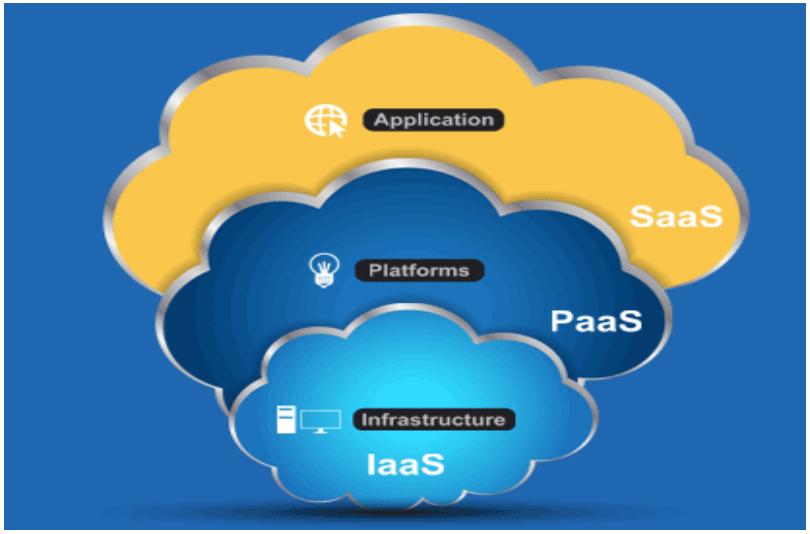
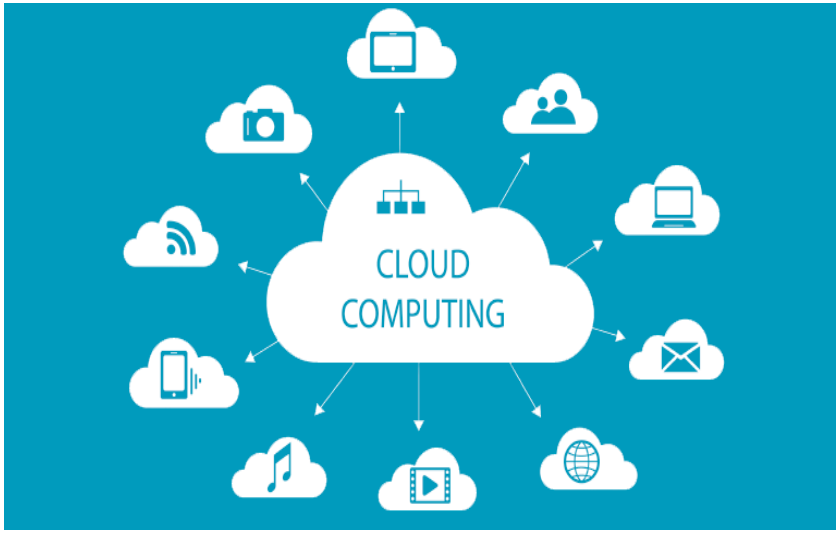
Fundamentos de las TICs y la Ciberseguridad

Eduardo Díaz-Mayordomo
Francisco de Santos
Facultad de CC. Jurídicas y Empresariales

CLOUD.





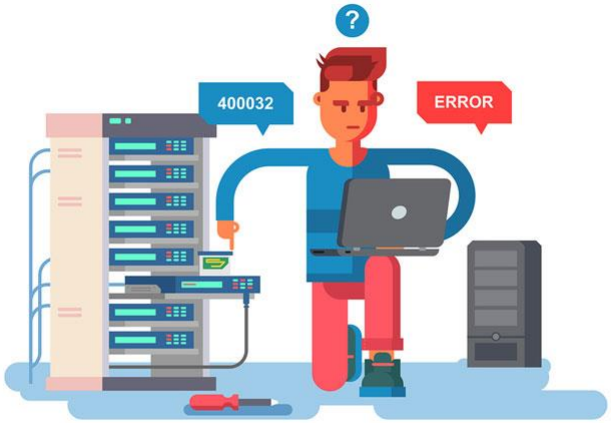
CLOUD. Índice.

