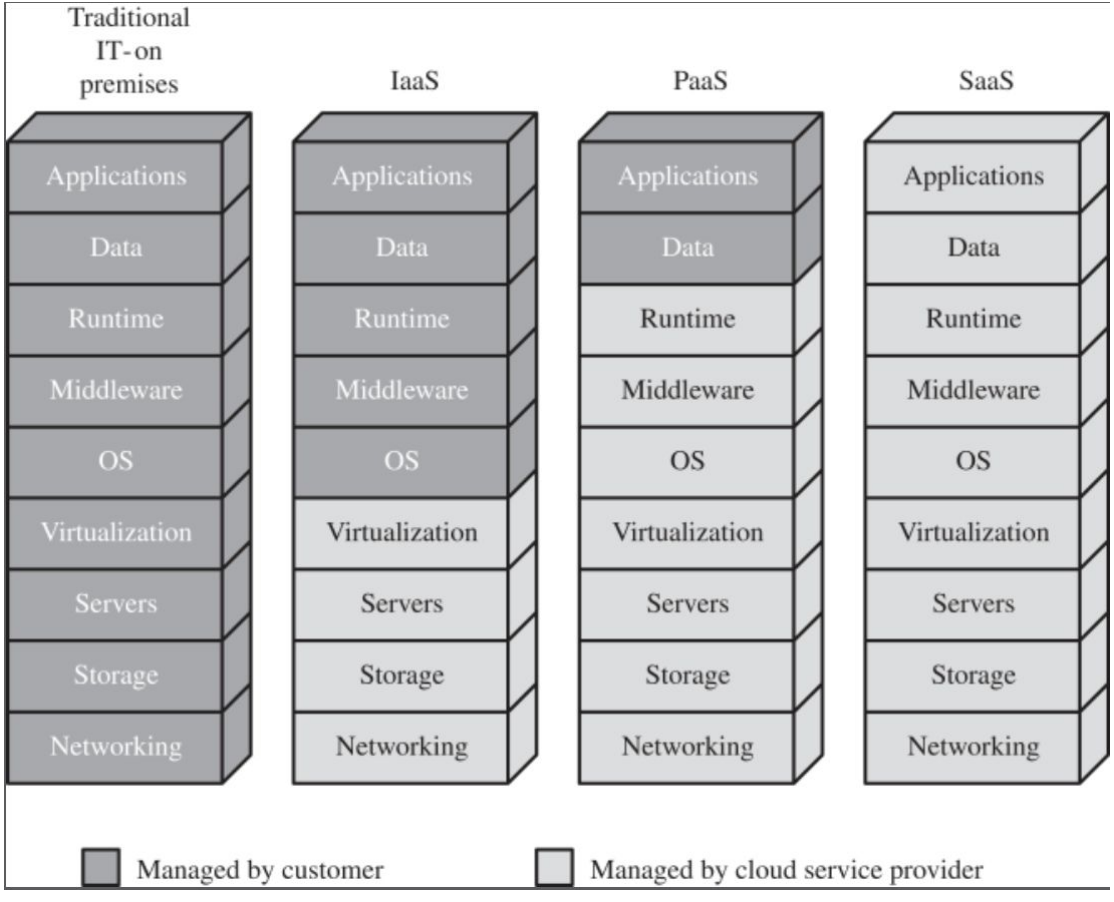
El National Institute of Standards and Technology (NIST) define cloud computing como:

“Un modelo para permitir un acceso ubicuo, conveniente, bajo demanda, a través de Internet, a un conjunto compartido de recursos computacionales configurables (por ejemplo servidores, almacenamiento, aplicaciones y servicios) que puedan ser rápidamente puestos a disposición con mínimo esfuerzo de gestión y mínima interacción con el proveedor de los servicios.”

Definición


Essential Characteristics
Broad Network Access
Rapid Elasticity
Measured Service
On-demand Self-service
Resource Pooling
Service Models
Software as a Service (SaaS)
Platform as a Service (PaaS)
Infrastructure as a Service (IaaS)
Deployment Models
Public
Private
Hybrid
Community

