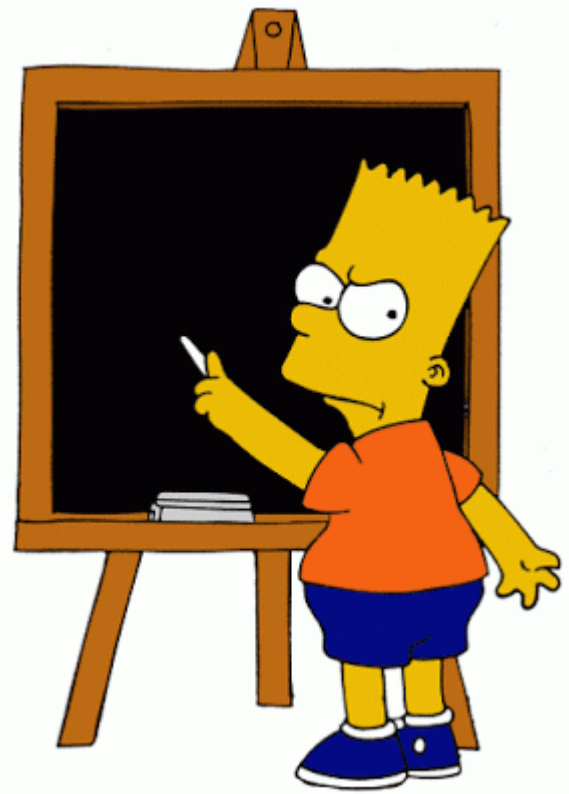
VIII JORNADAS STIC CCN-CERT

La defensa del patrimonio tecnológico frente a los ciberataques

10 y 11 de diciembre de 2014

Seguridad en las nubes



José A. Mañas

Universidad Politécnica de Madrid

jmanas@dit.upm.es

Índice

escenario

mi sistema

CSP cloud service provider(s)

"computing paradigm where the boundaries of computing will be determined by economic rationale rather than technical limits alone."
Prof. Ramnath Chellappa, 1997

pros y contras

- pros
  - alta disponibilidad
    - donde quieras
    - cuando quieras
    - economía de escala, incluso gratis
    - bueno … hay que leerse el SLA
- contras
  - todo lo demás
    - secreto, integridad, autenticidad, trazabilidad
    - propiedad intelectual
    - datos de carácter personal
    - responsabilidad(es)
    - etc.

gestión de riesgos

CCN STIC 823

seguridad--

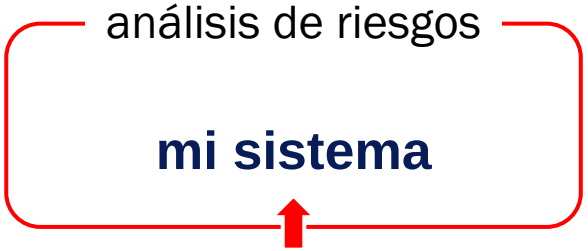
- sistemas [muy] complejos
  - amplia superficie de ataque
  - ... si es que alguien conoce la superficie de ataque
- el enemigo en casa [*multi-tenancy*]
  - la única frontera es software
  - fallos de productos y de configuración
- acceso por Internet
  - interfaz operacional
  - interfaz administrativa
- pérdida del control directo

despliegue

- públicas
  - entra quien paga
  - ventaja: economía de escala
- privada
  - sólo para mí
  - puedo ser el propietario, puedo contratarla; pero se reserva el derecho de admisión
- comunitarias
  - comunidad de interés (*birds of a feather*)
  - política de seguridad común
- híbridas

