

VIII Congreso

Académico Internacional
en Gobierno y Gestión del Servicio de TI

Martes 28 de Mayo 2013 (URJC - Madrid)



Universidad
Rey Juan Carlos

itSMF
E S P A Ñ A



Gestión del Cumplimiento regulatorio en el Cloud Computing como ventaja competitiva

Juan M. Pulpillo Fernández, Pulpillo & Counselors

**Formando profesionales:
de la sociedad de
la información
a la sociedad de
los servicios**



Speaker Bio & Company Information

- ❖ Abogado y consultor IT con más de 12 años de experiencia en este sector.
- ❖ Responsable del Grupo de Trabajo de Aspectos normativos de la Comisión de Cloud Computing de eticom.
- ❖ Profesor de Masters en la uc3m y ESNE.



- ❖ “Ofrecemos soluciones profesionales avanzadas a la altura de las necesidades, a través de una colaboración estrecha con el cliente, comprometida y fundamentada en la calidad y en la profesionalidad unida a una visión del negocio y del compliance global e internacional”.

Pulillo & Counselors

Privacy / Data Protection & Information Security Genome & Law Conveyancing & Law

Compliance IT Services e-Business & Law e-Commerce & Law Training

IT / ICT & Law Public & Law Marketing & Law Audiovisual & Law

¿Qué vamos a ver?

- ❖ Visión: El Cloud Computing como nuevo modelo de negocio
- ❖ Problemáticas
- ❖ Compliance como parte imprescindible en el Gobierno TI
- ❖ Aspectos básicos de Compliance para obtener resultados excelentes en el Gobierno TI
- ❖ Metodología y soluciones para integrar el Compliance en el Gobierno TI
- ❖ Conclusiones



Visión

- ❖ El Cloud Computing se configura como un nuevo modelo de negocio en la que se producen grandes tensiones entre la empresa (CEO-CIO) y los departamentos legales que asesoran la actividad empresarial.



- ❖ Este nuevo modelo de negocio se configura como una excelente oportunidad de negocio para las empresas que sepan posicionarse y adaptarse a un entorno global, integrado y cambiante y aprovechar la diversidad de marcos normativos.

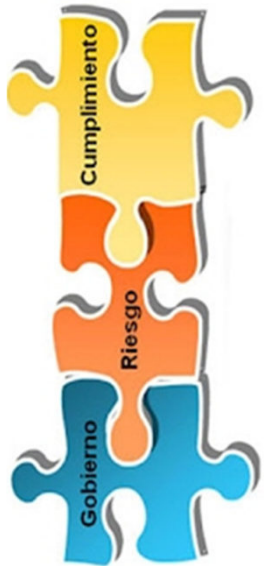
Visión

- ❖ Ante esta situación del mercado y de los marcos normativos existentes se abre una posibilidad muy interesante de negocio para las empresas de la Unión Europea con el modelo de Cloud Computing y teniendo como destinatarios de dichos servicios a las empresas y administraciones públicas de la propia Unión Europea e incluso de fuera de la propia Unión.



Visión

- ❖ Los elementos comunes al concepto de Cloud Computing son:
 - Servicios TI bajo demanda (recursos, software y/o datos)
 - A través de redes de telecomunicaciones



Problemáticas

❖ Realidades:

- Estudio de Vanson Bourne y Vmware presentado el 22/05/2013

Los responsables de TI reconocen las ventajas de las soluciones cloud, pero a la mitad le inquieta el riesgo que puede suponer para la seguridad de la compañía el hecho de que no sean soluciones aprobadas por el departamento de TI.

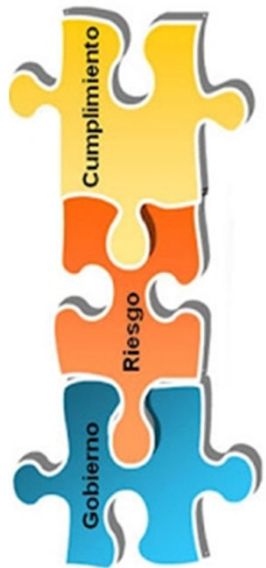
¿Sólo le debe preocupar el departamento TI?



