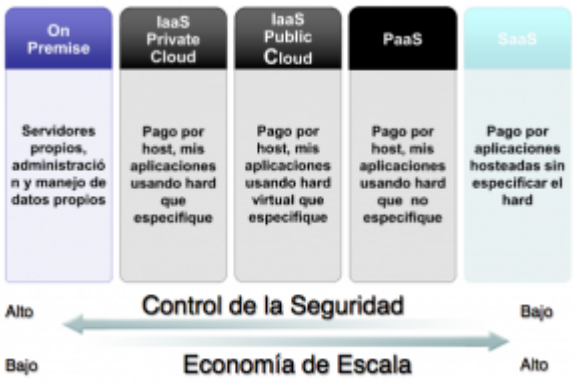
¿Dónde y cómo aseguro mi solución?

Cuando vamos a elegir una solución donde alojar nuestras aplicaciones, bien sean aplicaciones empresariales como CRM, ERP… u otro tiempo de herramientas como para desarrollo de aplicaciones (p. ej.: servidor Jenkins), la seguridad de la aplicación como la privacidad de los datos son dos pilares que marcan mucho la decisión. Un diseño cuidadoso de todas las capas de seguridad es clave para aumentar nuestra confianza en la decisión que vayamos a tomar.

Este post va a enfocarse en la seguridad y privacidad dentro de las áreas de soluciones en la nube e híbridas, ya que es donde nuestros datos y seguridad queda relegada en mayor o menor parte a una empresa tercera. Aunque las normativas y medidas que hay que tomar son las mismas, cuando contratamos a un proveedor el proceso que hay que seguir de implantación requiere de un paso previo de negociación, comprobación de sistemas, normativas, etc.



A todos nos preocupa tener nuestros datos en la nube, porque significa estar expuestos a ataques las 24 horas del día. Sin embargo, la nube puede proveer de soluciones que brinden más privacidad, más seguridad y más fiabilidad que las soluciones que las empresas pueden tomar por sí mismas. Debemos tener en cuenta que estas empresas no pueden permitirse una brecha de

seguridad, ya que significaría la pérdida masiva de los clientes. Solo tenemos que observar lo rápido que ha perdido peso plataformas como Yahoo o Ebay durante los últimos años, han pasado de tener la hegemonía a pasar un plano secundario. Por ello, las empresas que ofrecen sus servicios en la nube hacen mayores inversiones en aspectos de seguridad y privacidad que una empresa, seguramente, ni siquiera plantearía o no podría permitírselo. Existen dos aspectos principales en los que una empresa se debe enfocar: Gobernanza y temas legales, y la seguridad técnica.

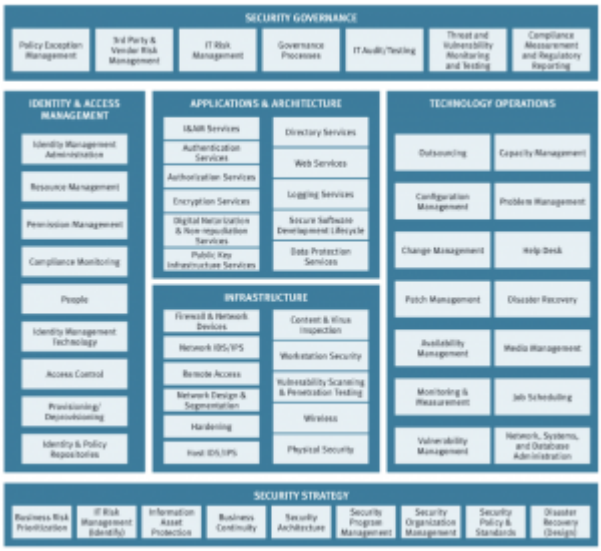
En el primer punto, hay que contactar con la empresa a la cual vamos a contratar los servicios y trabajar con el área de seguridad antes de firmar un contrato. Para eliminar preocupaciones en caso de que haya algún problema, el contrato debe cubrir las áreas de responsabilidades, jurisdicción, privacidad, leyes sobre seguridad, pedidos de información, cumplimiento de regulaciones y auditorias, acuerdo a nivel de servicio y retención de datos. Este paso es aún más crítico si la empresa a la que se va a contratar es extranjera, ya que las normativas que se van a aplicar van a ser la del país de residencia de la empresa. Por lo tanto, primero hay que firmar un acuerdo que la empresa contratante pueda estar satisfecha.

