CENTRE DE SUPERCOMPUTACIÓ
DE CATALUNYA

CESCA

Viviendo en las nubes – Mesa Redonda

Jordi Guijarro Olivares
jguijarro@cesca.cat

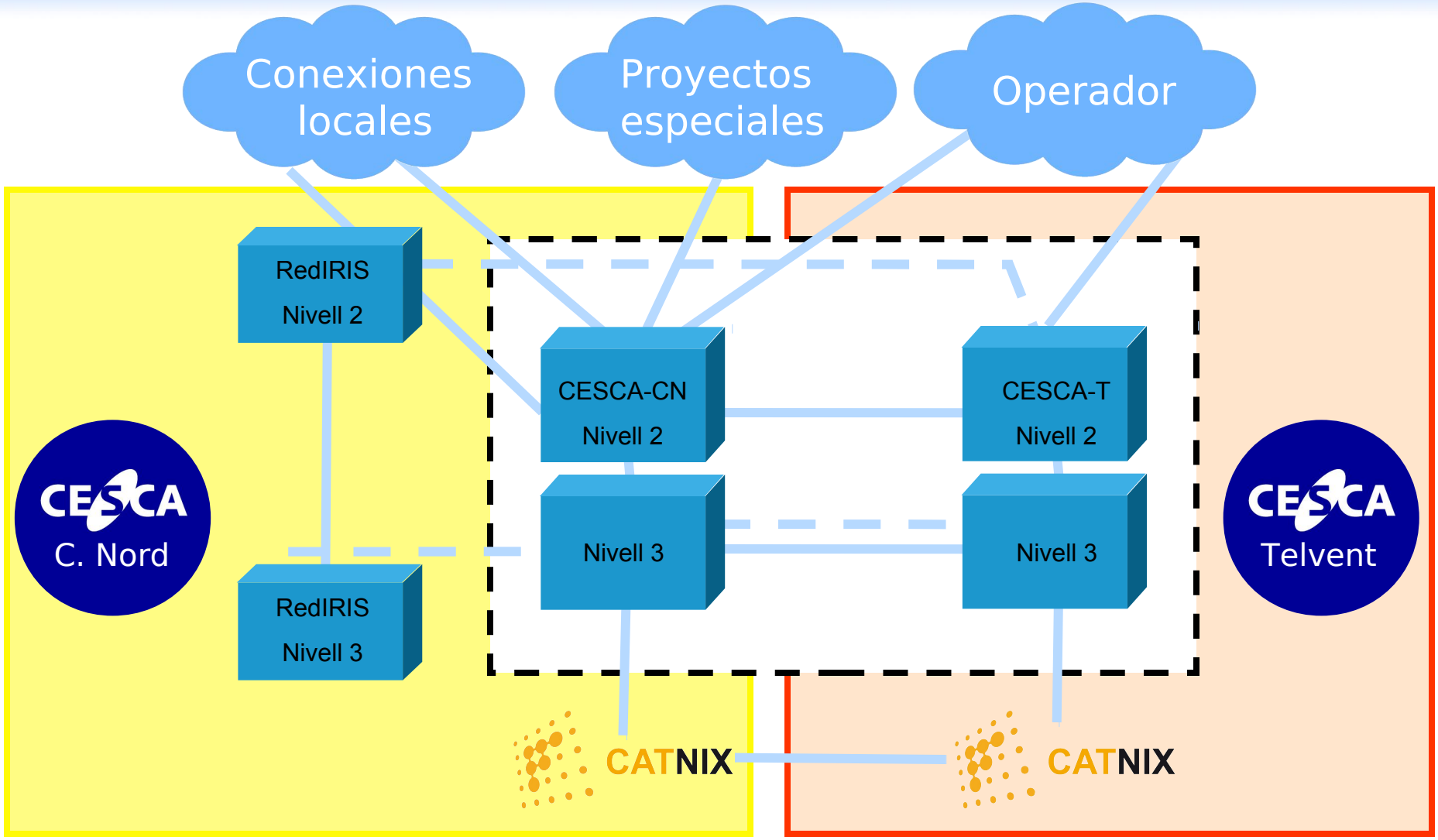
IX Foro Seguridad RedIris – UPV , 10/3/2011

Agenda

- ✓ Componentes de la nube
- ✓ El CESCA como proveedor de servicios
- ✓ Vinculación del subscriptor
- ✓ ¿Qué migrar/externalizar?
- ✓ Extensión hacia un modelo híbrido

✓Y a partir de aquí...