Problemáticas

❖ Realidades:

- El estudio exploró también la visión y las opiniones de 3.000 trabajadores en oficinas de toda Europa para saber cómo utilizan los servicios y productos en la nube para trabajar con eficacia. Casi la mitad de estos trabajadores (45%) utilizarían o comprarían servicios en la nube sin permiso para hacer el trabajo y más de un tercio (36%) ya lo han hecho. Los empleados con conocimientos tecnológicos son los más propensos a utilizar servicios en la nube a escondidas. Así, el 58% admitió que, dado el caso, utilizarían estos servicios sin permiso del departamento de TI.



Problemáticas

❖ Realidades:

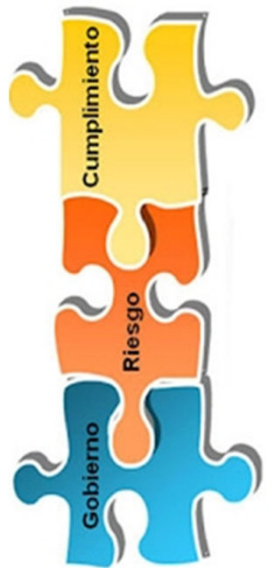
- Casi la mitad de los Responsables de TI encuestados (48%) también ha asegurado que aunque el gasto en servicios en la nube sin declarar presenta sus ventajas, también incrementa el nivel de amenazas a la seguridad de la compañía, al surgir un conflicto entre la creciente demanda de flexibilidad informática y la necesidad de mantener el control y reducir la carga de la gestión.



¿Sólo le debe preocupar el departamento TI?

Problemáticas

- ❖ ¿Dónde está mi información?
- ❖ ¿Dónde están mis servicios?
- ❖ ¿Qué hago si pasa algo? A quién me dirijo? Plazos de resolución? Costes aditivos y judiciales? Usos del lugar de establecimiento-usos del lugar de explotación-usos del lugar de desarrollo-usos del lugar del consumidor/cliente-usos del lugar de prestación.
- ❖ ¿Qué normativa me aplica? ¿qué consecuencias tiene?



Problemáticas

- ❖ Estado del arte: Fuente Informe Enisa
 - Más del 50 % de los proveedores de servicios Cloud no se adhieren a standares.
 - Sólo el 11 % de las empresas mantienen actualizados o formalizan SLA´s con sus proveedores de Cloud.
 - De las empresas que formalizan SLA, sólo en un 20% se involucra al departamento legal, en el 80% sólo se involucra el departamento TI.