La privacidad de los datos es un mundo enorme, voy a nombrar los pasos básicos que hay que tomar. En unas publicaciones de Bodlelaw [3] existe información desde niveles básicos a normativa avanzada sobre privacidad de los datos. Lo primero que haremos en la tarea de asegurar la situación de nuestros datos es comprobar si nuestro proveedor recolecta o analiza información del cliente, y si esta es de forma anónima. Si es una empresa situada fuera de la Unión Europea hay que comprobar si está en el pacto de Privacy Shield, y “otear” si lo cumple ya que comprobarlo puede resultar imposible. Servicios como los que ofrece Google, Microsoft o Salesforce hacen recolección de datos de forma anónima para la mejora de sus sistemas, o para el desarrollo de nuevos sistemas que

puedan ofrecer a una empresa en el futuro. Por ejemplo, Salesforce acaba de estrenar su sistema Einstein que emplea información de las empresas de forma anónima para que su inteligencia artificial pueda aprender, ofreciendo de esta forma un mejor servicio. Una vez asegurado lo básico, comprobaremos los siguientes puntos:

- Licencia Software: la licencia de nuestro software tiene que estar en sincronización con la de nuestro proveedor. ¿Qué compañías y terceros tendrán acceso al software, y en qué territorios?
- Propiedad intelectual: la empresa debe mantener en todo momento la propiedad de los datos y de sus sistemas.
- Ley aplicada, jurisdicción y lenguaje: establecer las normativas aplicadas y en caso de haber un conflicto entre interpretaciones, cuál es el lenguaje que prevalece en caso de discrepancias.
- Devolución de los datos: cómo van a ser devueltos los datos, en qué formato, y si se ofrece un servicio de migración de datos a otro proveedor.
- Protección de datos: llegar a un acuerdo de qué puede hacer el proveedor con nuestros datos.
- Acuerdo de nivel de servicio: dónde va a estar situado el centro de datos, quién lo va a manipular, procedimientos de seguridad y copias de seguridad, mantenimiento…

Como se puede observar, tanto en la seguridad como en la privacidad existen una inmensidad de puntos a comprobar. Y tan solo hemos rascado la superficie de lo que realmente es, en la siguiente figura se puede observar un modelo de seguridad que toda organización, que requiera un fuerte enfoque en seguridad, debería comprobar:



¿Aún quieres alojar la solución en tu servidor? Es una cantidad de información abrumadora, pero por tomar un punto de referencia existen las siguientes reconocidas normativas sobre seguridad y privacidad: ISO/IEC 27001/2, PCI, HIPAA, Privacy Shield, ISO 27018, entre muchas otras. Con todos los puntos a comprobar, ahora queda mucho más claro por qué las empresas contratan a auditores de seguridad especializados para comprobar sus sistemas.

Como conclusión personal, creo que en la mayor parte de las ocasiones es una tarea mucho más sencilla y barata el negociar y contratar un servicio en la nube para establecer el sistema de la empresa. Tan solo los casos de infraestructuras muy estratégicas y críticas merecen un desembolso tan enorme como para desplegar en la propia empresa un servicio bajo su responsabilidad y mantenimiento, con la excepción de soluciones tan sencillas como por ejemplo un repositorio Git.

REFERENCIAS

[1] “CIGRAS2014- Seguridad y Privacidad en la Nube”, 30 de octubre de 2016, http://www.isaca.org/chapters8/Montevideo/cigras/Documents/CIGRAS2014-%20Seguridad%20y%20Privacidad%20en%20la%20Nube.pdf

[2 “SaaS Agreements – Data Protection – Customer Privacy Policy”, 30 de octubre de 2016,

http://www.bodlelaw.com/saas/saas-agreements-data-protection-customer-privacy-policy]

[3] “Cloud Security KeepingData Safe in the ‘Boundaryless’ World of Cloud Computing“, 30 de octubre de 2016, https://www.knowledgeleader.com/KnowledgeLeader/Resources.nsf/Description/CloudSecurityKeepingDataSafeProtiviti/$FILE/Cloud-Security-Keeping-Data-Safe-Protiviti.pdf