Principales amenazas en Cloud Computing

Cristina Fernández

Records & Processes Manager

GRUPO SMS

Valor añadido a la Virtualización

Cuando se contrata la externalización de los servidores, la información debería ser monitorizada mediante la implantación de Procesos Information Governance(*), estableciendo los mecanismos de control, supervisión, seguimiento del uso y la gestión de los datos para transformarlos en un activo estratégico, gestionándolos adecuadamente y garantizando la calidad.

- Mecanismos de control
- Gestión de la información
- Salvaguarda y Seguridad

Seguridad gestionada en Cloud

• Fiabilidad, Calidad y Gestión del riesgo del servicio estableciendo una metodología aplicada y códigos de buenas prácticas de reconocido prestigio.

• Técnicas de seguridad de vigilancia tecnológica e inteligencia colectiva.

• Detección de nuevas amenazas y vulnerabilidades, permitiendo tomar acciones correctivas.

• Operación unificada, gestión y administración del servicio

Meta: mejores prácticas profesionales de sectores con riesgos equivalentes: servicios financieros, telecomunicaciones, stakeholders

“Hacia una gestión de seguridad unificada”

¿Asumimos los riesgos?

- Cumplimiento normativo, regulatorio y legal (transfronterizo)
- SLAs claros y medibles. Compensan las penalizaciones (*)?
- Disponibilidad y alternativas: Plan de Continuidad
- Seguridad de datos: donde y cómo? ⇒ probable utilización de terceros
- Costes medibles: pago por uso ⇒ ilimitado?
- Confianza en el proveedor (solidez y fiabilidad)
- Baja del servicio: eliminando rastros

(*) Ver referencia de la Cloud Security Alliance

Amenazas en Cloud Computing

Alcance

- Identificar el uso incorrecto de las tecnologías Cloud

7 "Pecados capitales" de Seguridad Cloud

- 1. Vulnerabilidad de la tecnología compartida
- 2. Suplantación de cuentas, tráfico y servicios
- 3. Pérdida o fuga de datos
- 4. Empleados que utilizan sus privilegios de forma inadecuada
- 5. Uso incorrecto del Servicio
- 6. APIs inseguras
- 7. Perdida de la trazabilidad

Fuente: "Top Threats to Cloud Computing" v1.0 -CSA

Posibles soluciones a las amenazas I

Pecados capitales / Soluciones

- Vulnerabilidad de la tecnología compartida
  - Implementar mejores prácticas en seguridad en la instalación/configuración.
  - Monitorización del entorno de actividad por cambios no autorizados.
  - Promover autentificación estable y control de accesos para el acceso administrativo y sus operaciones.
  - Controlar los SLAs para solventar la vulnerabilidad .
  - Dirigir auditorias de configuración y monitorización de vulnerabilidad.

- Suplantación de cuentas, tráfico y servicios
  - Prohibir el compartir cuentas entre usuarios y servicios .
  - Implementar al menos dos factores de autenticación siempre que sea posible.
  - Emplear proactivamente la monitorización, para detectar actividad no autorizada.
  - Entender las políticas de seguridad de los SLAs del proveedor cloud.

- Pérdida o fuga de datos
  - Implementar controles de acceso y APIs robustas.
  - Encriptar y proteger la integridad de los datos en su tránsito.
  - Analizar la protección de los datos tanto en el diseño como en la ejecución.
  - Desarrollar sistemas de generación de claves robustas, almacenamiento, gestión y prácticas de destrucción.
  - Solicitar a los proveedores mediante contrato los medios necesarios antes de iniciar el servicio, así como las estrategias de backup y conservación.

- Empleados que utilizan sus privilegios de forma inadecuada
  - Implementar una política de gestión del cambio firme y comprensible para evaluiación de empledos
  - Especificación de los perfiles de los recursos como parte del contrato.
  - Requerir transparencia en la seguridad de la información y prácticas de gestión, así como sus informes de cumplimiento.
  - Determinar la violación de seguridad en los procesos de notificación.

Fuente: "Top Threats to Cloud Computing" v1.0 -CSA

Posibles soluciones a las amenazas II

Pecados capitales / Soluciones

Uso incorrecto del Servicio
- Registros iniciales y procesos de validación rígidos y estables.
- Supervisión de la coordinación y monitorización de posibles fraudes del servicio.
- Interpretación del tráfico de la red de cliente.
- Monitorización de listas negras públicas para bloqueo de redes propias.

