Auditar es Controlar

En artículos anteriores he hablado de diferentes aspectos del outsourcing TI, como su historia, evidencias sobre su práctica, ventajas y desventajas de su aplicación, riesgos asociados… El único punto a tratar que no he comentado es el control de dichos riesgos. Todo riesgo es considerado como una incertidumbre, algo que puede ocurrir durante el funcionamiento normal o las acciones de la empresa y que tiene impacto (generalmente negativo) en los resultados. Cuando hablo de acciones, esto es perfectamente aplicable a la acción de externalizar la tecnología de la empresa, que es el tema que nos incumbe. Para que este proceso sea lo más satisfactorio posible, es necesario establecer una serie de medidas para comprobar cuál es el nivel del riesgo (o la probabilidad de que dicho riesgo ocurra) en cada caso y que permitan obtener una mayor certeza (diría **seguridad**, los humanos somos inseguros por naturaleza) de la fiabilidad de la empresa.

Siguiendo el artículo anterior, en el que establecí 4 riesgos importantes [1] (riesgo operacional y transaccional, riesgos de la confidencialidad de la información, riesgo de la continuidad del negocio y riesgo de conformidad), podemos hacer el trabajo de un auditor y establecer la siguiente matriz de riesgos y controles. Los riesgos asociados pueden ser controlados o mitigados en cada caso. El control es posible gracias a una serie de evidencias que confirman el buen hacer de la empresa que está dando el servicio que se ha externalizado.

Riesgo	Control / Mitigación
Riesgo operacional y transaccional	• Conocer en detalle el flujo de las operaciones y transacciones. • Conociendo el flujo, analizar y descubrir donde una transacción puede fallar y determinar qué rol tiene la empresa que provee el servicio en dicho fallo. • A futuro, establecer posibles acciones a tomar en respuesta al fallo (contractuales, …).
Riesgo de confidencialidad de la información	• Determinar los datos transmitidos a la empresa. • Comprobar y garantizar la seguridad y los controles de protección de datos de la empresa (in situ). • Pedir el SSAE16/SOC (o SAS 70), que evalúa los controles y la seguridad de la empresa (según un auditor externo). • Aumentar la frecuencia de visitas a la empresa en función de la importancia de los datos.

Riesgo de la continuidad del negocio	• Simular una crisis y preguntar a la empresa para determinar cómo reaccionan a dicha situación y en cuanto tiempo. • Preguntar los efectos de dicha crisis en la empresa contratada y establecer a la empresa la importancia de los procesos externalizados para la empresa que la contrata (pérdidas de dinero, confianza, clientes…). • Disponer de una estrategia en caso de fallo del proveedor, es decir, un plan de contingencia. • Comprobar y evitar demasiados "lazos" de externalización con una misma empresa.
Riesgo de conformidad	• Comprobación de que la empresa dispone de los medios necesarios para realizar la función crítica en el tiempo establecido.

Tabla 1: Matriz riesgos/controles

Después de analizar esta matriz, tenemos los riesgos, los controles a esos riesgos y creo que me dejó algo…. ¡ah sí! falta la importantísima figura del "árbitro", es decir, el auditor. Como en cualquier otro área, a la hora de comprobar que los servicios TI son adecuados, cumplen con la ley y demás temas de vital importancia, el auditor juega su papel para comprobar que lo dicho o escrito está en consonancia con lo hecho. Cabe destacar, que como apunta el documento de GTAG para el outsourcing TI [2], este proceso tiene un ciclo de vida, desde la decisión de externalizar, pasando por la implementación y revisión, para posteriormente realizar una renegociación de lo acordado para las futuras colaboraciones. Sin embargo, debido a lo extenso del documento, supongamos que nos encontramos en la posición de evaluar los servicios externalizados, con lo que seguiríamos la siguiente tabla:

Stages	Objectives	Key Activities	Manager Roles *	Risks	Auditor Involvement
E: Monitoring and Reporting	Oversee and control the outsourced operation.	■ Manage relationship. ■ Assess results and performance. ■ Design ongoing reporting and process improvement model.	Process owner,* retained team, project sponsor, finance, HR, risk, and other experts.	■ Relationship and deliverables devolve with customer damage and loss of assets and ROI. ■ Process is not sustained and is not optimized as planned.	■ Determine how provider performance and compliance to the contract will be assessed and routinely reviewed by management. ■ Ask what metrics and other key performance indicators are used. ■ Ask how concerns and areas for improvement are communicated and leveraged to improve current and future operations/ contracts.