1. Introducción
2. IaaS. Infraestructura como Servicio.
3. PaaS. Plataforma como Servicio.
4. SaaS. Software como Servicio.
5. Seguridad en Servicios Cloud.

On Premise

- El cliente dispone de la arquitectura y el software en sus dependencias.
- Inmovilizado a nivel Contable.
- Reclama un mantenimiento continuo.
- Depende de un espacio físico.
- Controles para garantizar la disponibilidad del servicio.
- SLAs? → Service Level Agreement.

- Servidores, Comunicaciones, Software.



On Cloud

- La nube, ¿pero que es realmente la nube?
- Todos los temas vistos hasta ahora establecen los pilares básicos para conocer que es la nube.

¿Cuál es? → Hay muchas nubes.

CLOUD. Introducción.

On Cloud

- Cloud Computing → Ofrecer a organizaciones y usuarios servicios de computación a través de una red (internet, vpn, punto a punto, etc…).

- **Tipos:**
  - **Privado** → Solamente tiene acceso la organización.
  - **Público** → Abierta a usuarios externos a la organización.
  - **Híbrida** → Servicios privados y públicos.

- **Asociado a la virtualización.**

  - **Múltiples aplicaciones para cada nodo físico:**
    - Servidor de ficheros.
    - Servidor web.
    - Servidor bases de datos.
    - Aplicaciones.

CLOUD. Introducción.