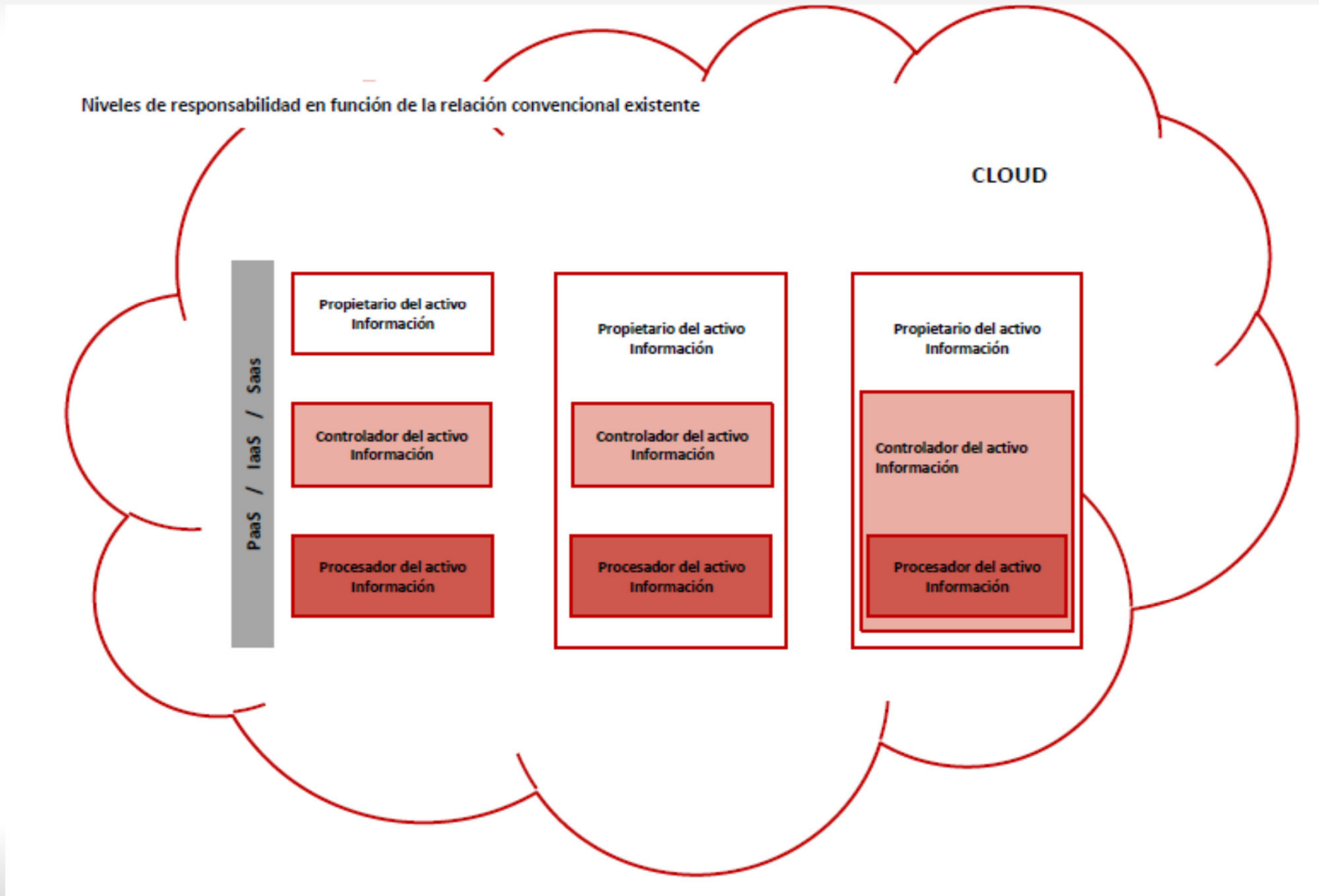
Problemáticas

❖ Estado del arte: Fuente Informe Enisa

- De las empresas que formalizan SLA, en más del 55 % no se clasifican los incidentes de seguridad.
- De las empresas que formalizan SLA, sólo el 12 % testean la portabilidad de la información.
- De las empresas que formalizan SLA, sólo el 15% reciben reports del funcionamiento del servicio.

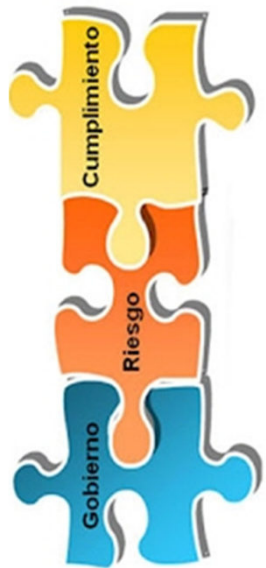


Compliance como parte imprescindible en el Gobierno TI



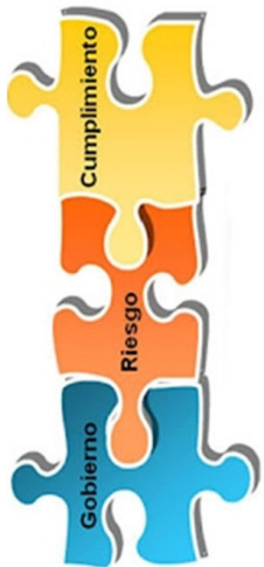
Aspectos básicos de Compliance para obtener resultados excelentes en el Gobierno TI

- ❖ Las grandes preocupaciones de las empresas (usuarias, o que van a adoptar) de servicios de Cloud Computing son:
 - la seguridad y confidencialidad de la información,
 - la pérdida o transferencia de control de procesos,
 - la dependencia del proveedor (neutralidad-retorno de la información-interoperabilidad),
 - la disponibilidad de la información y/o del servicio,
 - la integridad de la información,



Aspectos básicos de Compliance para obtener resultados excelentes en el Gobierno TI

- ❖ Las grandes preocupaciones de las empresas (usuarias, o que van a adoptar) de servicios de Cloud Computing son:
 - la responsabilidad del proveedor (cadenas de subcontratación, deslocalización, nivel del servicio, negligencia profesional, transferencia de datos, legislación aplicable, limitaciones de responsabilidad –common law vs continental law, continuidad del servicio, cumplimiento normativo, etc),
 - la dificultad de recuperar la información en caso de resolución o extinción del servicio de manera adecuada y en su totalidad, manteniendo la confidencialidad de la misma y
 - la eliminación total de dicha información como obligación postcontractual.