APIs inseguras
- Analizar el modelo de seguridad de los interfaces de los proveedores cloud.
- Asegurar el control de acceso encriptado y robusto.
- Entender la cadena de dependencia asociada al API.

Perdida de la trazabilidad:
- Divulgación de datos y logs aplicables.
- Parcial/total difusión de los detalles de infraestructura (sw corrector, firewalls, etc.).
- Monitorización y alertas de la información necesaria.

Fuente: "Top Threats to Cloud Computing" v1.0 -CSA

Universo Normativo en la Nube

Comités nacionales

AENOR → UNE (España)

(Alemania)

(Francia)

(Gran Bretaña)

...

European Telecommunications Standards Institute (TIC)

International Electrotechnical Commission

Universo regulatorio II

GRUPO SMS participa en diferentes organismos de normalización y Comités Técnicos donde se definen y publican estándares a nivel mundial:

INTERNACIONAL

- ISO (INTERNATIONAL STANDARDS ORGANIZATION):
  - -TC46SC11 “Gestión Documental” : ISO 30300, 30301, 30302, etc.
  - - JTC1/SC38 “Plataformas de aplicaciones distribuidas y servicios”: normas ISO - **Cloud**
- ETSI (European Telecommunications Standards Institute) conjuntamente con CEN (European Committee for Standardisation)/CENELEC (European Committee for Electrotechnical Standardization) especificamente en el grupo de trabajo que publica normativa **Cloud**.
- BSI (BRITISH STANDARD INSTITUTION): comunidad conocimiento - Continuidad de Negocio
- NORMAPME (European Office of Crafts Trades and Small and Medium-sized Enterprises for Standardisation), colaboración en los Comités arriba referenciados.