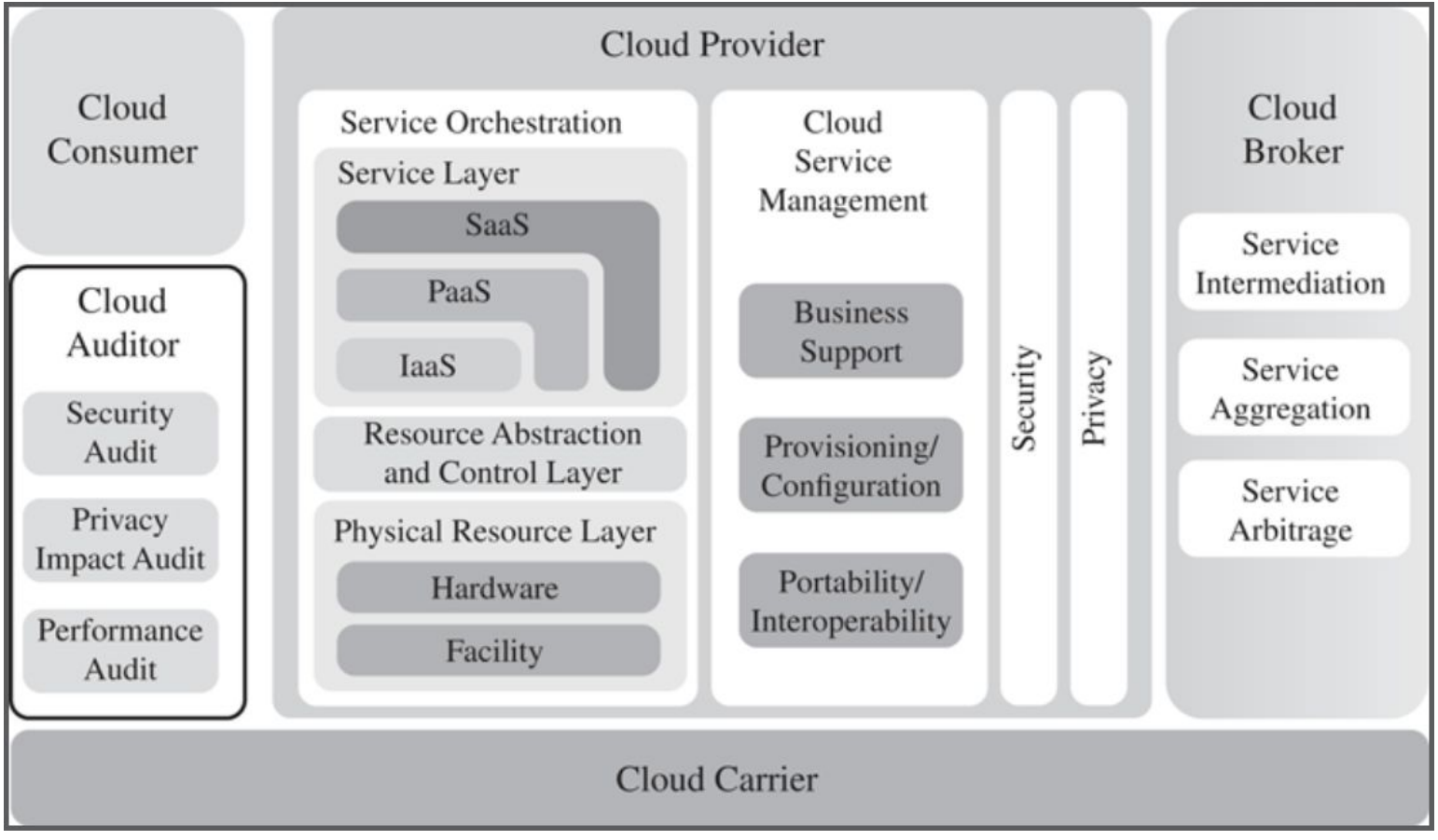
Definición


Traditional IT-on premises
IaaS
PaaS
SaaS
Applications
Data
Runtime
Middleware
OS
Virtualization
Servers
Storage
Networking
Managed by customer
Managed by cloud service provider

Comparación de los modelos de despliegue

	Private	Commu-nity	Public	Hybrid
Scalability	Limited	Limited	Very high	Very high
Security	Most secure option	Very secure	Moderately secure	Very secure
Perfor-mance	Very good	Very good	Low to medium	Good
Reliability	Very high	Very high	Medium	Medium to high
Cost	High	Medium	Low	Medium

Arquitectura de referencia del NIST



Actores principales (de servicios Cloud)

- **Consumidor**: una persona u organización que mantiene una relación de negocios con, y usa servicio de, un proveedor Cloud.
- **Proveedor**: una persona, organización o entidad responsable por prestar el servicio a los interesados.

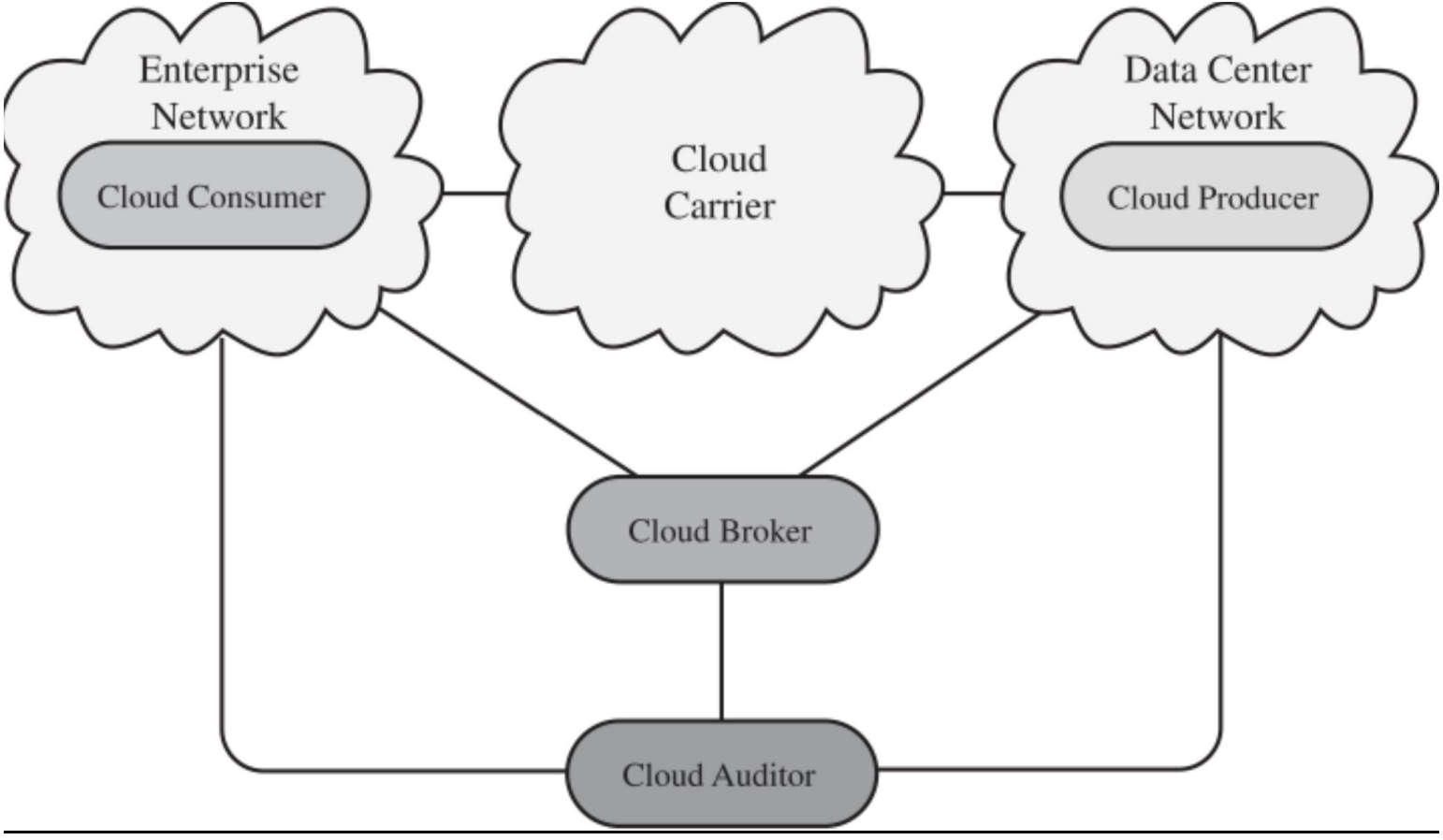
Actores principales (II)