Compliance como parte imprescindible en el Gobierno TI

- ❖ En este orden de cosas, a la hora de tomar decisiones acerca de una posible migración a servicios Cloud Computing deberemos tener en cuenta si el Cloud se encuentra en España, en territorio UE o Fuera de territorio UE y los servicios que vamos a utilizar para valorar los requerimientos e implicaciones normativas de tal decisión.



Aspectos básicos de Compliance para obtener resultados excelentes en el Gobierno TI

- ❖ Diferenciaremos para cada ámbito normativo cuatro tipos de Cloud Computing: Uno
 - Cloud Español: Servicios Cloud localizados en España.



Como regla general, en este tipo de relación Cloud, en principio atenderemos a la propia normativa española. Salvo que en los contratos de servicios se establezca otra cosa.

Aspectos básicos de Compliance para obtener resultados excelentes en el Gobierno TI

- ❖ Diferenciaremos para cada ámbito normativo cuatro tipos de Cloud Computing: Dos
 - Cloud Europeo: Servicios Cloud localizados en territorio europeo.



Como regla general, en este tipo de relación Cloud, atenderemos a la normativa estatal del territorio del cliente y de localización de los servicios Cloud y a la normativa europea atendiendo a los supuestos que puedan producirse. Salvo que en los contratos de servicios se establezca otra cosa.

Aspectos básicos de Compliance para obtener resultados excelentes en el Gobierno TI

- ❖ Diferenciaremos para cada ámbito normativo cuatro tipos de Cloud Computing: Tres
 - Cloud No Europeo Homogéneo: Servicios Cloud localizados en territorio no europeo pero con normativas homogéneas a la europea.



Como regla general, en este tipo de relación Cloud, atenderemos a la normativa estatal del territorio del cliente y de localización de los servicios Cloud y a la normativa europea atendiendo a los supuestos que puedan producirse. Salvo que en los contratos de servicios se establezca otra cosa.

Aspectos básicos de Compliance para obtener resultados excelentes en el Gobierno TI

- ❖ Diferenciaremos para cada ámbito normativo cuatro tipos de Cloud Computing: Cuatro
 - Cloud No Europeo No Homogéneo: Servicios Cloud localizados en territorio no europeo pero con normativas no homogéneas a la europea.

Como regla general, en este tipo de relación Cloud, atenderemos a la normativa estatal del territorio del cliente y de localización de los servicios Cloud y a la normativa europea atendiendo a los supuestos que puedan producirse. Salvo que en los contratos de servicios se establezca otra cosa.