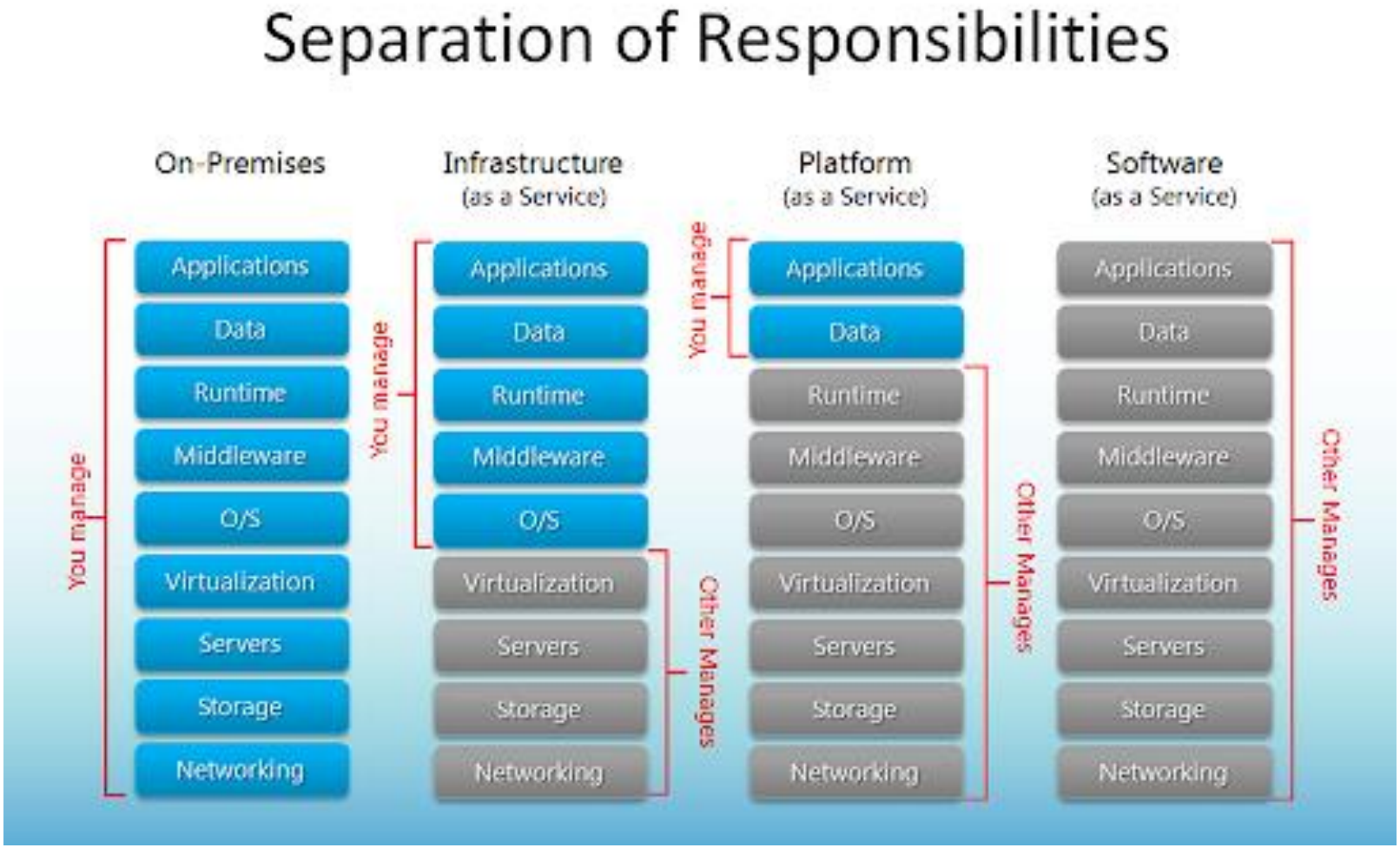
Características del Cloud		
Pago Por uso	Cálculo del precio en base a las necesidades del cliente.	En un pico de trabajo se pueden aumentar los recursos y pagar la diferencia.
Acceso desde la Red	Acceso desde cualquier ubicación.	Navegadores, móviles.
Recursos Compartidos	Los recursos (servidores, comunicaciones, almacenamiento) son compartidos.	Disponer de hardware de elevado coste a disposición puntual.
Recursos a la carta	El cliente puede redimensionar sus recursos de manera rápida y eficaz.	Desde paneles de administración intuitivos.
Servicio Supervisado	El control se realiza de manera automática. Transparente al usuario.	No hay que realizar aprovisionamiento de hardware y software.

CLOUD. Introducción.