- **Auditor**: un actor que puede llevar a cabo una evaluación independiente de los servicios cloud, rendimiento y seguridad de las implementaciones.
- **Corredor** (broker): entidad que gestiona el uso, rendimiento y entrega (delivery) de servicios cloud, y negocia relaciones entre los CSP y los consumidores.

Actores principales (III)

- **Transportista** (carrier): intermediario que provee conectividad y transporte de los servicios cloud desde el CSP a los consumidores.

Actores principales y sus interacciones



Conceptos de Seguridad Cloud

Gobernanza

- **Extender** las **prácticas** de la organización respecto de las políticas, procedimientos y estándares para el desarrollo de aplicaciones y suministro de servicios en la nube.
- Lo mismo se aplica al diseño, implementación, prueba, uso y monitorización de servicios desplegados o comprometidos.
- Poner en marcha mecanismos y herramientas de **auditoría**

Conformidad (Compliance)

- **Entender** las **leyes y reglamentos** que imponen obligaciones de seguridad y privacidad en las organizaciones.
- **Entender** el **impacto potencial** en las iniciativas cloud:
  - Localización de los datos
  - Controles de privacidad y seguridad
  - Gestión de registros
  - Requisitos de e-discovery

Conformidad (Compliance) II

- **Revisar** y **evaluar** las ofertas Cloud (y los términos de los contratos) con respecto a los **requisitos** que la organización **debe cumplir**.
- **Asegurar** que los procesos y capacidades de e-discovery del proveedor cloud **no comprometen** la privacidad y seguridad de los datos y las aplicaciones.

Confianza

- **Asegurar** la **visibilidad** de los controles y procesos de seguridad y privacidad del proveedor cloud, y su desempeño en el tiempo.
- **Establecer** claramente los **derechos de propiedad** sobre los datos.
- **Establecer** un programa de gestión de riesgos **flexible**.
- **Monitorización** continua

Arquitectura

- **Entender** la tecnología subyacente.
- El **impacto** de las técnicas de control sobre:
  - Seguridad y privacidad del sistema.
  - Ciclo de vida del sistema completo.
  - Todas las componentes del sistema.

Gestión de Identidad y Acceso

- **Asegurar** que las medidas de seguridad adecuadas están en marcha para asegurar:
  - Autenticación.
  - Autorización.
  - Otras funciones de gestión de identidad y acceso.
- **Comprobar** su **adecuación** a la organización.

Aislamiento del Software

- **Entender** la **virtualización** y otras técnicas de aislamiento lógico.
- **Evaluar** los **riesgos** implicados para la organización.

Protección de datos

- **Evaluar**:
  - La adecuación de las soluciones de gestión de datos del proveedor a los datos de la organización.
  - Capacidad de controlar accesos a los datos.
  - Capacidad de asegurar los datos en uso, en tránsito y "*at rest*".
  - Capacidad de desinfectar (sanitizar) los datos.

Protección de datos II

- **Tomar en consideración** el riesgo de “juntar” los datos propios con los de otras organizaciones:
  - ¿Son **altos** sus **perfiles de amenazas**?
  - Los datos representan, **colectivamente**, un valor concentrado significativo?
- **Entender** y **sopesar** los **riesgos de la gestión de claves** criptográficas ofrecida por el proveedor.