- propia
- externalizada

nube contratada



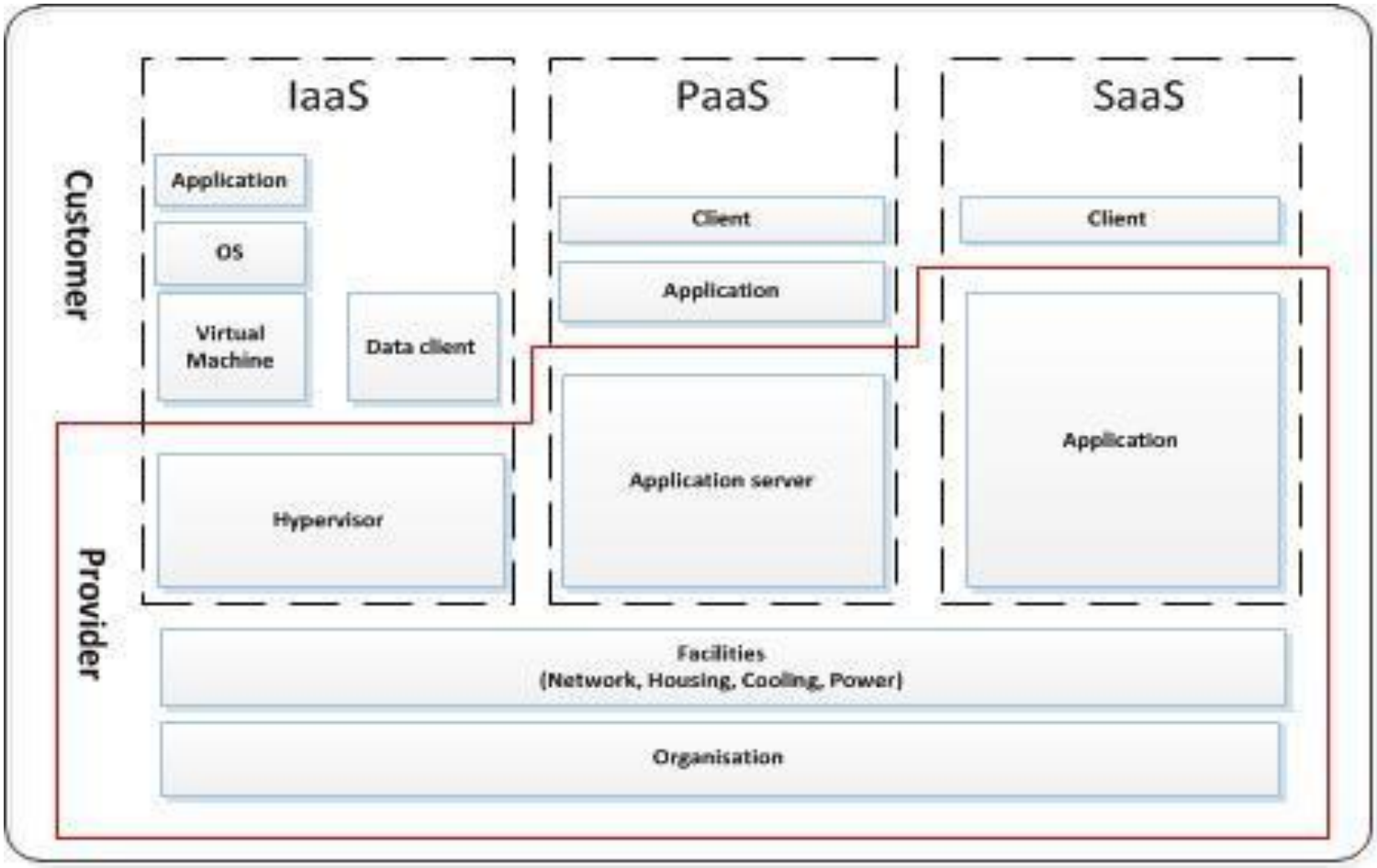
cloud service provider

opaco

- mi sistema
  - gestión técnica directa
- la nube se convierte en un agente que supone una amenaza para mi sistema

- debo proteger mi sistema frente a incidentes que ocurren en el proveedor
- pero cuyo control se me escapa
  más allá del contrato y la gestión coordinada de incidentes

activos - ¿quién es responsable de qué?



CCN STIC 823

Cloud Security Guide for SMEs, ENISA, 2014

análisis de riesgos - amenazas

- ISP
  - denegación de servicio
  - interceptación pasiva y activa
  - suplantación de identidad
    - servidor
    - cliente
- CSP
  - interrupción del servicio
  - protección interna de la información
    - personal propio
    - terceros
      - aislamiento técnico
      - acceso legal