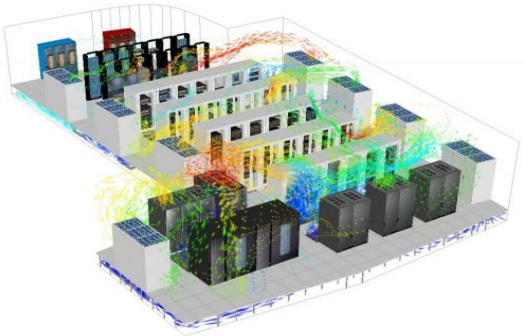
La red: Autopistas de la nube



Política de uso de la Anella Científica

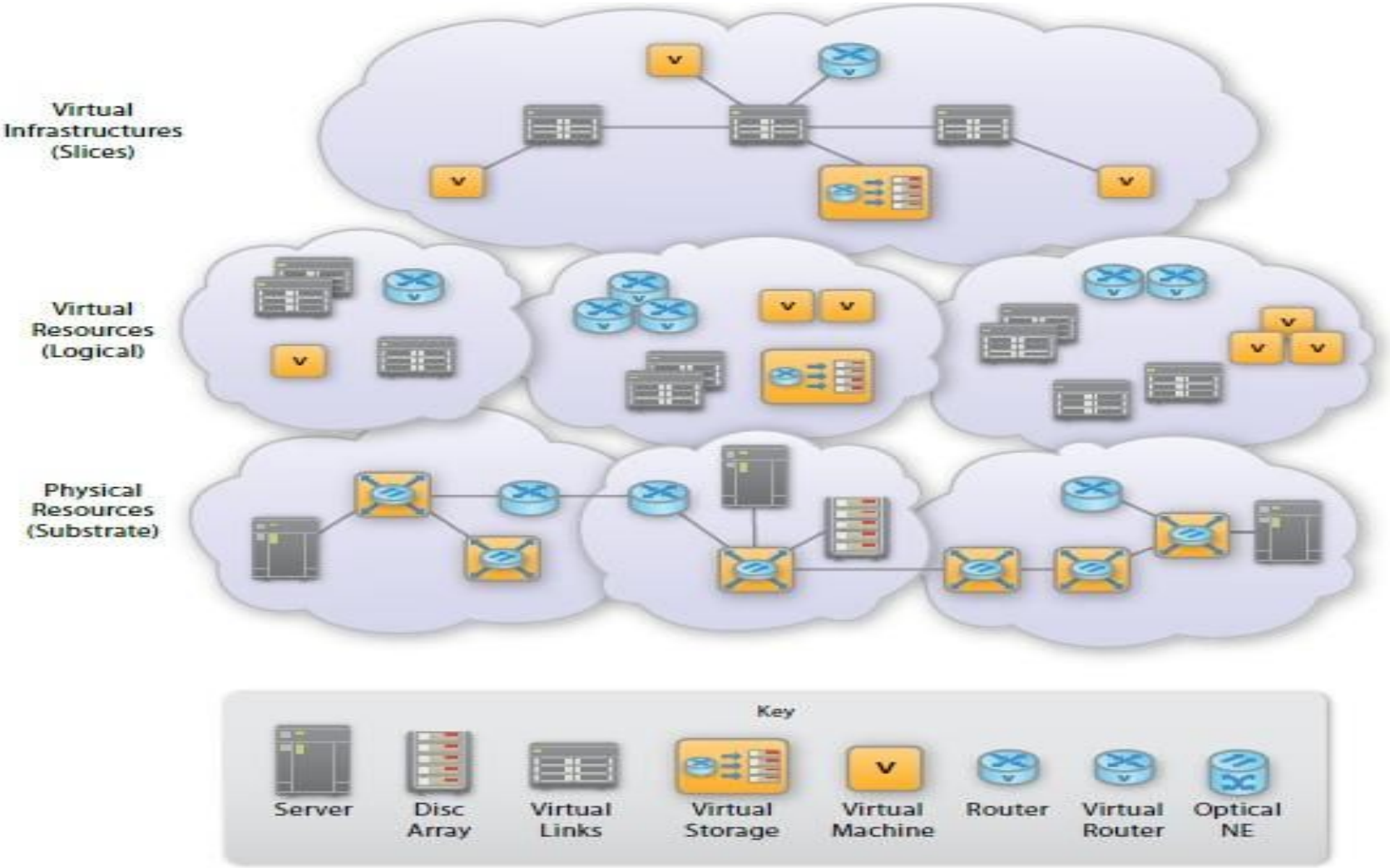
- ✓ No se han de aceptar ni estimular las prácticas ilegales
- ✓ Usar correctamente y eficazmente los recursos
- ✓ Preservar la confidencialidad del los usuarios (permitiendo su identificación)
- ✓ Reconocer y defender los derechos de propiedad intelectual
- ✓ Difundir sus objetivos y su política de uso

CPD's : Islas en la nube



- ✓ Control de acceso / Seguridad Física
- ✓ Plataformas de SAI redundantes.
- ✓ Grupos Electrógenos.
- ✓ Sistema de Climatización redundante.
- ✓ Monitoraje proactivo 24x7.
- ✓ Garantias de disponibilidad Tier II+

Arquitecturas de virtualización

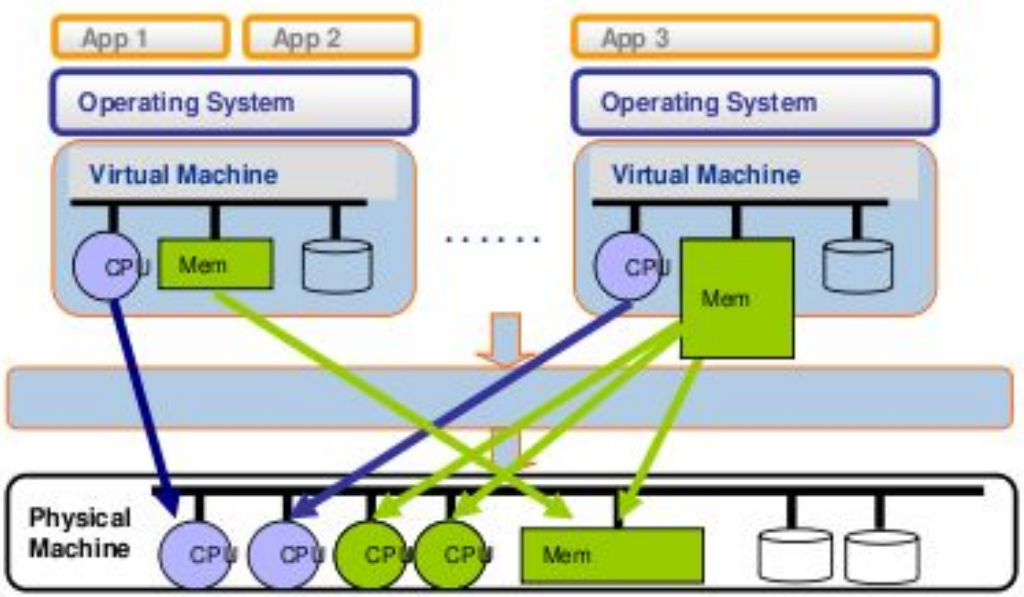


Escenario: Recursos compartidos al 100%

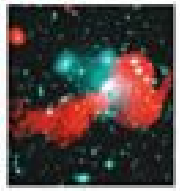
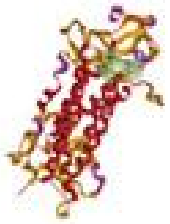
Multitenancy: refers to a principle in software architecture where a single instance of the software runs on a server, serving multiple client organizations (tenants). With a multitenant architecture, a software application is designed to virtually partition its data and configuration, and each client organization works with a customized virtual application instance.