Disponibilidad

- **Entender** los términos del contrato para:
  - Disponibilidad;
  - Backup y recuperación de datos;
  - Recuperación ante desastres.
- **Asegurar** que satisfagan los **planes de contingencia** y continuidad de la organización:
  - En caso de corte prolongado o desastre las operaciones críticas pueden reiniciarse inmediatamente, y el resto de las operaciones lo hagan a tiempo y organizadamente.

Respuesta a Incidentes

- **Entender** los términos del contrato y procedimientos para la respuesta a incidentes, y asegurar que satisfacen los requisitos de la organización.
- **Asegurar** que el proveedor:
  - Tiene implementando un mecanismo de **respuesta transparente**.
  - Tiene mecanismos suficientes para **compartir información** durante y después del incidente.

Respuesta a Incidentes II

- **Asegurar** que la organización puede responder a incidentes de **forma coordinada** con el proveedor.
  - De acuerdo con sus respectivos roles y responsabilidades para el modelo adoptado.

Cuestiones de seguridad

Cuestiones a considerar

- La **seguridad** debe ser una de las **principales consideraciones** al evaluar una migración de on-premise a un servicio cloud.
- Aliviar las preocupaciones al respecto suele ser uno de los requisitos previos para considerar la migración.
  - **Disponibilidad** suele ser la otra preocupación básica.
- En la práctica, sólo suele ser una preocupación cuando se trata de sistemas "*mission critical*". Sistemas como e-mail y pago de nóminas parecen preocupar menos, a pesar de tener datos sensibles.

Cuestiones a considerar II

- La **auditabilidad** también puede ser importante en algunos contextos, dependiendo de la regulación:
  - Infraestructuras críticas.
  - Sistemas con datos de salud.
- La regulación suele ser la misma independientemente de la ubicación de los datos.

Cuestiones a considerar: división de responsabilidades

- La seguridad a nivel aplicación es responsabilidad del usuario.
- Los proveedores son responsables de la seguridad física y algunas cuestiones de software, como las políticas implementadas por los firewalls.
- La responsabilidad por los niveles intermedios es compartida.
  - Puede haber 3ras partes en las que el usuario confíe parte de las medidas de seguridad.

Cuestiones a considerar: compartición de recursos

- Los recursos del proveedor son compartidos con otros usuarios.
- Los usuarios deben ser protegidos unos de los otros:
  - Robo de datos, ataques DOS.
- Virtualización suele ser la respuesta. Pero:
  - No todos los recursos estarán virtualizados.
  - La virtualización puede tener errores.

Cuestiones a considerar: Protección contra el proveedor

- Por ejemplo, ¿qué pasa en caso de pérdidas de datos (inadvertidas)?
  - El proveedor mejora infraestructuras, cambia discos… ¿qué pasa con los discos viejos?
- Errores que permisos que hagan los datos visibles a partes no autorizadas.
  - El usuario puede ser cifrado de datos, pero el proveedor debe proveer sus propios mecanismos.

Tratamiento de las preocupaciones de seguridad

Recomendaciones de seguridad

- Aunque las cuestiones de seguridad pueden variar con el modelo adoptado (SaaS, IaaS, PaaS), múltiples recomendaciones son generales.
- Por ejemplo NIST recomienda proveedores que:
  - Ofrezca cifrado fuerte.
  - Implementados mecanismos de redundancia.
  - Implementados mecanismos de autenticación.
  - Ofrezca visibilidad sobre los mecanismos de protección de unos usuarios de otros, y del propio proveedor

Funciones y clases de control

Technical	Operational	Management
Access Control	Awareness and Training	Certification, Accreditation and Security Assessment
Audit and Accountability	Configuration and Management	Planning Risk Assessment
Identification and Authentication	Contingency Planning	System and Services Acquisition
System and Communication Protection	Incident Response	
	Maintenance	
	Media Protection	
	Physical and Environmental Protection	
	Personnel Security System and Information Integrity	

Enfoques de seguridad Cloud

Riesgos y contramedidas

- La idea esencial es que aunque la organización pierde control sobre recursos, servicios y aplicaciones…
- … debe mantener responsabilidad por las políticas de seguridad y privacidad.
- La Alianza para la Seguridad en la Nube (Cloud Security Alliance - CSA) lista las siguientes amenazas específicas:

Abuso y uso malintencionado

- Muchos CSPs facilitan el registro y uso inicial de sus servicios, incluso ofreciendo demos gratuitas.
- Esto facilita que los delincuentes usen el servicio cloud para realizar ataques:
  - Spamming;
  - Código malicioso;
  - DOS.
- Tradicionalmente riesgo para proveedores de PaaS, ahora también lo es para proveedores de IaaS.

Abuso y uso malintencionado II

- La carga principal de proteger contra estos ataques es del CSP, pero los usuarios tb deben monitorizar la actividad sobre sus datos y recursos.
- Contramedidas:
  - Procesos de registro y validación más estrictos.
  - Mejora en la monitorización y coordinación de fraudes con tarjetas bancarias.
  - Inspección exhaustiva del tráfico de red de los clientes.
  - Monitorización de listas negras públicas (por si la red propia está bloqueada)

Interfaces y APIs inseguras

- La disponibilidad y seguridad de los servicios cloud dependen de la seguridad de las APIs básicas.
- Deben estar diseñadas para proteger contra intentos de evasión de las políticas de seguridad.
- Contramedidas:
  - Análisis del modelo de seguridad de las interfaces.
  - Asegurar que se implemente autenticación y control de acceso seguros, así como transmisión cifrada.
  - Comprensión de la cadena de dependencias de las APIs.