NACIONAL

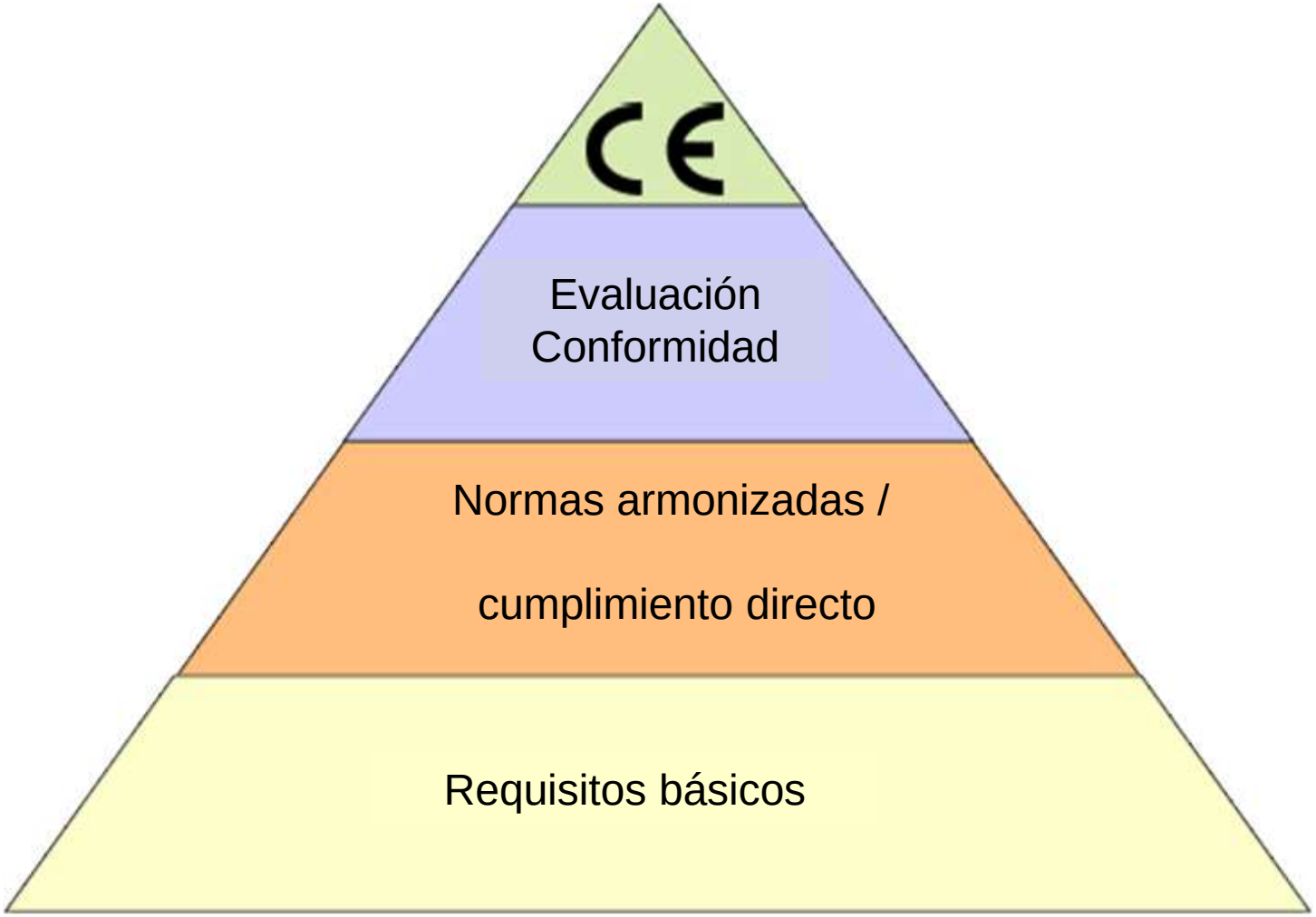
- Ministerio de Industria/ Mº de Cultura: asistencia a reuniones, jornadas, etc. sobre la Sociedad de Telecomunicaciones e Información española, y presentación de Proyectos I+D.
- AENOR (ASOCIACIÓN ESPAÑOLA DE NORMALIZACIÓN Y CERTIFICACIÓN):
  - -CTN50/SC1: Comité Técnico sobre Gestión de Documentos y Aplicaciones: traducción de normas ISO (a UNE) y elaboración y adopción de estándares propios.
  - -CTN71: CT Tecnología de la Información, Seguridad en **Cloud**
- CONETIC (Confederacion Española de Empresas de las TICs), financiación proyectos I+D.

Ampliamos nuestra labor normativa con la participación activa en distintos foros especializados tanto de Cloud como de los distintos Sistemas de Gestión e Information Governance.

Sistemas de Gestión y Funciones de Negocio

MARCO DE GOBIERNO DE UN SERVICIO GENÉRICO

Tendencias Cloud Computing



Registro de Seguridad, Fiabilidad y Aseguramiento

Control Area	Control ID	Control Specification	Control Notes	Architectural Relevance						Corp Gov Relevance	Cloud Service Delivery Model Applicability		
				Phys	Network	Compute	Storage	App	Data		SaaS	PaaS	IaaS
Data Governance - Ownership / Stewardship	DG-01	All data shall be designated with stewardship with assigned responsibilities defined, documented and communicated.				X	X	X	X	X	X	X	X
Data Governance - Classification	DG-02	Data, and objects containing data, shall be assigned a classification based on data type, jurisdiction of origin, jurisdiction domiciled, context, legal constraints, contractual constraints, value, sensitivity, criticality to the organization and third party obligation for retention and prevention of unauthorized disclosure or misuse.				X	X	X	X	X	X	X	X
Data Governance - Handling / Labeling / Security Policy	DG-03	Polices and procedures shall be established for labeling, handling and security of data and objects which contain data. Mechanisms for				X	X	X	X	X	X	X	X

Consensus Assessments Initiative Questionnaire v1.1

Control Group	CGID	CID	Consensus Assessment Questions
		IS-34.2	Do you have a capability to detect attacks which target the virtual infrastructure directly (ex. shimming, Blue Pill, Hyper jumping, etc.)?
		IS-34.3	Are attacks which target the virtual infrastructure prevented with technical controls?
Legal			
Nondisclosure Agreements	LG-01	LG-01.1	Are requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details identified, documented and reviewed at planned intervals?
Third Party Agreements	LG-02	LG-02.1	Do you select and monitor outsourced providers in compliance with laws in the country where the data is processed and stored and transmitted?
		LG-02.2	Do you select and monitor outsourced providers in compliance with laws in the country where the data originates?
		LG-02.3	Does legal counsel review all third party agreements?
Operations Management			
Policy	OP-01	OP-01.1	Are policies and procedures established and made available for all personnel to adequately support services operations roles?

