

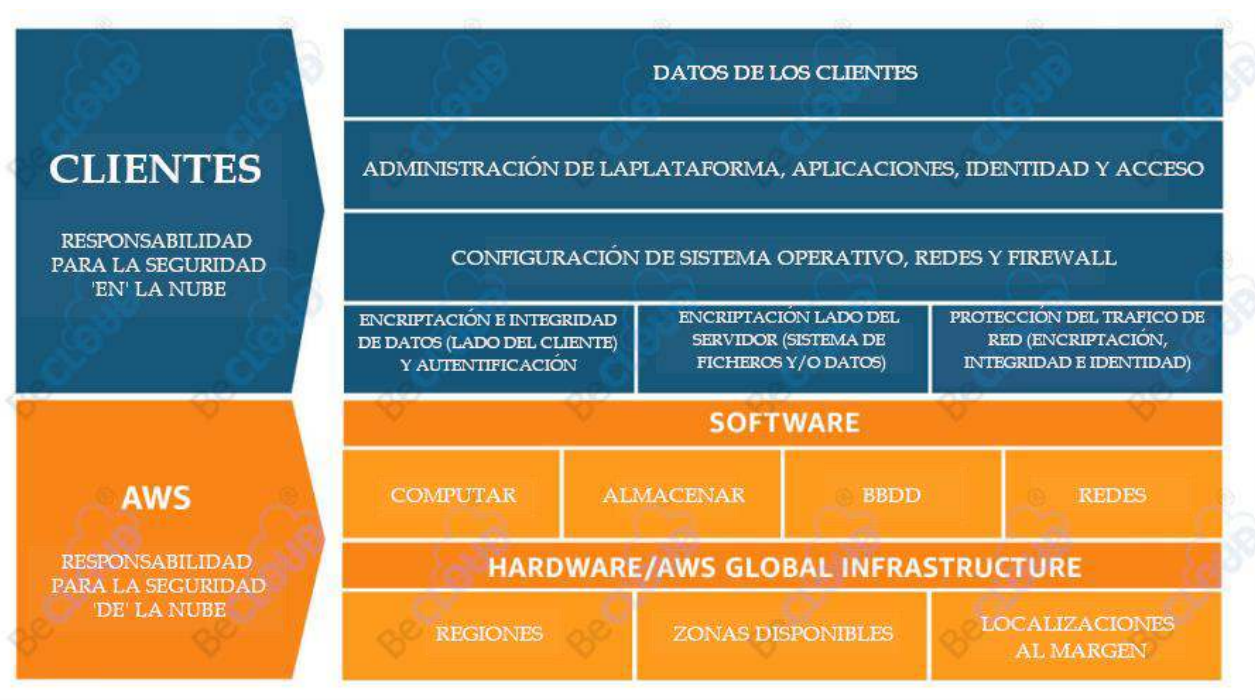
La nube responsabilidad compartida

Cuando subimos nuestra infraestructura informática (balanceadores, firewall, servidores, etc.) a la nube, los proveedores de esta, es decir los GAMI (Google, Amazon, Microsoft, IBM) nos recuerdan que si algo falla la responsabilidad de **los datos** es totalmente nuestra, circunstancias que muchos responsables de informática quieren eludir y la propiedad lo ignora o simplemente no entra a valorarlo.

Si bien podemos provisionarnos de máquinas potentes en los 6 continentes en minutos y crear cluster de microservos gestionados con Kubernetes en la nube híbrida, combinando los distintos actores GAMI, la responsabilidad de que todo funcione sigue siendo del responsable informático en primera instancia y de la empresa o corporación al final. A nivel jurídico, la llamada la CULPA "IN VIGILANDO" (versus la CULPA IN ELIGENDO, por voluntad), recogida en el artículo 1903 del Código Civil, sin perjuicio de las sanciones contempladas específicamente sobre Protección de Datos, indica respecto de las obligaciones la exigibilidad no sólo por los actos u omisiones propios, sino por los de aquellas personas de quienes se debe responder (desde la cúspide de la pirámide y el gobierno de las empresas, hasta los responsables de informática y sus equipos, los delegados de protección de datos ..): *"lo son igualmente los dueños o directores de un establecimiento o empresa respecto de los perjuicios causados por sus dependientes en el servicio de los ramos en que los tuvieran empleados, o con ocasión de sus funciones"*. La culpa in vigilando supone el reconocimiento de la responsabilidad por hechos ajenos. A pesar de que el acto que genera la responsabilidad haya sido realizado por otra persona, el responsable será la persona que debía vigilar o supervisar al individuo que los ha ocasionado. Y ¿qué sucedería si al responsable le denegaron las inversiones necesarias para la adecuada protección de los datos, que le indicaron que optara por el servicio más barato, aunque su consejo profesional es que no cumplía un mínimo de garantías o el estándar

europeo que se ha de cumplir, ...? De esto y de anonimización & pseudonimización de datos, como formas de prevenir y evitar sanciones, hablaremos en otro artículo.

Por tomar un ejemplo Amazon (AWS) nos deja clara la responsabilidad compartida:



*1 Traducción libre [BeCLOUD](https://www.becloud.es)

Los Devops, están obligados siempre a custodiar los datos, depende del producto contratado bajaremos capas de responsabilidad, hasta parchear sistemas operativos. Hablando de infraestructuras como servicio, IBM CLOUD® nos muestra el siguiente cuadro:

Tabla 1. Responsabilidades compartidas de los productos IaaS

Recurso	Gestión de incidencias y operaciones	Gestión de cambios	Gestión de identidad y acceso	Seguridad y conformidad normativa	Recuperación tras desastre
Datos	Cliente	Cliente	Cliente	Cliente	Cliente
Aplicación	Cliente	Cliente	Cliente	Cliente	Cliente
Sistema operativo	Cliente	Cliente	Cliente	Cliente	Cliente
Servidores virtuales y nativos	IBM	IBM	IBM	IBM	Compartido
Almacenamiento virtual	IBM	IBM	IBM	IBM	Compartido
Red virtual	IBM	IBM	IBM	IBM	Compartido
Hipervisor	IBM	IBM	IBM	IBM	IBM
Servidores físicos y memoria	IBM	IBM	IBM	IBM	IBM
Almacenamiento físico	IBM	IBM	IBM	IBM	IBM
Red física y dispositivos	IBM	IBM	IBM	IBM	IBM
Instalaciones y centros de datos	IBM	IBM	IBM	IBM	IBM

[Fuente IBM CLOUD®](#)

Autores:

[Pablo Cubero](#)

[Francisco Folgado](#)