Insider malicioso

- Con este paradigma la organización cede el control directo sobre muchos aspectos de seguridad.
- Confiere niveles de confianza sin precedentes al CSP.
- Una preocupación grave es el riesgo de insiders.
- Hay roles necesarios pero peligrosos:
  - Administrador de sistemas.
  - Proveedor de servicio de seguridad gestionada.

Insider malicioso II

- Contramedidas:
  - Forzar una gestión estricta de la cadena de suministros y evaluación profunda de los proveedores;
  - Especificar requisitos de los recursos humanos en el contrato.
  - Exigir transparencia sobre la información de seguridad y prácticas de gestión, así como informes de cumplimiento.
  - Determinar el proceso de notificación de brechas de seguridad.

Riesgos por tecnología compartida

- A veces los componentes subyacentes de la infraestructura compartida no están diseñados para proveer un aislamiento seguro (caché de CPU, GPUs, etc.)
- La solución típica es el uso de VM, pero enfoque también tiene vulnerabilidades, y debe ser solo una parte de la estrategia global de seguridad

Riesgos por tecnología compartida II

- Contramedidas:
  - Implementación de “mejores prácticas” para instalación/configuración.
  - Monitorización de cambios/actividades no autorizadas.
  - Promover el uso de autenticación y control de accesos fuertes para accesos y operaciones administrativas.
  - Forzar SLAs para actualización y reparación de vulnerabilidades.
  - Llevar a cabo monitorización de vulnerabilidades y auditorías de configuración.

Pérdida o escape (*leakage*) de datos

- Para algunos clientes es el mayor riesgo.
- Contramedidas:
  - Implementar control fuerte de acceso a la API.
  - Cifrar y proteger la integridad de los datos, en tránsito o en reposo.
  - Analizar la protección de datos tanto en tiempo de diseño como de ejecución.
  - Implementar creación, almacenamiento y gestión fuerte de claves, así como prácticas de destrucción.

Secuestro (hijacking) de cuenta/servicio

- Una de las principales amenazas.
- A veces se usan credenciales robadas.
  - En este caso pueden acceder a áreas críticas de los servicios cloud desplegados, permitiendo comprometer los principios CIA.
- Contramedidas:
  - Prohibir compartir credenciales (entre usuarios y servicios).
  - Utilizar técnicas fuertes de 2 factores.
  - Monitorización proactiva de actividad no autorizada.
  - Entender la política y SLA de seguridad del CSP.

Protección de datos en Cloud

Riesgos para los datos

- Los datos se pueden comprometer de muchas formas:
  - Borrado o alteración de registros sin copia de respaldo.
  - Desvinculación de un registro del contexto general lo dejaría inutilizable.
  - Pérdida de una clave de codificación.
  - Acceso a los datos de actores no autorizados.
- La amenaza a los datos se incrementa en el entorno Cloud.

  Riesgos y desafíos:
  - únicos del entorno cloud.
  - más peligrosos por sus características.

Seguridad en Bases de Datos

- Pueden variar mucho de una a otra.
- Modelo multi-instancia: cada suscriptor tiene un DBMS único ejecutando en MV propia.
  - El suscriptor tiene control total sobre definiciones de roles, autenticación de usuarios y otras tareas de gestión de seguridad.
- Modelo múlti-arrendatario: el entorno es compartido con otros suscriptores, típicamente etiquetando los datos.
  - Apariencia de uso exclusivo, pero la seguridad depende de que el CSP mantenga un entorno seguro.