Fuente: "Consensus Assessments Initiative Questionnaire v1.1CSA

Esquema Conceptual de un SLA

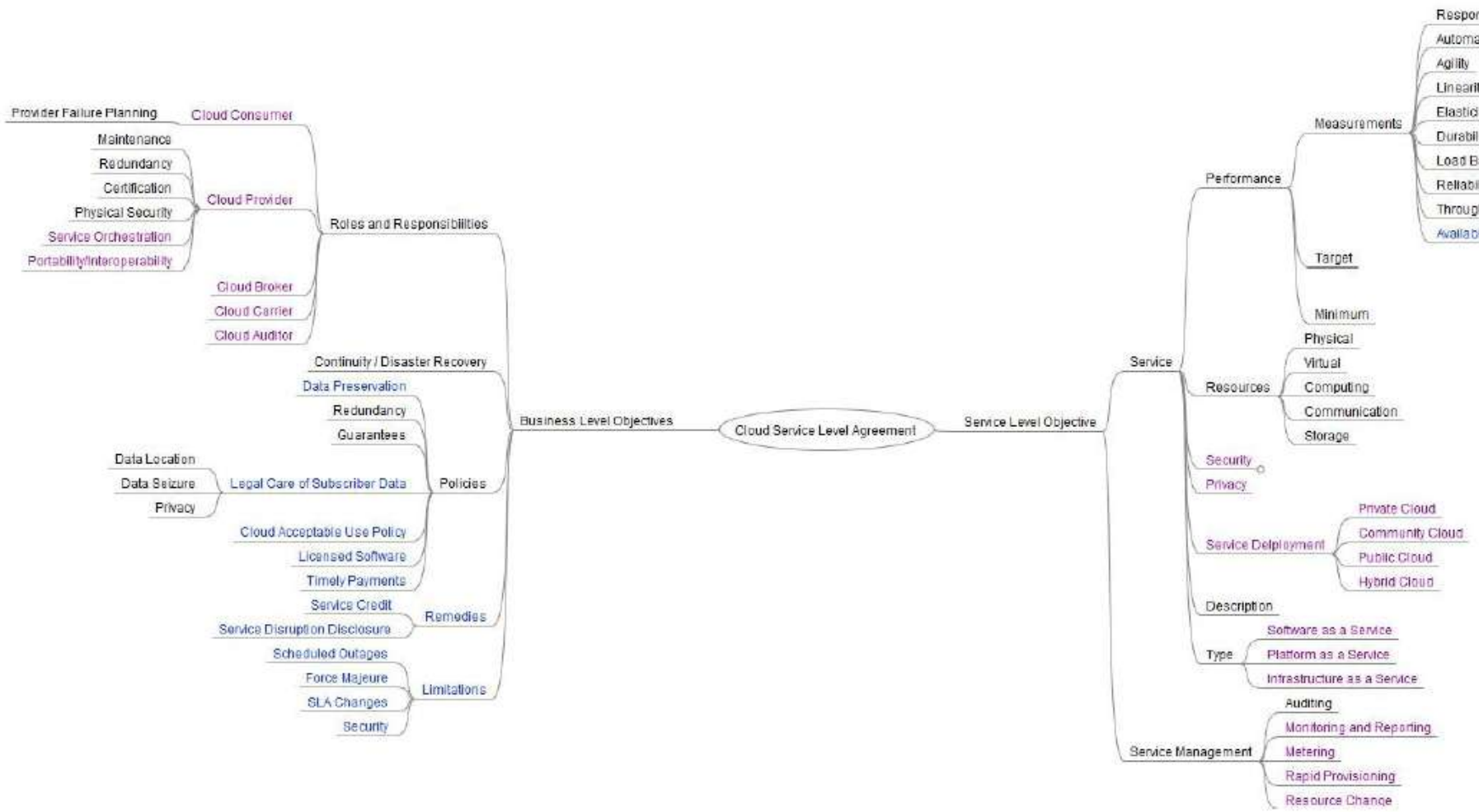


Table 10: Cloud-Specific SLA Concepts Mindmap

Fuente: Security Guidance for Critical Areas of Focus in Cloud Computing V2.1 - CSA