Sin dudar exprimir al máximo la infraestructura...

/dev/ksm: dynamic memory sharing



Recursos ya en una nube con connotación de "comunidad"

Cálculo y Archivo	Comunicaciones	Portales y Repositorios
CAP 	ANELLA CIENTÍFICA	TDR RECERCAT
SED 	Red IRIS Node Catalunya	RACO RECYT
SDF 	CATNIX	mdx padicat
AUC		Padicyt CALAIX

Política de seguridad I

- ✓ Herramienta necesaria la cuál proporciona :

  - Descripción global de la seguridad de la información: intenciones, activos y medidas de control.

  - Marco para crear o redefinir de manera consistente les normas y procedimientos en los sistemas de información.

  - Concienciación de la seguridad y el cumplimiento de las mejores prácticas frente a requisitos normativos.

  - ...

Política de seguridad II

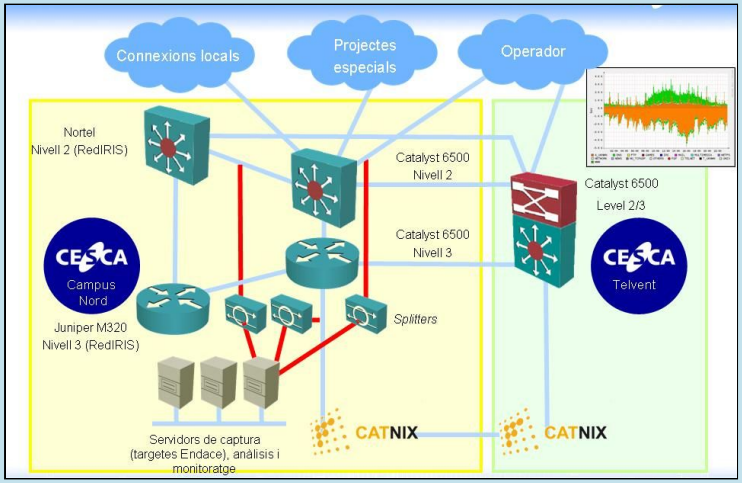
- ✓ La información:
  - Activo fundamental per la activitat de cualquier organización.
  - Convenientemente protegida frente posibles amenazas
  - Minimizar el riesgo (manipulación o destrucción no autorizada)

- ✓ La política de seguridad del CESCA:
  - Garantiza la confidencialidad, integridad y disponibilidad
    - Propia (interna)
    - Relacionada con los servicios que presta
  - Asume la responsabilidad de custodiarla
  - Expresa su compromiso de protegerla
  - Promueve un buen uso por parte de las instituciones usuarias

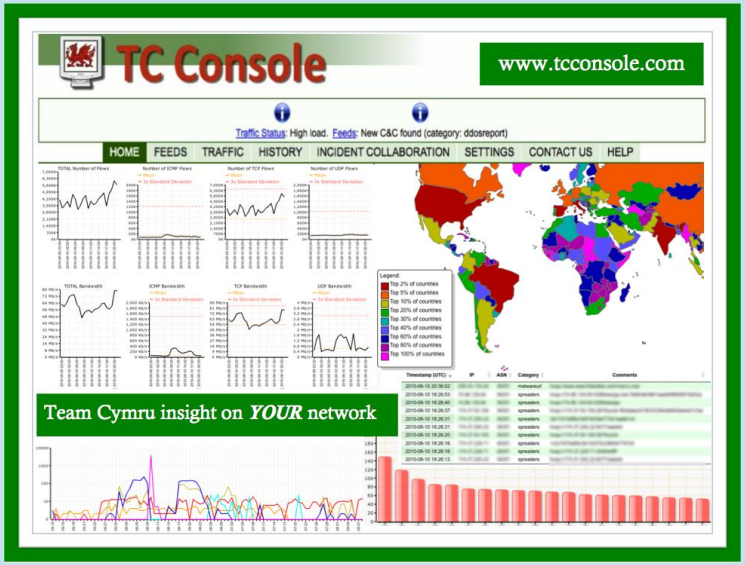
Equipo de Respuesta a Incidentes (ERIAC)

- ✓ **Des del 2003**
- ✓ **Servicios**
  - Equipo de Respuesta a Incidentes de la Anella Científica (ERIAC)
    - Reactivo y proactivo
    - Coordinación con otros equipos de respuesta y instituciones vinculadas
  - Sistema d'análisis: SMARTxAC