Compliance como parte imprescindible en el Gobierno TI

❖ **Precio Vs Servicios Vs Seguridad Vs**

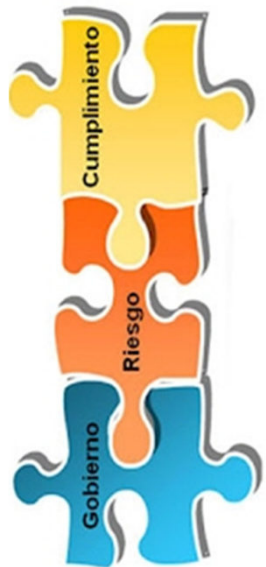
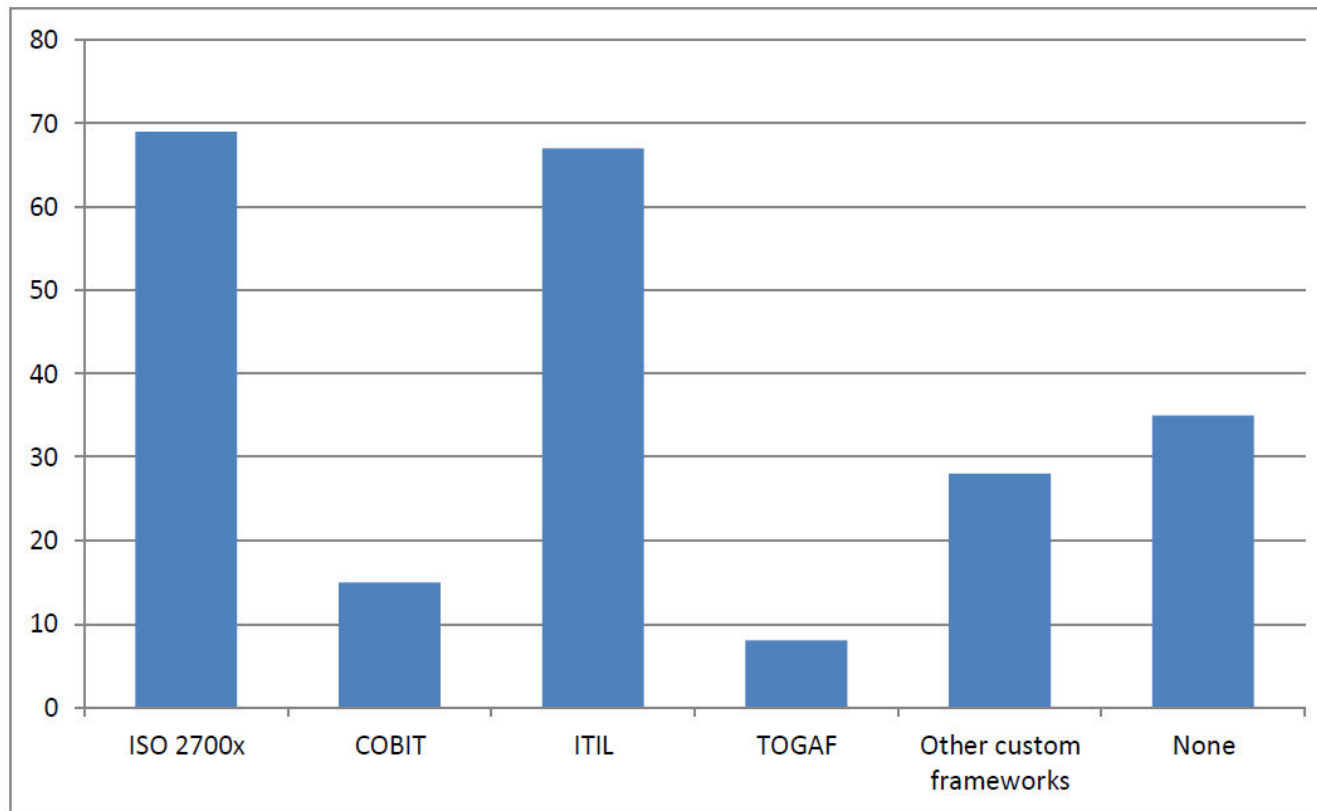
Regulación Vs Eficiencia Vs Confianza =

Equilibrio (**Gobernanza IT**)



Metodología y soluciones para integrar el Compliance en el Gobierno TI

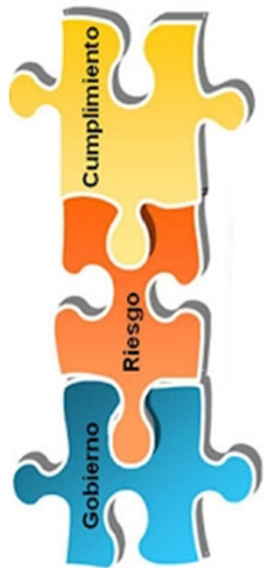
1.3 Governance frameworks and security standards used (number of respondents)



Certificaciones Vs Compliance Vs Due Dilligence una buena opción para Gobierno TI: Representaciones y Garantías

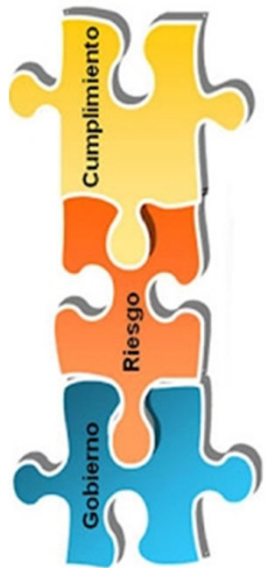
Conclusiones

- ❖ El Cloud Computing se configura como un nuevo modelo de negocio en el que se producen grandes tensiones entre la empresa (CEO-CIO) y los departamentos legales que asesoran la actividad empresarial. Encontrar el equilibrio mediante un trabajo coordinado y complementario es garantía de éxito.
- ❖ Necesidad de la existencia de una Asistencia especializada de Compliance en las empresas que presten servicio en el Cloud Computing o tengan servicios en el Cloud Computing.