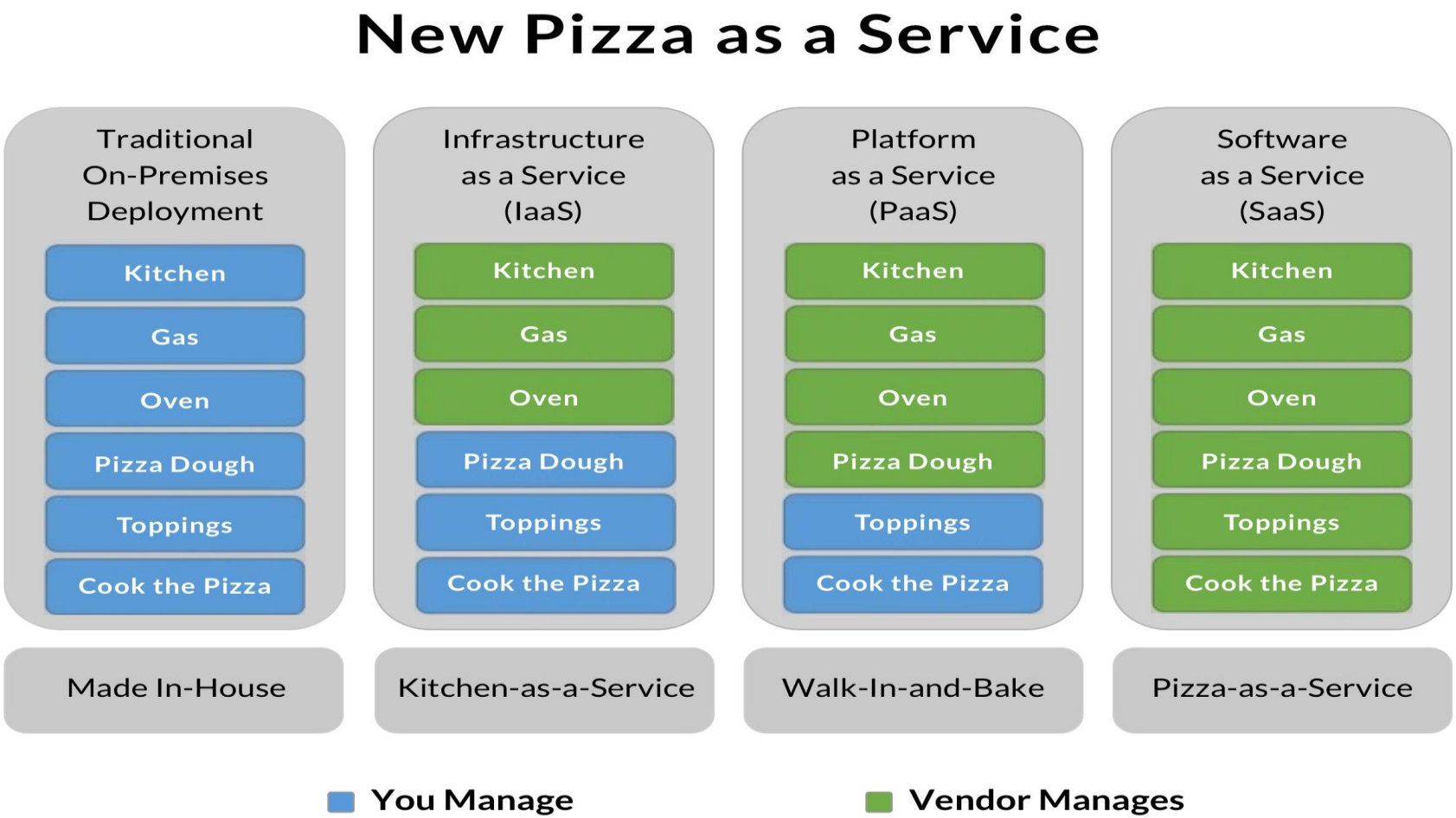
Ventajas del uso Cloud	
Ahorro de costes.	Reducción de costes en infraestructura.
Optimización de recursos.	Los recursos se utilizan cuando se necesitan.
Recuperación ante desastres.	La información está en varias ubicaciones. Disponibilidad.
Tecnología actualizada.	El proveedor realiza las tareas de mantenimiento.
Dedicación al negocio	Menor administración → Mayor Gestión.

Desventajas del uso Cloud	
Perdida de Control.	Revisión de contratos de suministros: ubicación, disponibilidad, responsabilidades → SLAs.
Confidencialidad y seguridad.	Un problema en el proveedor compromete nuestra información.
Disponibilidad del servicio.	Una caída del servicio o las comunicaciones restringe el acceso.
Acceso a Internet.	Es condición indispensable para su uso.

On Cloud


Separation of Responsibilities
On-Premises
Infrastructure (as a Service)
Platform (as a Service)
Software (as a Service)
Applications
Data
Runtime
Middleware
O/S
Virtualization
Servers
Storage
Networking
You manage
You manage
You manage
Other Manages
Other Manages
Other Manages

On Cloud


New Pizza as a Service
Traditional On-Premises Deployment
Kitchen
Gas
Oven
Pizza Dough
Toppings
Cook the Pizza
Made In-House
Infrastructure as a Service (IaaS)
Kitchen
Gas
Oven
Pizza Dough
Toppings
Cook the Pizza
Kitchen-as-a-Service
Platform as a Service (PaaS)
Kitchen
Gas
Oven
Pizza Dough
Toppings
Cook the Pizza
Walk-In-and-Bake
Software as a Service (SaaS)
Kitchen
Gas
Oven
Pizza Dough
Toppings
Cook the Pizza
Pizza-as-a-Service
You Manage
Vendor Manages