SMARTxAC



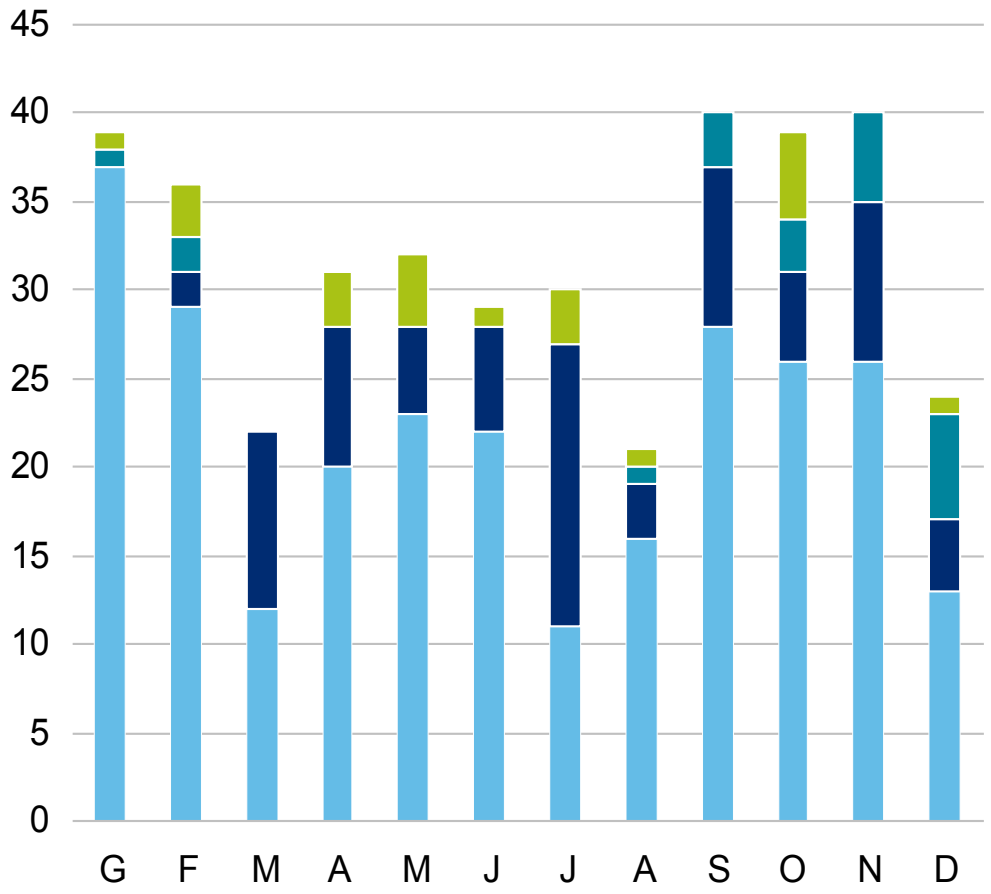
ERIAC: Fuentes externas



shadowserver

Google

ERIAC: Incidentes de seguridad



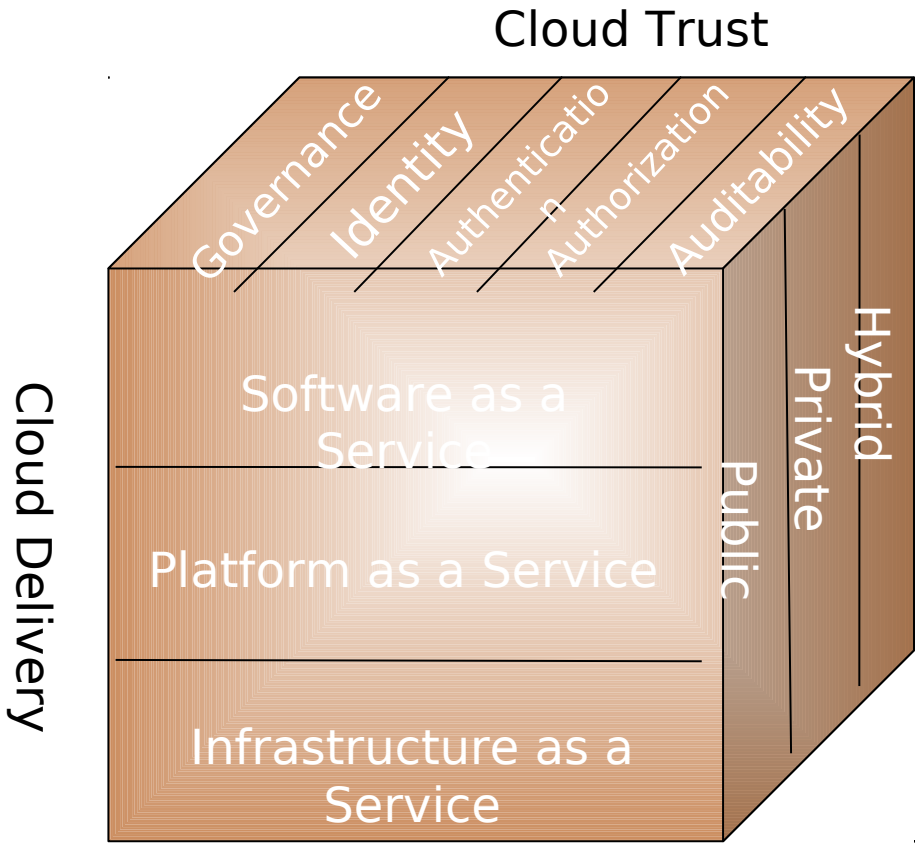
	2008	2009	2010
Contenido abusivo	27%	23%	23%
Disponibilidad	4%	5%	2%
Fraude	10%	15%	7%
Código malicioso	10%	9%	20%
Recogida inf.	8%	7%	12%
Seguridad inf.	1%	1%	8%
Intrusión	5%	4%	4%
Intento de intrusión	34%	35%	22%
Otros	1%	1%	1%

	Total	Crítica	Alta	Med.	Baja
2008	205	4%	9%	26%	60%
2009	223	4%	10%	23%	63%
2010	365	5%	6%	23%	66%