Proceso Documental de los requisitos técnicos Cloud

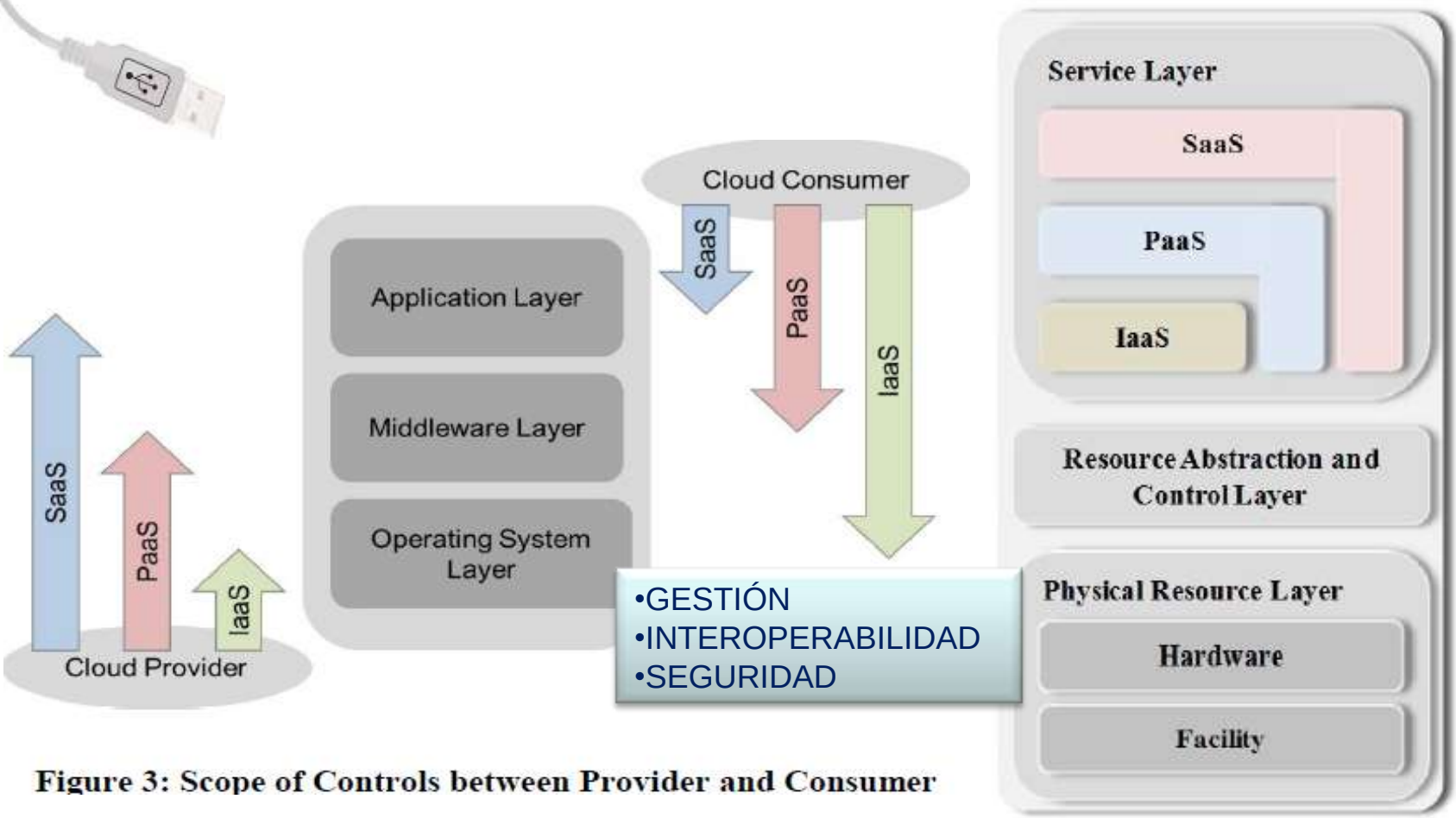


Figure 3: Scope of Controls between Provider and Consumer

Figure 4: Cloud Provider - Service Orchestration

Fuente: Security Guidance for Critical Areas of Focus in Cloud Computing V2.1 - CSA