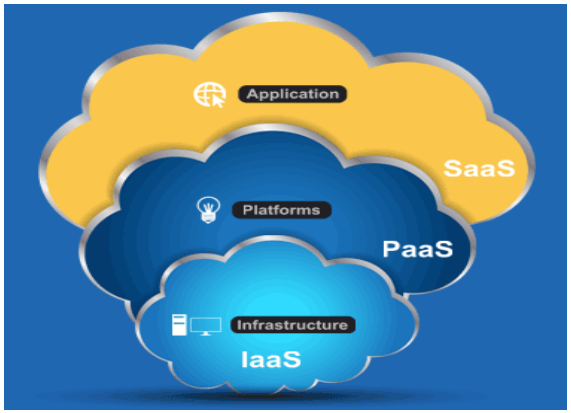
CLOUD. Introducción.

On Cloud

Algunos recursos web:

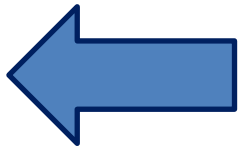
https://www.youtube.com/watch?v=36zducUX16w

https://www.youtube.com/watch?v=lO0pMFqUehQ



CLOUD. Índice.

1. Introducción
2. IaaS. Infraestructura como Servicio.
3. PaaS. Plataforma como Servicio.
4. SaaS. Software como Servicio.
5. Seguridad en Servicios Cloud.



CLOUD. IaaS. Infraestructura como Servicio.

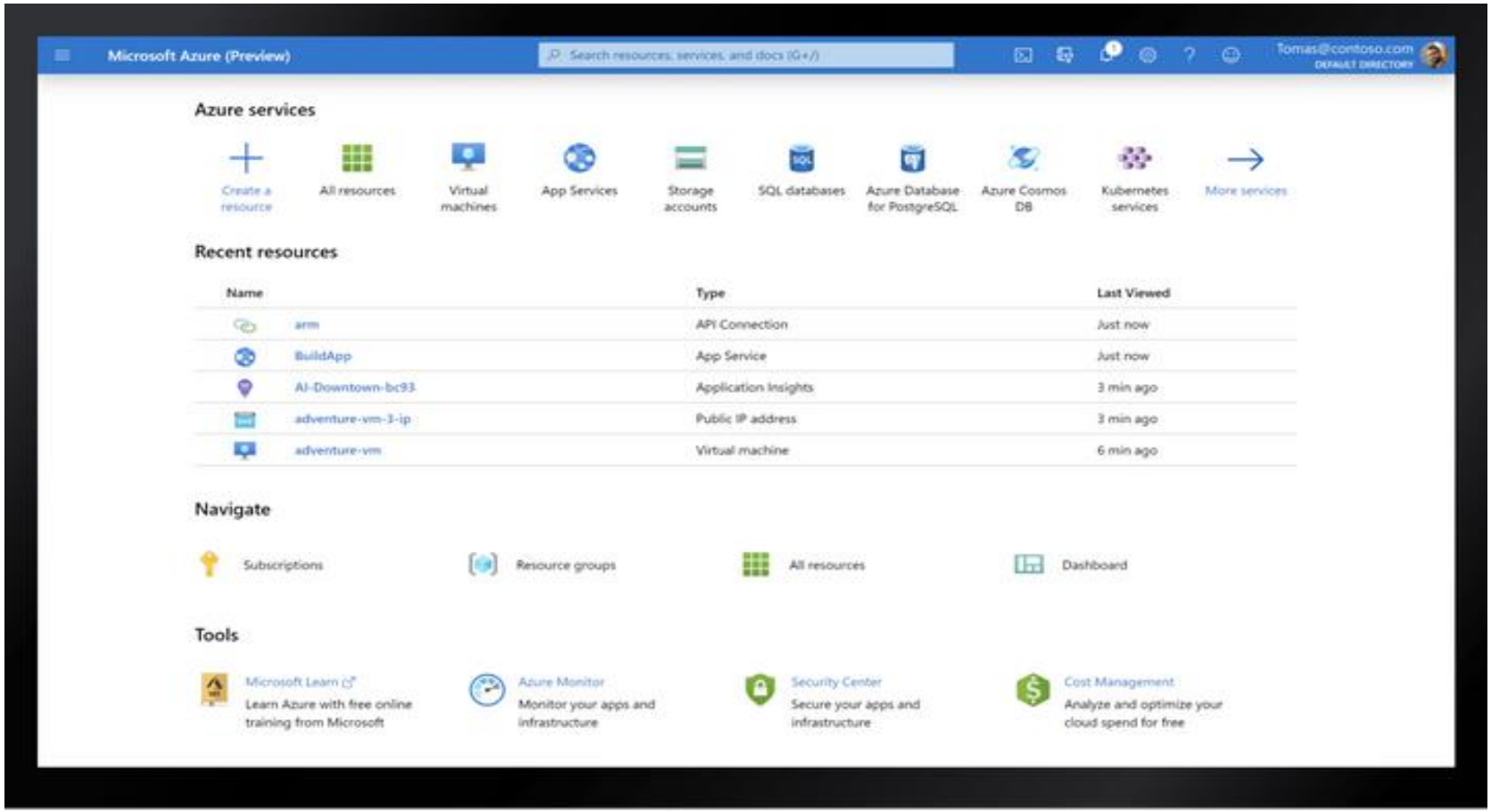
IaaS → Infraestructura como Servicio.