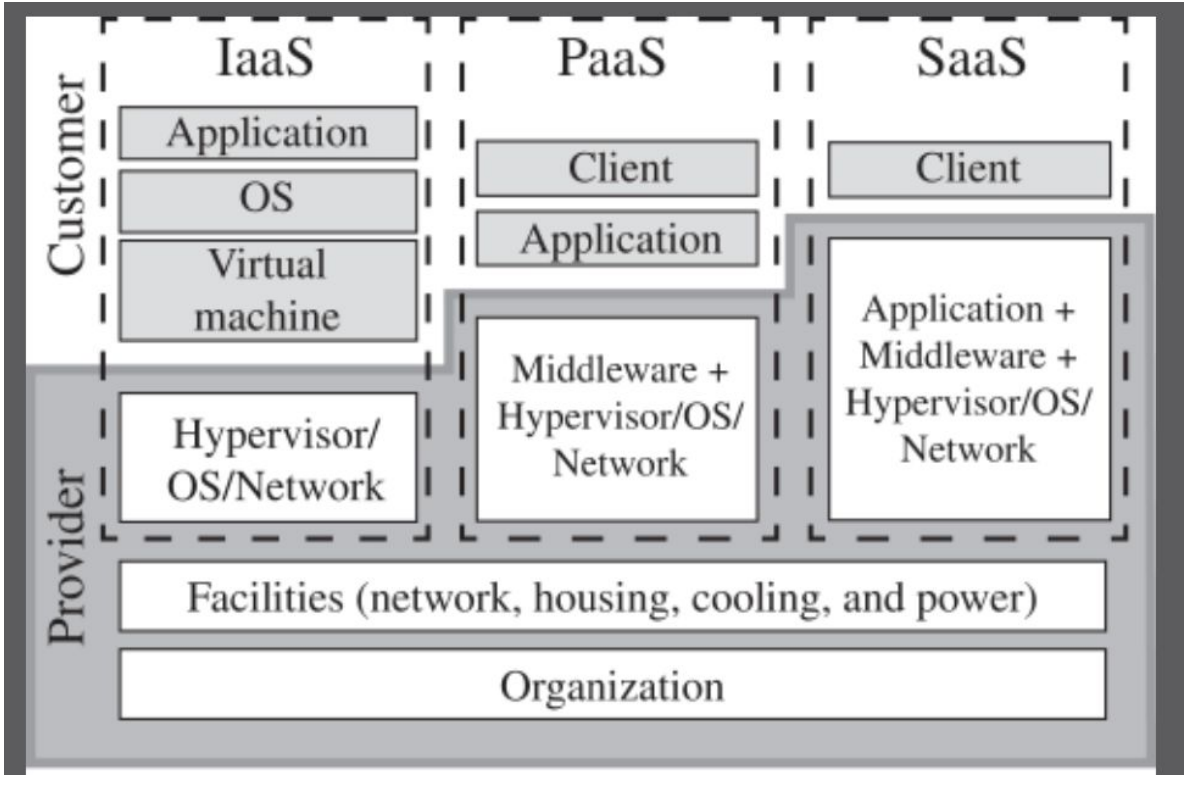
Seguridad de los Datos

- Una vez más, los datos se deben asegurar cuando están en reposo, en tránsito o en uso, y el acceso a ellos debe ser controlado.
  - El cliente puede usar cifrado para el tránsito → implica responsabilidades de gestión de claves para el CSP.
  - El cliente puede forzar técnicas de control de acceso → el CSP se ve involucrado en cierta medida, dependiendo del modelo usado.
  - Datos en reposo: idealmente cifrar la BdD y sólo almacenar datos cifrados en la nube. Si la clave permanece segura, el CSP no puede descifrar los datos (corrupción y otros ataques DOS siguen siendo un riesgo)

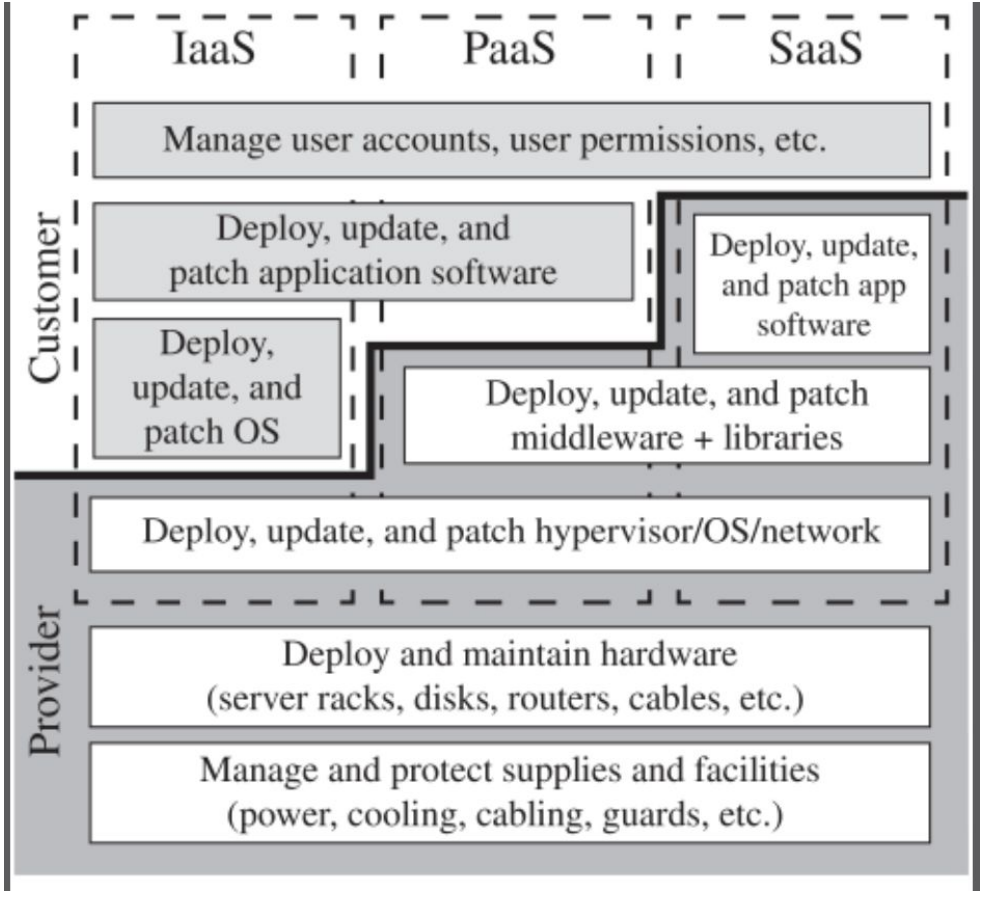
Enfoques de seguridad para los activos en la nube