CCN STIC 823

actividades intransferibles

- categorización del sistema (Anexo I)
- política de seguridad del organismo [org.1]
  - incluye roles, funciones y nombramientos
  - segregación de funciones [op.acc.3] **(coordinar)**
  - calificación de la información [mp.info.2]
- normativa de seguridad [org.2]
- análisis de riesgos [op.pl.1] **(coordinar)**
- **servicios externos [op.ext]**
  - proceso de autorización [org.4] **(coordinar)**
  - **gestión diaria [op.ext.2] (coordinar)**
  - **gestión de incidencias [op.exp.7] (coordinar)**
- protección de los equipos (clientes) [mp.eq.*]

CCN STIC 823

actividades que probablemente no deba hacer el CSP

- firma electrónica [mp.info.4]
- sellos de tiempo [mp.info.5]

recurrir a una tercera parte de confianza

- identificación de usuarios [op.acc.1]
- requisitos de acceso [op.acc.2]
- gestión de derechos de acceso [op.acc.4]
- mecanismo de autenticación [op.acc.5]

- registro de actividad de los usuarios [op.exp.5]
- protección de los registros de actividad [op.exp.10]
- protección de las claves criptográficas [op.exp.11]

- sistema de métricas [op.mon.2] **(coordinar)**

CCN STIC 823

comunidades por nivel

comunidad	I	C	A	T
BAJO	≤ BAJO	≤ BAJO	≤ BAJO	≤ BAJO
MEDIO	≤ MEDIO	≤ MEDIO	≤ MEDIO	≤ MEDIO
ALTO	≤ ALTO	≤ ALTO	≤ ALTO	≤ ALTO

CCN STIC 823

requisitos comunes

- El CSP debe cumplir en Anexo II en la medida en que disponga de los tipos de activos correspondientes. Esto incluye instalaciones y personal.
- En particular, el CSP elaborará un análisis de riesgos según [op.pl.1].
- Los elementos virtualizados y los elementos de virtualización se tratarán igual que los elementos físicos correspondientes a efectos de configuración, mantenimiento, reglas de seguridad y aspectos regulatorios.
- Las imágenes de los elementos virtuales se tratarán como datos con los mismos requisitos de seguridad que la información y los servicios manejados por dichos elementos virtuales.
- Debe cumplir los requisitos de la norma CCN-STIC 811 relativa a interconexión, en función de la categoría del sistema propio y del otro lado de la interconexión.

comunidad nivel BAJO

- Los componentes de seguridad del tipo DMZ, cortafuegos o agentes (proxy) no deberán residir en la misma máquina base que los componentes de producción.
- El perímetro de la red física que soporte la comunidad cumplirá los requisitos de la guía CCN-STIC-811 relativa a puntos de interconexión.
- Se registrarán todas las actuaciones de creación, traslado, activación y destrucción de elementos virtuales. Así mismo se registrará el montaje y la retirada de soportes de información, físicos o virtuales.
- Los requisitos de identificación y autenticación del administrador del hipervisor corresponderán a los de un sistema de categoría MEDIA según el ENS.

comunidad nivel MEDIO

- No se compartirán equipos base con otras comunidades.
- No se compartirá el mismo hipervisor con otras comunidades.
- La administración del hipervisor estará separada de la administración de los elementos virtualizados:
  diferentes interfaces, diferentes cuentas de administrador y diferentes administradores.
- Los requisitos de identificación y autenticación del administrador del hipervisor corresponderán a los de un sistema de categoría ALTA según el ENS.

comunidad nivel ALTO

- La red administrativa estará separada lógica (red privada virtual) o físicamente (red específica) de la red administrativa de otras comunidades.

contratación

- capacidad de negociación
  - tamaño del proveedor
  - tamaño de la parte contratante
  - ¿la AGE contra el imperio?
- ítem del contrato
  - calidad de servicio (SLA) & compensaciones
  - propiedad y confidencialidad de la información
  - cumplimiento de la normativa de protección de datos personales
  - ubicación geográfica de los datos: servidores y redes
  - **gestión de incidencias**
  - **reversibilidad & terminación**
  - **auditoría**
    - subcontratación a terceros

- **E-Mails**
  - ccn-cert@cni.es
  - info@ccn-cert.cni.es
  - ccn@cni.es
  - sondas@ccn-cert.cni.es
  - redsara@ccn-cert.cni.es
  - carmen@ccn-cert.cni.es
  - organismo.certificacion@cni.es
- **Websites**
  - www.ccn.cni.es
  - www.ccn-cert.cni.es
  - www.oc.ccn.cni.es

Síguenos en Linked in