- El proveedor proporciona la Infraestructura TI.
- Escalable.
  - Almacenamiento, alojamiento, computación (CPU).

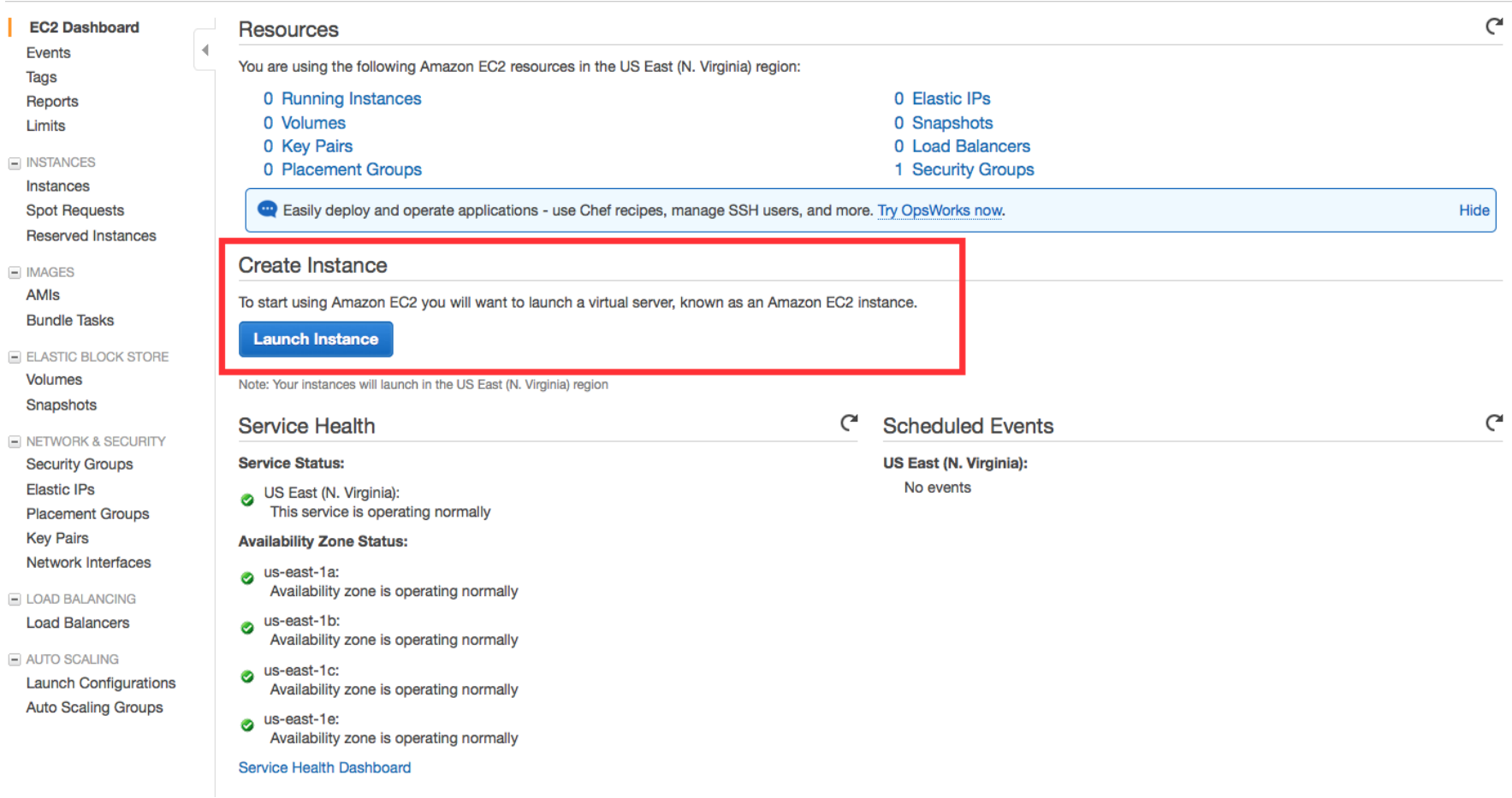
- El cliente gestiona la administración y gestión de la infraestructura.
- Máquinas virtuales.
- Ahorro en licencias de software y aprovisionamiento de hardware.

CLOUD. IaaS. Infraestructura como Servicio.

IaaS → Infraestructura como Servicio.

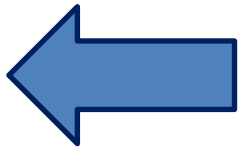


IaaS → Infraestructura como Servicio.



CLOUD. Índice.

1. Introducción
2. IaaS. Infraestructura como Servicio.
3. PaaS. Plataforma como Servicio.
4. SaaS. Software como Servicio.
5. Seguridad en Servicios Cloud.



CLOUD. PaaS. Plataforma como Servicio.

PaaS → Plataforma como Servicio.

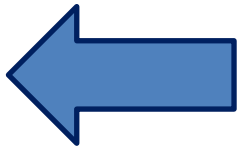
- El proveedor proporciona la Infraestructura TI + Capacidades y Herramientas para desarrollar nuevas aplicaciones.
- Escalable.
    - Middleware, bases de datos, sistemas operativos.

- Proporciona al desarrollador todas las herramientas necesarias.
- Máquinas virtuales → Sistema operativo + Aplicativos (servidor web, servidor de bases de datos).
- Gasto y no inmovilizado.

PaaS → Plataforma como Servicio.

CLOUD. Índice.

1. Introducción
2. IaaS. Infraestructura como Servicio.
3. PaaS. Plataforma como Servicio.
4. SaaS. Software como Servicio.
5. Seguridad en Servicios Cloud.



CLOUD. SaaS. Software como Servicio.

SaaS → Software como Servicio.

- El cliente paga el alquiler de un software.
- Servicio basado en web + Apps móviles.

- Proporciona al usuario una experiencia completa.
- Cliente Pesado (nativo) → Cliente web.
- Coste fijos de licencias de software.