DISPONIBILIDAD CLOUD

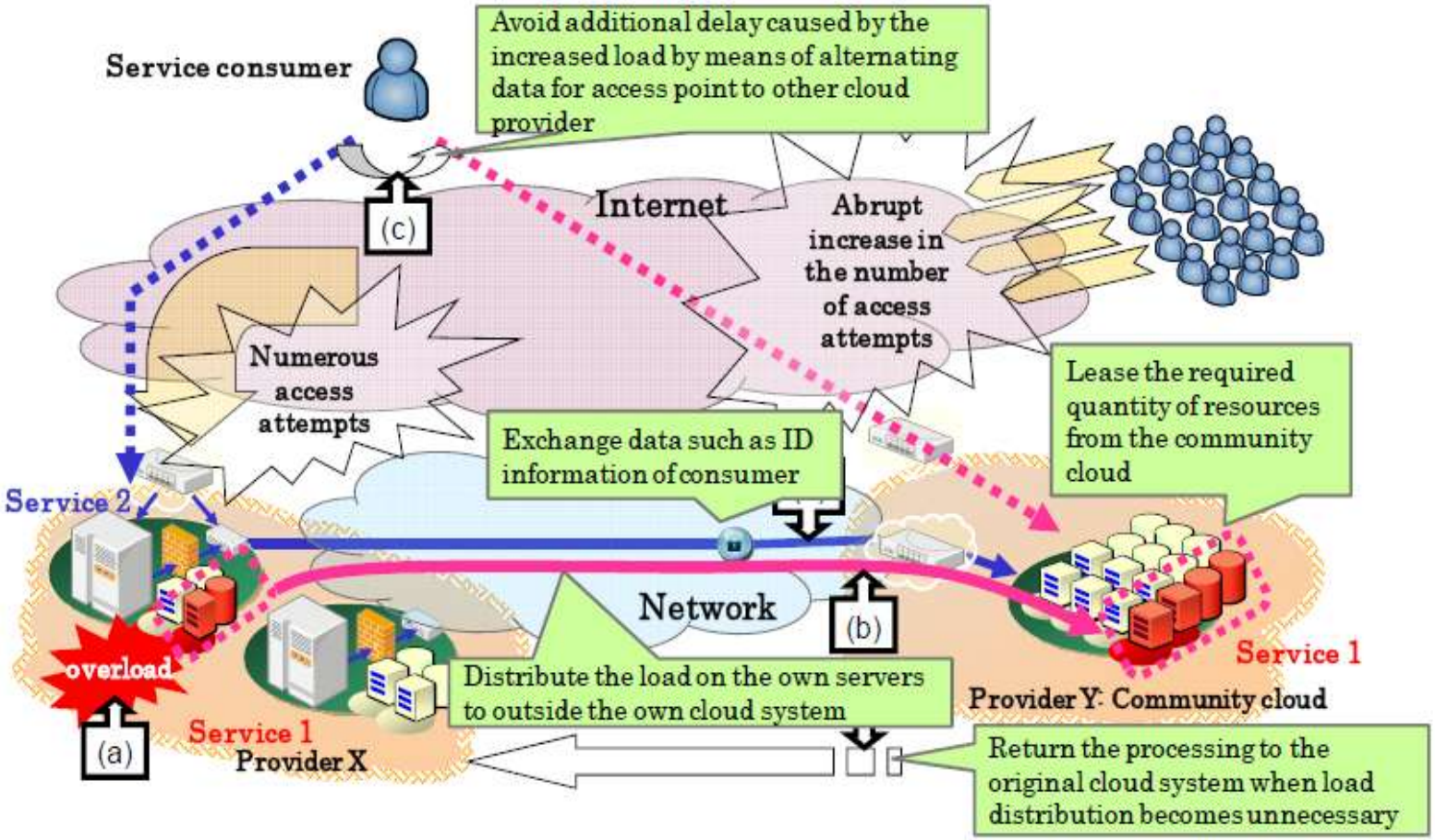