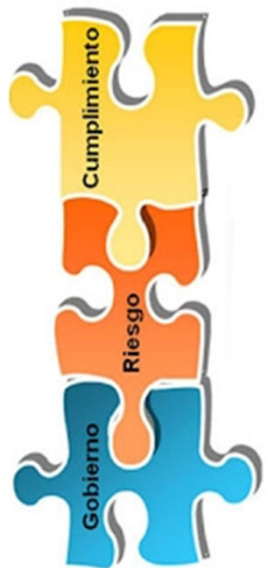
Conclusiones

- ❖ Necesidad de establecer Corporate rules y Cloud Computing Sector Rules and Agreements promovidas por el sector, la administración pública y las propias empresas.
- ❖ Necesidad de que se promuevan Acuerdos internacionales sobre Cloud Computing.
- ❖ Necesidad de que la regulación se ajuste a las necesidades del mercado para propiciar un mercado nacional saludable para el Cloud Computing, que se traduce necesariamente en un mercado que está en armonía con las leyes de otros países de una manera que permite el flujo de datos sin problemas a través de las fronteras.



Conclusiones

- ❖ Establecer vías de asesoramiento experto para dar a conocer a los CEO y CIO de empresas que realizan negocios en Cloud las reglas, normas o cláusulas de los contratos en uso para así poder llevar a cabo un buen trato que favorezca a ambas partes. Promover la cultura de los SLA y ANS.
- ❖ Actuar de manera razonable con nuestros clientes para hacerles reflexionar acerca de que un uso y abuso del Cloud Computing pone en riesgo a la organización y por ende puede hacer disminuir la actividad empresarial o, en el peor de los casos, la eliminación de tejido productivo.



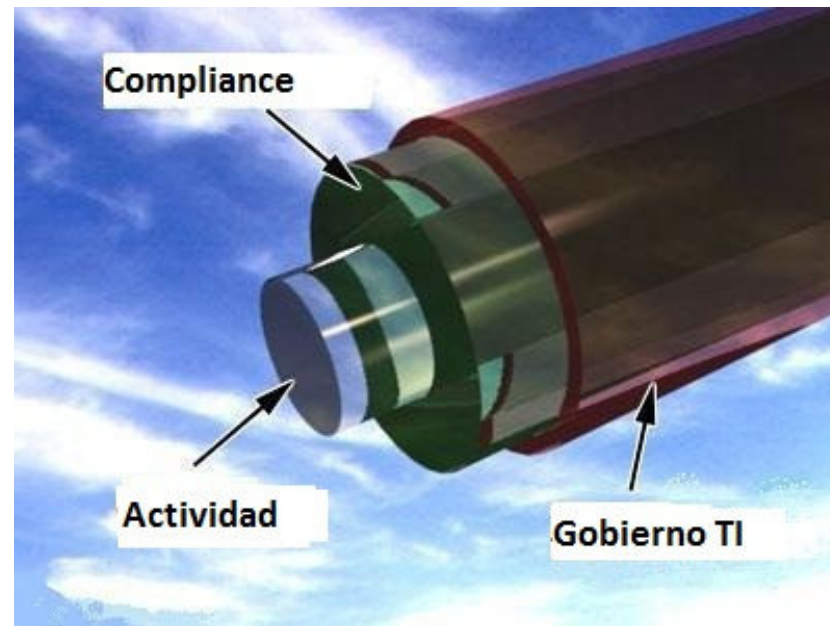
Conclusiones

- ❖ Tomar el Compliance, en el marco normativo europeo, como una ventaja competitiva frente a los proveedores de servicios de Cloud extracomunitarios.



Compliance IT & Risk
evaluate & Privacy &
New regulations

Gobierno TI
multidisciplinar más
que nunca



¡ Muchas gracias !



Contact details:

Juan M Pulpillo

- Email: legal@legal-itc.com
- Web: <http://www.legal-itc.com>
- Twitter: [@derechotic](https://twitter.com/derechotic)
- Blog: <http://derechotic.wordpress.com/>

Pulpillo & Counselors