Dropbox

CLOUD. Índice.

1. Introducción
2. IaaS. Infraestructura como Servicio.
3. PaaS. Plataforma como Servicio.
4. SaaS. Software como Servicio.
5. Seguridad en Servicios Cloud.

Seguridad en la Nube.

¿Qué debemos tener en consideración al elegir un proveedor de servicios Cloud?

- Tratamiento de los datos.
- Localización de los datos.
- Portabilidad de los datos.

Acuerdos de Nivel de Servicio → SLAs.

- Unilateral → No se negocia el acuerdo → Cloud Pública.
- Parcialmente definido → Negociación de clausulas → Cloud Híbrida y Privada.
- Negociable → Negociación casi total → Cloud Privadas.

Seguridad en la Nube. SLAs.

- Medidas de seguridad adoptadas por el proveedor.
- Confidencialidad de los datos almacenados.
- Calidad de servicio.
- Seguridad en las transacciones de datos.

Seguridad en la Nube. Consideración en contratos.

Subcontratación

- El proveedor no dispone de los recursos propios y subcontrata.
- Proceso recursivo. Subcontrata vuelve a subcontratar servicios.

Localización

- Al contratar, es importante conocer la ubicación de los proveedores e infraestructura.
- Consecuencias legales. Incumplimiento de normativa.

Transparencia

- Los servicios pueden ser auditables o transparentes en función de:
  - Posibilidades de reclamación.
  - Condiciones de seguridad.

Seguridad en la Nube. Tipos de contrato.

Negociado

- El cliente puede fijar algunas condiciones en relación:
  - Tipo de datos.
  - Medidas de seguridad.
  - Localización.
  - Portabilidad.

Adhesión

- El cliente no puede fijar las condiciones.
- Adaptación a las condiciones del proveedor. Iguales para todos los clientes.
- Común en nubes públicas e híbridas.

Mixto

- Fijar condiciones parciales, otras determinadas por el proveedor.
- Dependen de la flexibilidad del proveedor.

Seguridad en la Nube. Amenazas.

1. Acceso no autorizado.
2. Amenazas internas → Empleados.
3. Interfaces → Manipulables por atacantes.
4. Tecnologías compartidas → Una vulnerabilidad expone a varios clientes.
5. Fuga de información → Importancia del cifrado.
6. Suplantación de identidad → Phising.
7. Desconocimiento del entorno.
8. Ataques de hacking.

Seguridad en la Nube. Riesgos.

1. Acceso de usuarios con privilegios.
2. Cumplimiento normativo.
3. Localización de los datos.
4. Aislamiento de datos.
5. Recuperación ante desastres.
6. Análisis forense → Trazabilidad.
7. Viabilidad en el tiempo.

CLOUD. Seguridad en Servicios Cloud.

Riesgos	Mitigación	Responsabilidad del cliente
Acceso de usuarios con privilegios	Solo los usuarios con privilegios los tengan establecidos.	Decidir que privilegios de acceso tendrán los empleados.
Cumplimiento normativo	Realización de auditorías externas y certificaciones de seguridad.	Velar por el cumplimiento normativo. Control de auditorías.
Localización de los datos	Conocer el marco regulatorio aplicable al país del suscriptor del servicio.	Conocer la localización para conocer la legislación aplicable.
Aislamiento de información	Datos en reposo aislados y cifrados.	Conocer la localización y adoptar medidas de protección.
Recuperación	Exigir capacidad de recuperación y tiempo de respuesta.	
Análisis Forense	Logs, bitácoras y datos se gestionan de manera centralizada.	
Viabilidad	Posibilidad de recuperación de datos ante cambio de dirección del proveedor.	

- Asegurar condiciones en acuerdo.
- Conveniente disponer de datos replicados en otra plataforma.

Fundamentos de las TICs y la Ciberseguridad

¡Muchas gracias!