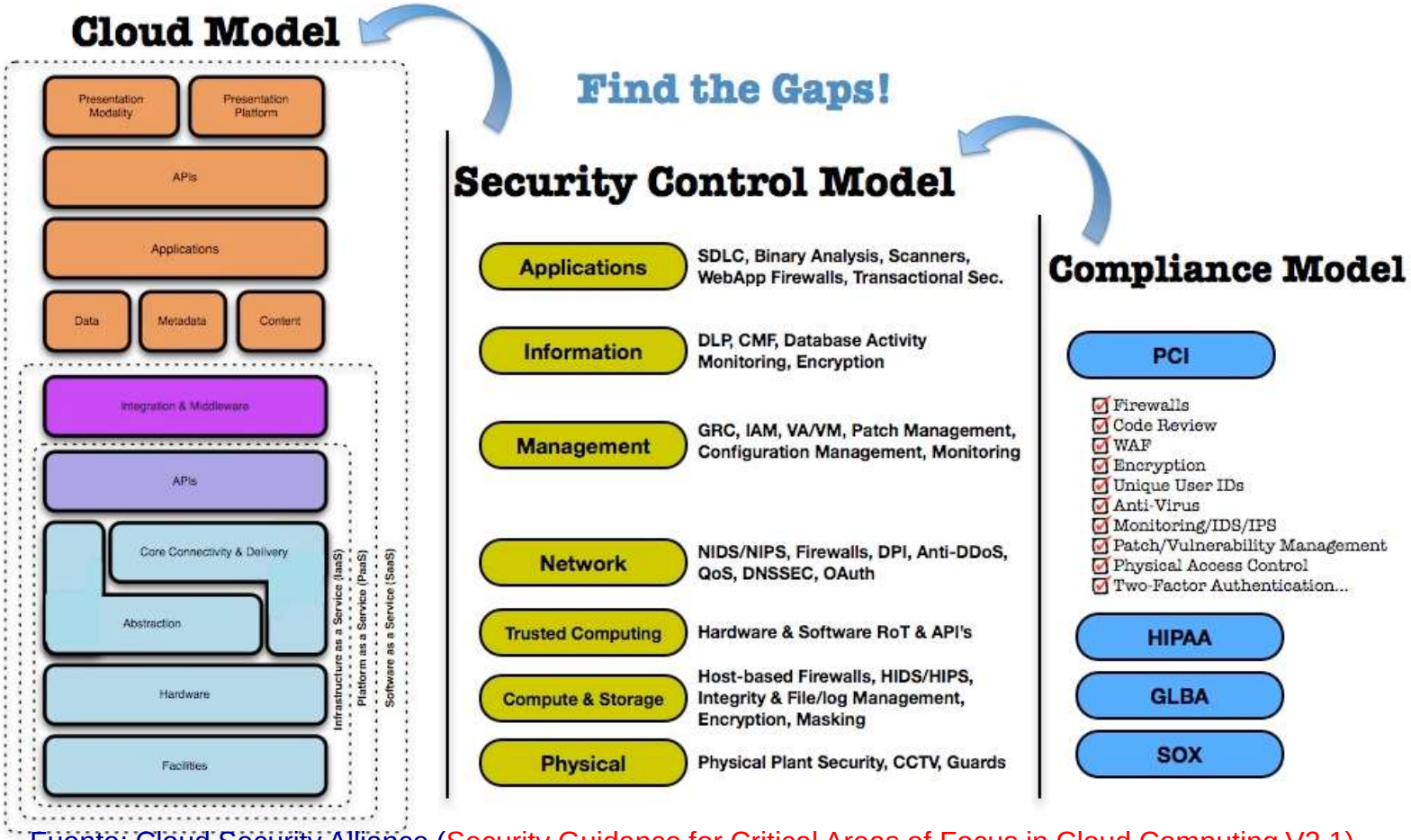