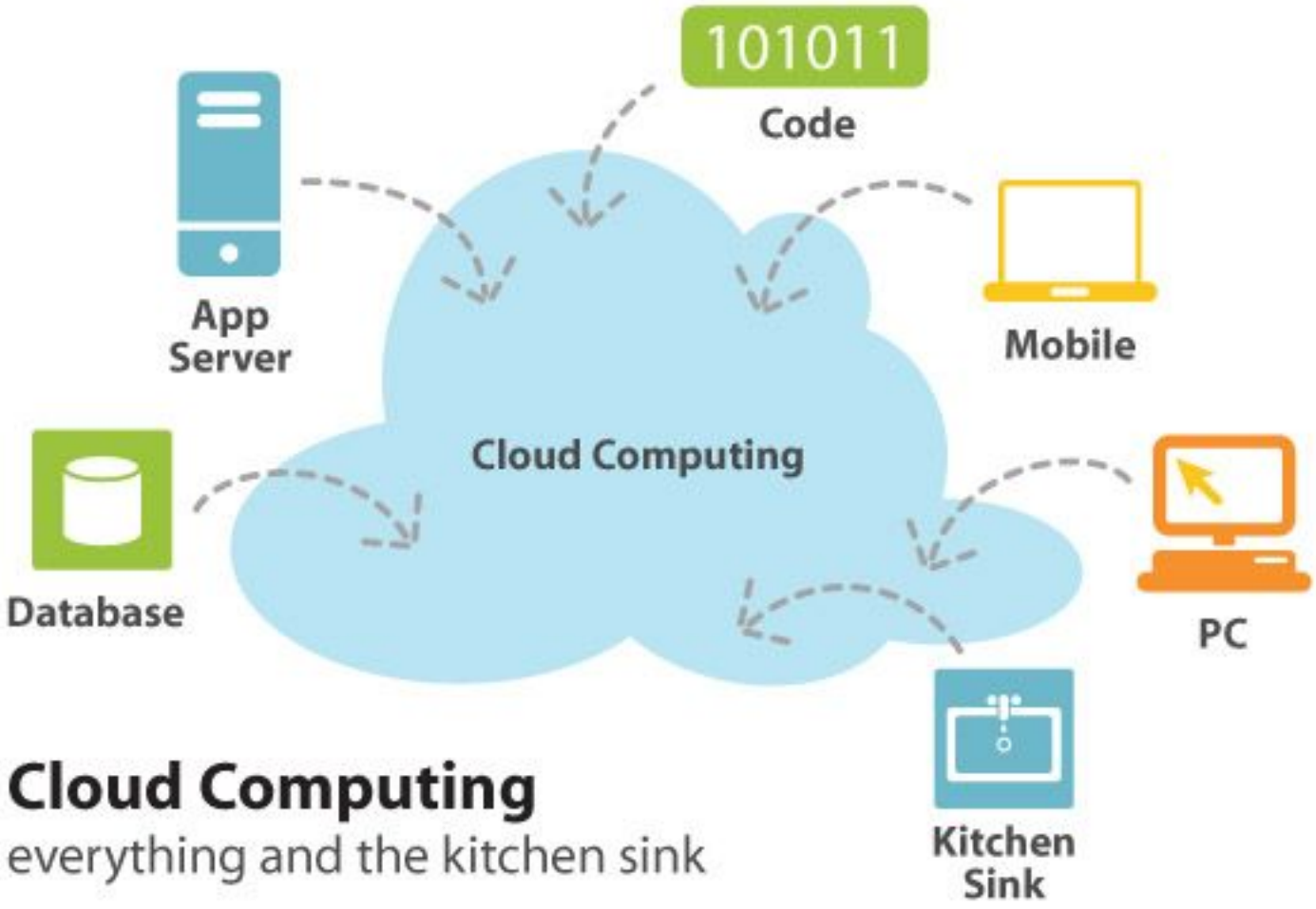
Requisitos de un Servicio

a) Seguridad Física
b) Garantia de suministro
c) Seguridad Perimetral
d) Protección de les comunicaciones
e) Tolerancia a Fallos
f) Sistemas auditables
g) Servicio Escalable
h) Gestión vulnerabilidades
i) Recuperación ante desastres
j) Niveles de servicio
k) ...

Hacia la nube: Cubo de confianza

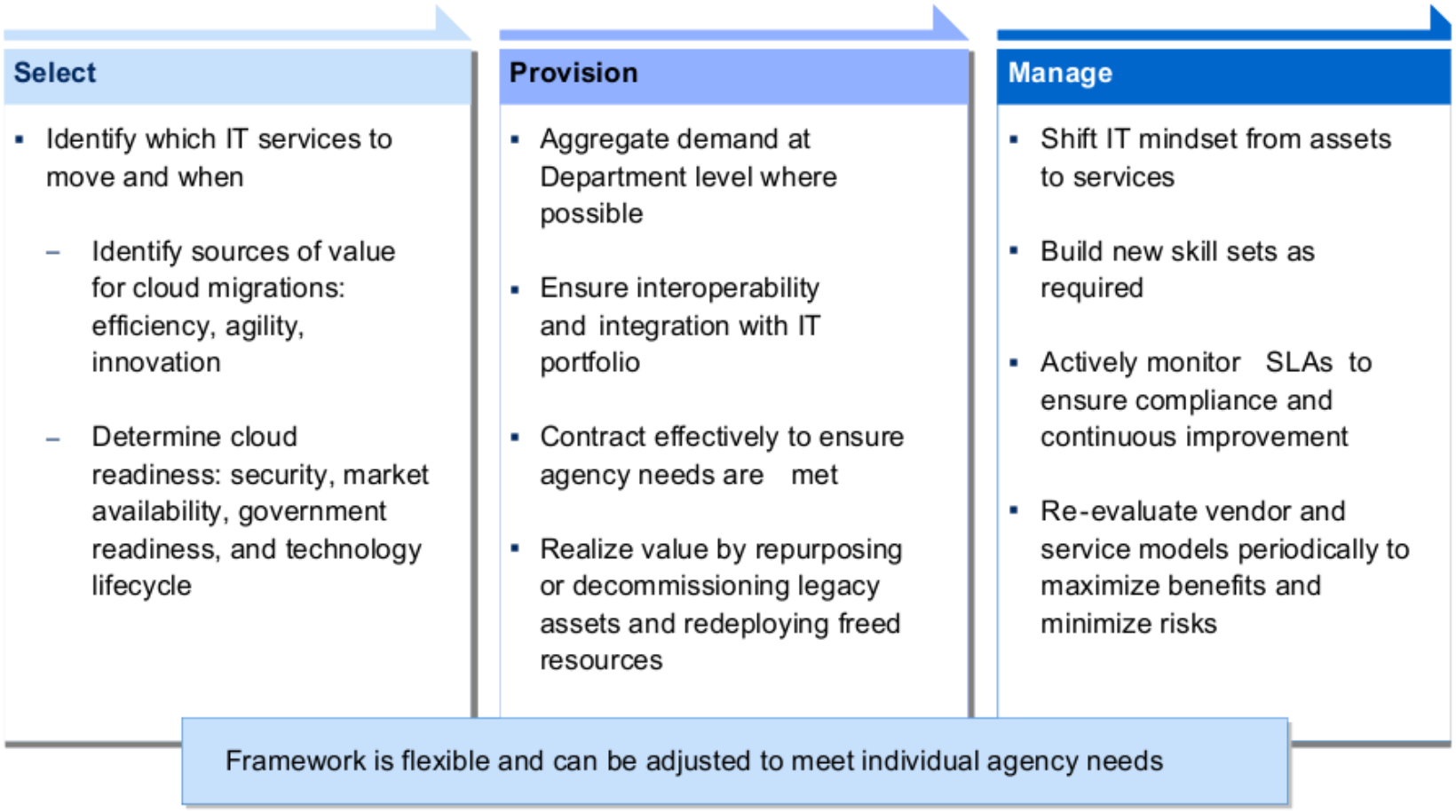


Atención : NO sin un análisis de riesgos...