Activos del CSP

- Además de los datos, el CSP debe proteger sus activos



Tareas claves del CSP y CSC



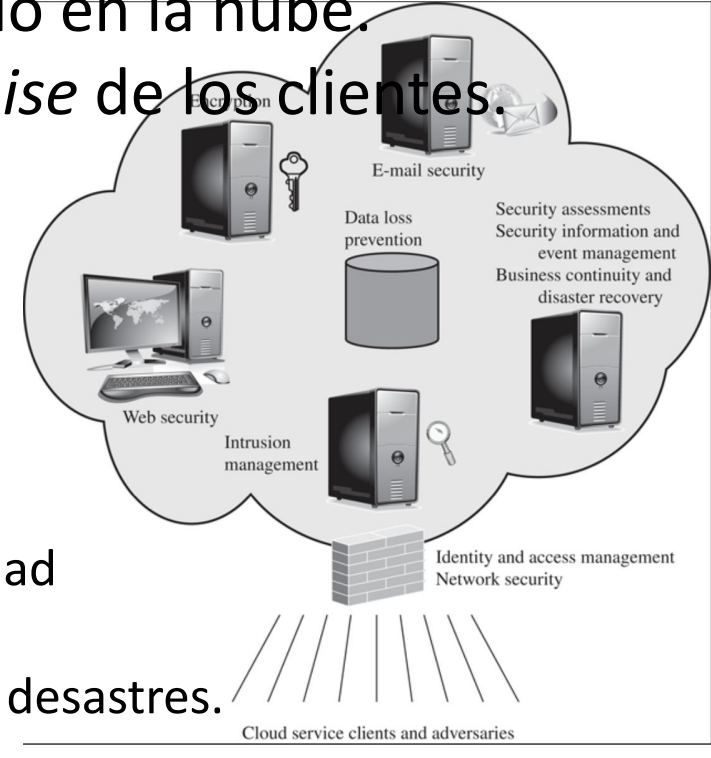
Seguridad Cloud como servicio

Seguridad como Servicio

- En general seguridad como servicio: descargar mucha de la responsabilidades por seguridad en un proveedor:
  - Autenticación
  - Anti-virus
  - Antimalware / spyware
  - Detección de intrusiones
  - Gestión de eventos de Seguridad
- SecaaS (cloud security as a service) es una parte del SaaS ofrecido por el CSP.

SecaaS

- Suministro de servicios y aplicaciones de seguridad a través de la nube. Puede ser:
  - A infraestructura y software basado en la nube.
  - Desde la nube a sistemas *on-premise* de los clientes.
- Servicios:
  - Gestión de identidades y acceso
  - Prevención de pérdidas de datos
  - Seguridad Web, e-mail y de la red
  - Evaluaciones de seguridad
  - Gestión de Intrusiones
  - Gestión de información y eventos de seguridad
  - Cifrado
  - Continuidad de negocio y recuperación ante desastres.



Gestión de Identidad y acceso

- En general seguridad como servicio: descargar mucha de la responsabilidades por seguridad en un proveedor:
  - Autenticación
  - Anti-virus
  - Antimalware / spyware
  - Detección de intrusiones
  - Gestión de eventos de Seguridad
- SecaaS (cloud security as a service) es una parte del SaaS ofrecido por el CSP.