Fig. 9 Procedures for guaranteeing performance against an abrupt increase of load

Fuente: Security Guidance for Critical Areas of Focus in Cloud Computing V2.1 - CSA

Mapeo Sistema Cloud/Controles IG



Fuente: Cloud Security Alliance (Security Guidance for Critical Areas of Focus in Cloud Computing V2.1)

CLAVES A TENER EN CUENTA

• **AUTENCIDAD/METODOLOGÍA:** TRANSPARENCIA Y HONESTIDAD CON NUESTROS CLIENTES

ESTABLECIENDO UN MARCO DE GOBIERNO QUE SE TRADUZCA EN LA PRESENTACIÓN DE SLAs Y CUADROS DE MANDO CON ITEMS MÍNIMOS (DISPONIBILIDAD, RENDIMIENTO Y SEGURIDAD) INDEPENDIENTEMENTE DEL SERVICIO QUE SE OFREZCA.

• **INNOVACIÓN/CUALIFICACIÓN**: ESPECIALIZACIÓN EN SECTORES Y A CUALQUIER ESCALA

✓DISCURSO COMÚN SOBRE NUESTRA IMPLICACIÓN EN LA DEFINICIÓN DE NORMAS EN LOS ORGANISMOS DE NORMALIZACIÓN MAS EMBLEMÁTICOS, INCIDIENDO EN QUE ESPAÑA ESTÁ EN LA VANGUARDIA.

✓NO NOS HEMOS ACOMODADO EN NUESTRA ZONA DE CONFORT, SIENDO REACTIVOS.

•**ANTICIPACIÓN/ADAPTACIÓN**: REINVENTARSE, ADQUIRIENDO UNA ESTRATEGIA PROACTIVA

EN SERVICIOS DE CERTIFICACIÓN DE SISTEMAS DE GESTIÓN (EJEMPLO ISO 30300= OPORTUNIDAD DE PASAR DEL PLANO OPERATIVO AL ESTRATÉGICO), DISPONER DE PROYECTOS ESCALABLES A NIVEL INTERNACIONAL Y CONTAR CON UN EQUIPO HUMANO MULTIDISCIPLINAR.

• **AFINIDAD/COMPETENCIA**: OFRECER SERVICIOS POR SECTORES

LA DEBILIDAD DE NUESTRA COMPETENCIA ES NUESTRA ***FORTALEZA***, Y EL ELEMENTO DIFERENCIADOR QUE NOS PUEDE AYUDAR A GANAR LA CONFIANZA DE UN CLIENTE POTENCIAL.

Referencias

Enlaces de interés Riesgos:

ENISA - Evaluación de Riesgos Cloud Computing
http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment

Foro Jericho – Esquema de autoevaluación
https://www.opengroup.org/jericho/self-assessment.htmCarnegie

Mellon OCTAVE – Evaluación de Riesgos
http://www.cert.org/octave/Microsoft

STRIDE – Modelo de amenazas
http://msdn.microsoft.com/en-us/magazine/cc163519.aspxFactor

Análisis de Gestión de Riesgos (FAIR)
http://fairwiki.riskmanagementinsight.com/

Modelo de Madurez Aseguramiento
http://common-assurance.com/BITS

Evaluación compartida
http://www.sharedassessments.org/

Enlaces de interés “Information Governance“- GRUPO SMS:

http://blog.grupo-sms.com/category/normalizacion/

http://www.linkedin.com/groups?gid=2103672&trk=myg_ugrp_ovr

LA GESTIÓN DE LA INFORMACIÓN ES UN PROCESO CONTINUO,

¡ESTÉS O NO EN LA NUBE!

MUCHAS GRACIAS POR TU ATENCIÓN

Cristina Fernández
Records & Processes Manager
cfernandezf@grupo-sms.com
Tfs. 91 203 84 83/639049313
GRUPO SMS

ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD
AEC
COMITÉ DE LOS SISTEMAS Y LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

CSTIC 2012

Dominando los riesgos se compite mejor

18 de Septiembre de 2012 #CSTIC12

Patrocinadores

Caelum

SEI Partner | Carnegie Mellon

GOBIERNO DE ESPAÑA

MINISTERIO DE DEFENSA

Organizador

ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD

AEC

COMITÉ DE LOS SISTEMAS Y LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

Patronos de la AEC:

Aena

aena aeropuertos

AENOR

fundación enresa

renfe

Colaboradores

grupo SMS

DiCe

UNIVERSIDAD PONTIFICIA ICAI ICADE COMILLAS MADRID

Cooperadores

ati

CONCITI.org