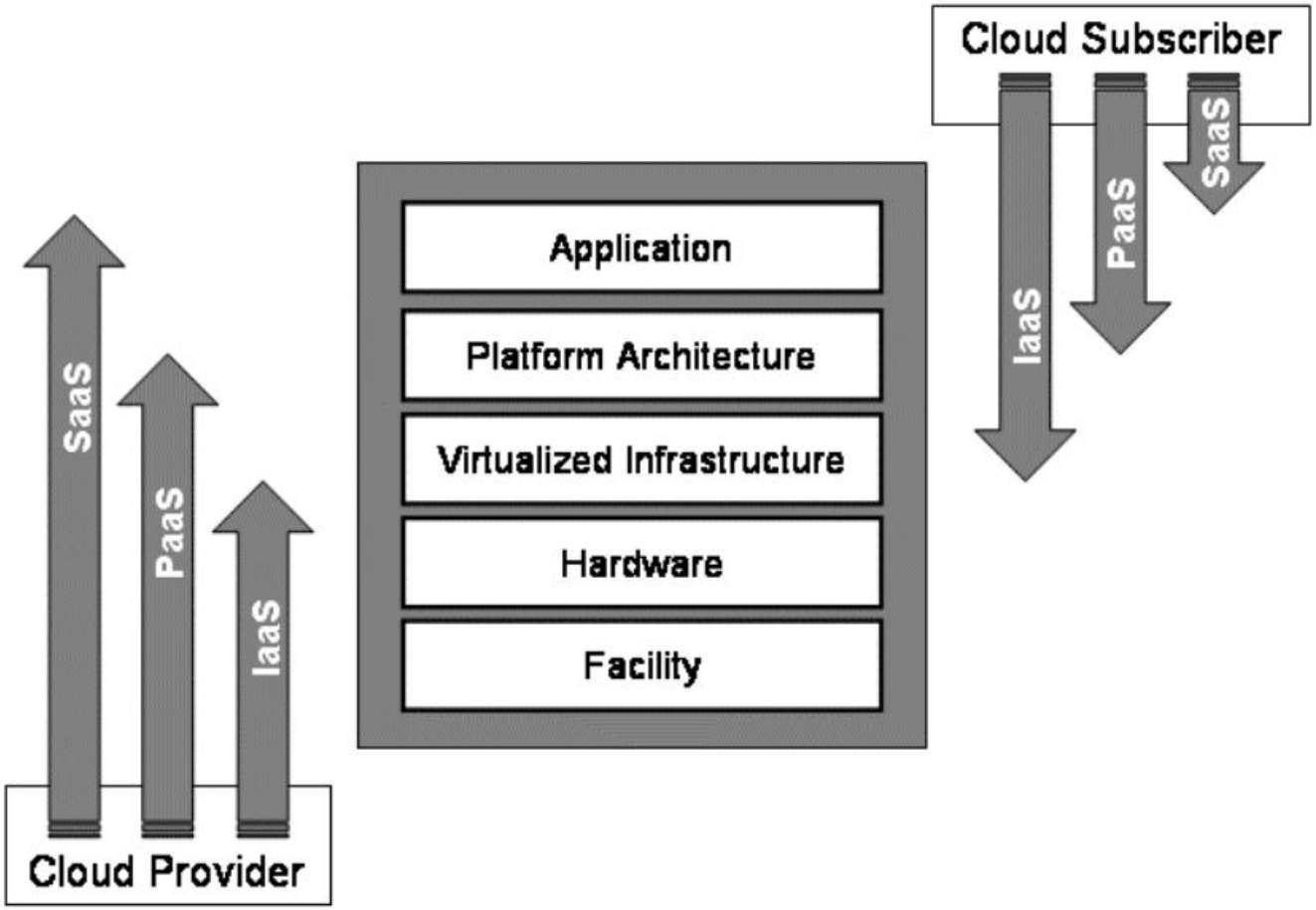


Caso Agencia Federal - WhiteHouse

Figure 3: Decision Framework for Cloud Migration



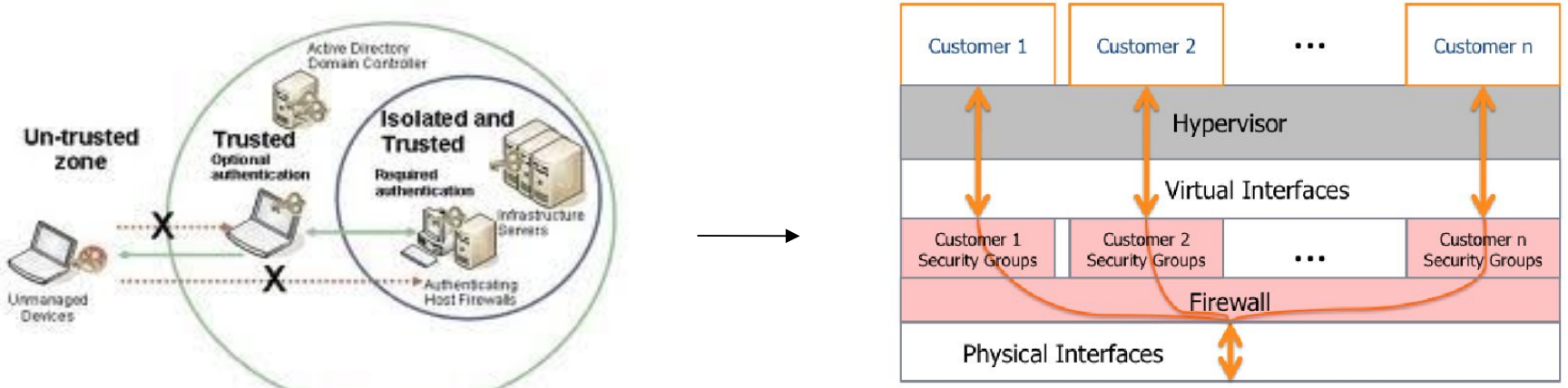
Capas de responsabilidad Proveedor - Subscriptor