Un módulo Open Source para seguridad Cloud

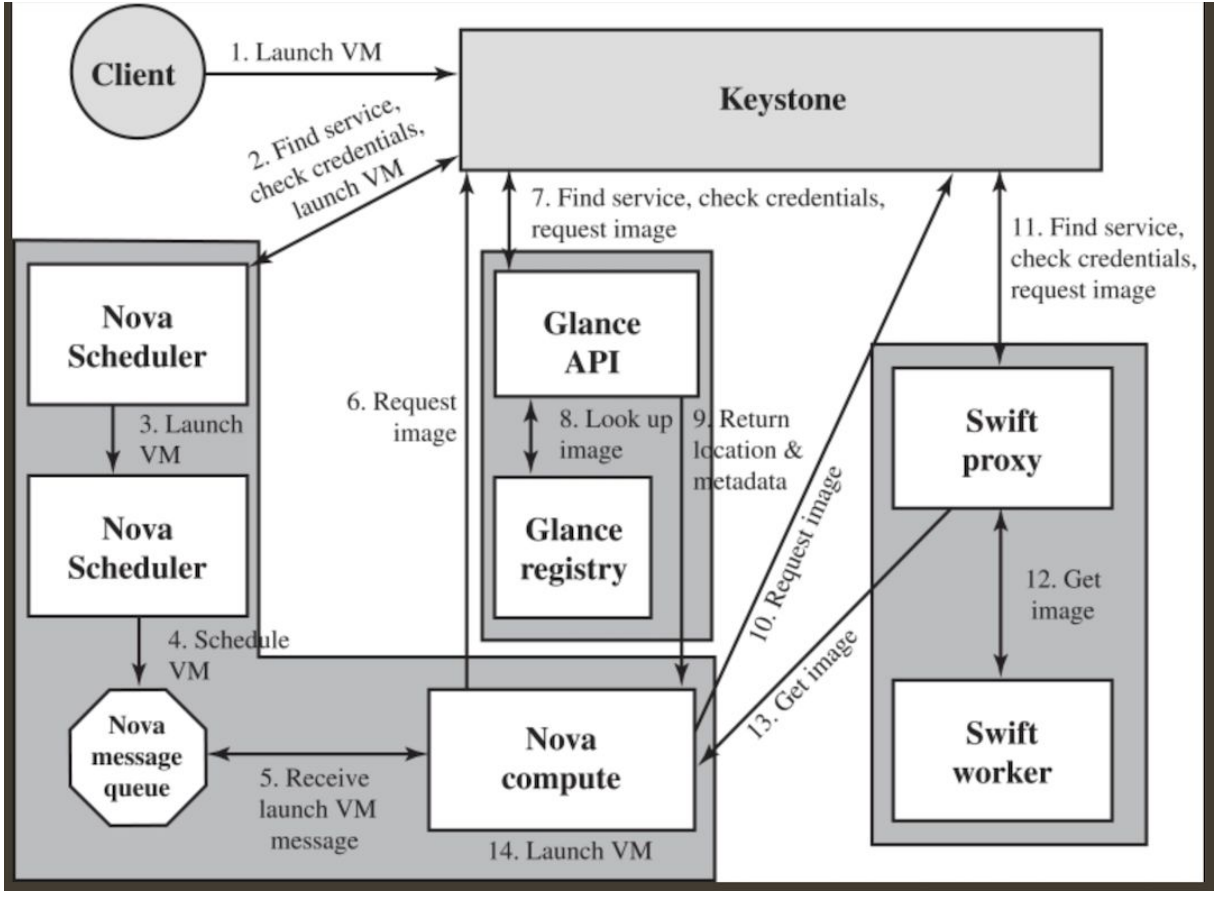
OpenStack cloud OS

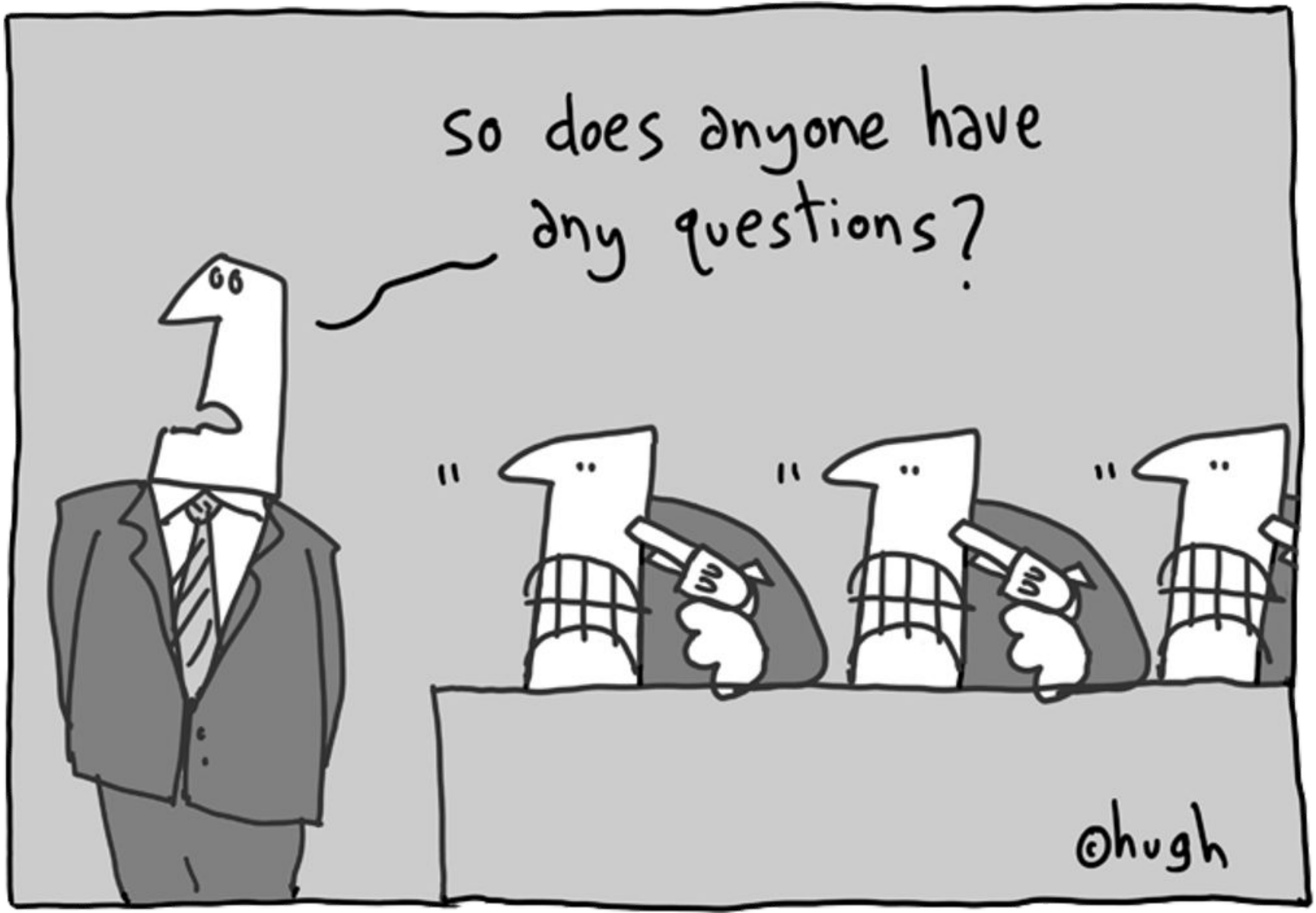
- Proyecto de software abierto para producir un sistema operativo abierto para la nube.
- Objetivo: crear y gestionar grandes grupos de servidores virtuales privados en un entorno cloud.
- Dirigido a satisfacer las necesidades de nubes públicas o privadas, independientemente de su tamaño.

Módulo de seguridad: Keystone

- Servicios principales:
  - Identidad
  - Token
  - Catálogo de servicios
  - Políticas

Lanzando una MV con OpenStack




so does anyone have any questions?
©hugh