Extensión de la nube privada en un modelo IaaS

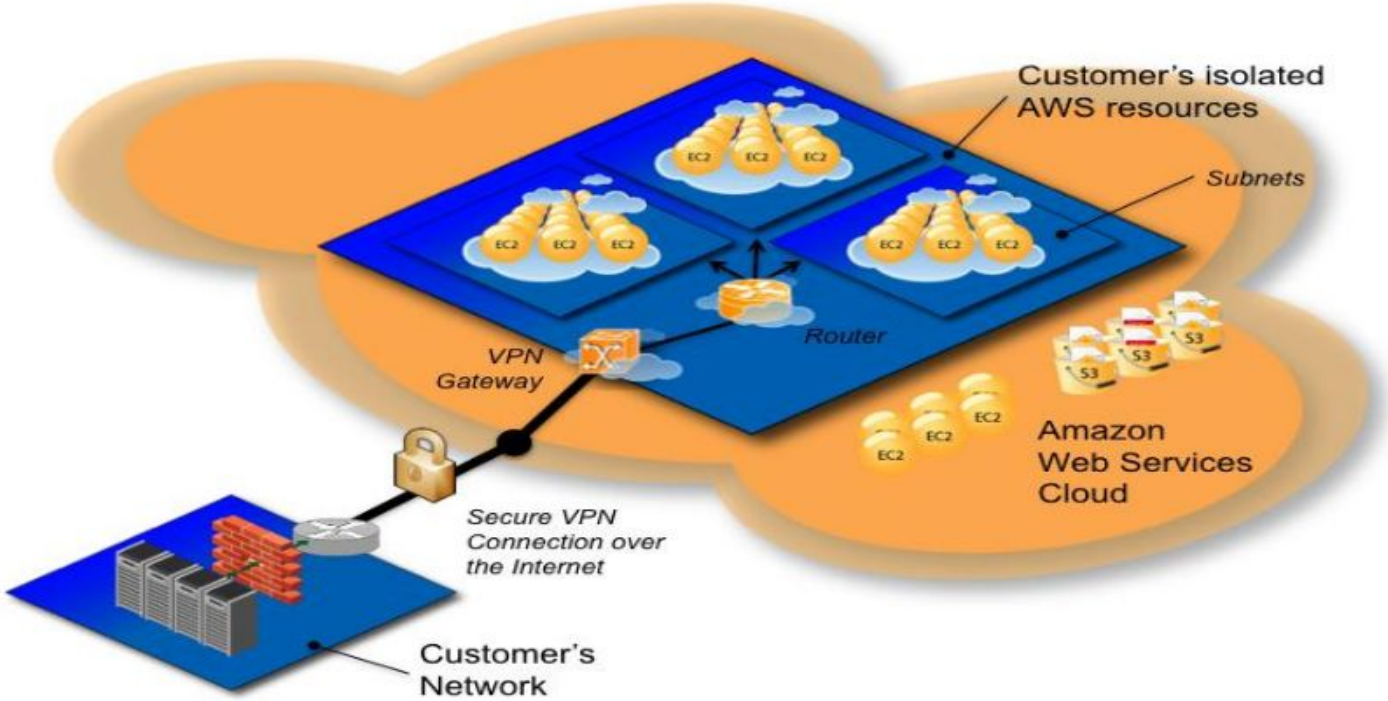
The security related features of the cloud computing products include "**advanced contextualization**" and "**network isolation**". These features allow (at least partial) implementation of the required security limitations and restrictions for VMs in a DMZ.

Big Grid Initiative – Dutch e-sciencie grid



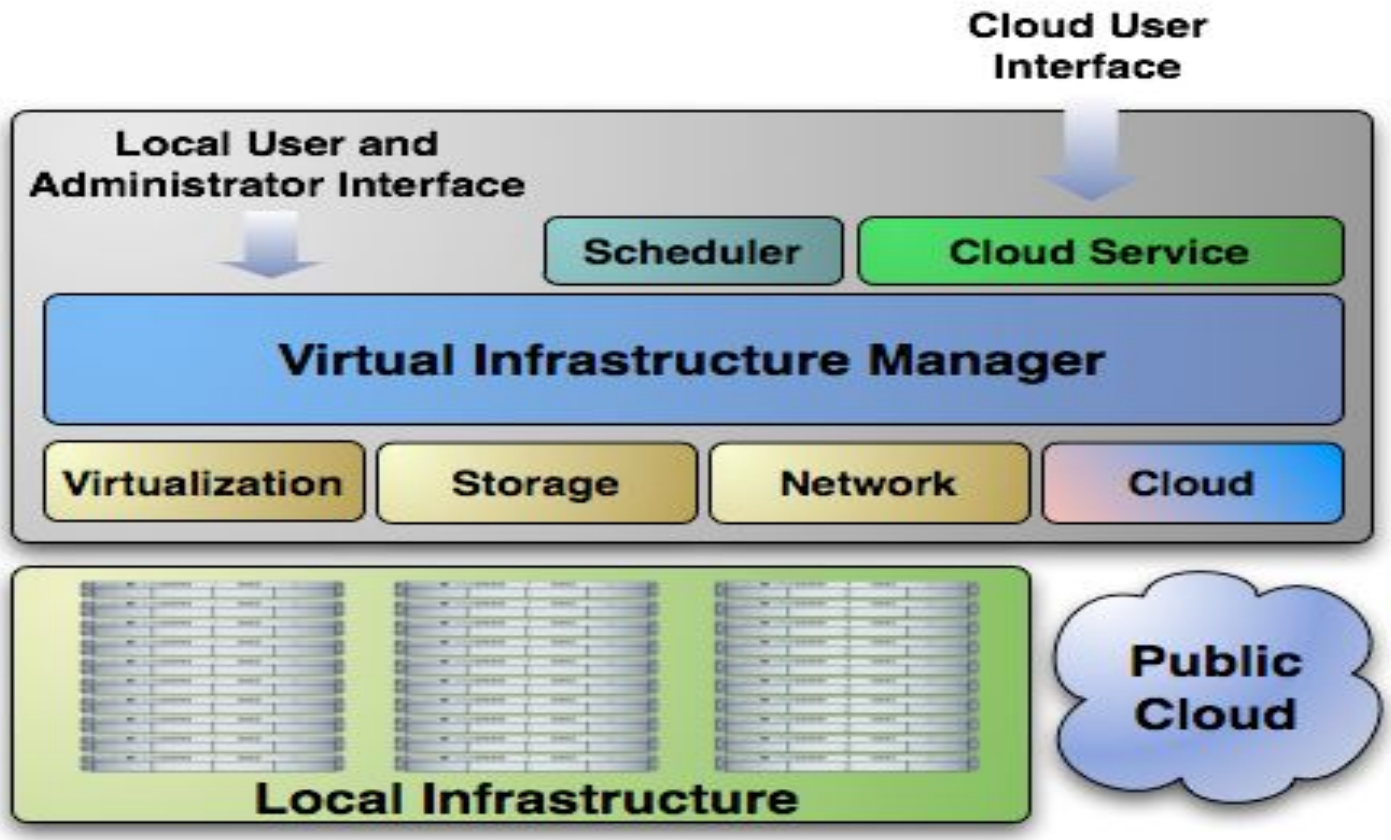
Extensión de la nube privada en un modelo IaaS

Nube privada virtual Amazon AWS



Extensión de la nube privada en un modelo IaaS

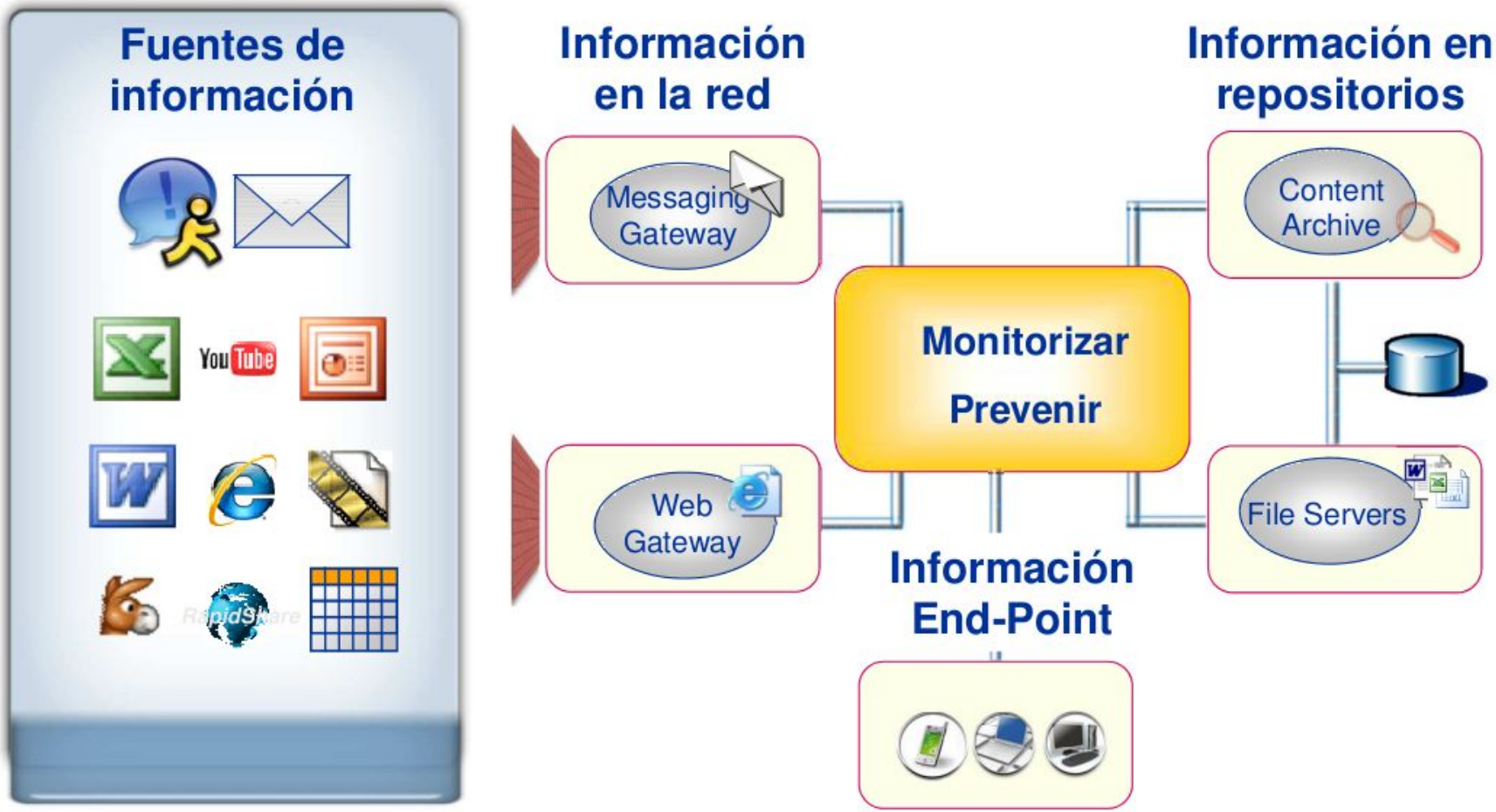
Y para mover todo esto y no morir en el intento... OpenNebula



Visibilidad en la capa de aplicación

Data Loss Prevention (DLP)

Implantación MultiPunto



Redes académicas y las nubes tipo “Comunidad”

Community cloud. The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party and may exist on premise or off premise.

¿Qué esperamos de la nube ?

Gracias por su atención!