Tabla 2: Puntos clave a la hora de auditar las operaciones externalizadas

En este caso, como se apunta en la tabla, el auditor deberá determinar si el proveedor ha tenido un rendimiento adecuado y ha cumplido con el contrato.

Deberá pedir también las métricas utilizadas para medir el rendimiento, así como las áreas de mejora a tener en cuenta, las acciones a tomar en esas áreas para mejorar futuras acciones y operaciones. Aunque esto puede considerarse muy genérico, puede plasmarse de una manera más exacta mediante el plan descrito en un documento de ISACA [3]. Siguiendo un enfoque guiado por el riesgo, el auditor debe seguir 4 pasos importantes: realizar una evaluación del nivel del riesgo obtenido, realizar un trabajo de campo (si es offshore en el país, sino mediante reuniones), realizar un reporte sobre lo obtenido y continuar con las operaciones externalizadas, amoldándolas a las conclusiones obtenidas. El paso uno es el más importante y donde el auditor realiza gran parte del trabajo. En dicho paso, su función es entrevistarse con los stakeholders de la compañía, así como el proveedor del servicio, determinar los objetivos, riesgos y controles y comprobar si el proveedor dispone de algún tipo de informe (SOC1, ISO 2700X o similar). A partir de lo obtenido, deberá ajustar el alcance de la auditoría en función de los controles, desarrollar una matriz de riesgos y controles (similar a la que se ha visto en este artículo), así como un programa de auditoría. Finalmente, quizás sea necesario disponer del conocimiento de expertos, como abogados, para tomar decisiones, como por ejemplo en el tema de leyes y regulaciones.

Resumiendo, el trabajo de establecer controles para evitar, mitigar o gestionar riesgos es una tarea importante en cualquier acción de cualquier tipo, con especial importancia en el outsourcing TI. Al fin y al cabo, estás delegando funciones que podrían realizarse dentro de la empresa fuera de la empresa, con personas que no tienen ninguna unión con tu empresa (fuera del contrato) y que tienen métodos de funcionamiento o estrategias distintas a las que tu tenias y tienes. De similar manera, muchas veces se piensa que no se debe externalizar algo porque es demasiado arriesgado o, dicho de otra manera, puede tener mucho riesgo asociado. Pero la solución es clara: para obtener unos beneficios determinados hay que arriesgarse, disponiendo de una serie de controles que nos ofrezcan un mínimo de seguridad. Esa seguridad que nos puede transmitir un auditor cuando nos dice que los controles son correctos y que todo marcha como la seda. Aunque es cierto que el futuro es imprevisible y no se puede estar preparado para todo…

Referencias:

[1] ”4 IT Outsourcing Risks and How to Mitigate Them”, The Wall Street Journal (Deloitte), acceso el 31 de Octubre del 2016, http://deloitte.wsj.com/cio/2012/07/10/it-outsourcing-4-serious-risks-and-ways-to-mitigate-them/

[2] “Information Technology Outsourcing”, GTAG Global Technology Audit Guide, acceso el 31 de Octubre del 2016, https://chapters.theiia.org/montreal/ChapterDocuments/GTAG%207%20-%20Information%20technology%20outsourcing_2nd%20ed.pdf

[3] Adnan Dakhwe, “Risk & Control Considerations for Outsourced IT Operations”, ISACA, Core Competencies – C32, San Francisco, acceso el 31 de Octubre del 2016,

http://www.sfisaca.org/images/FC13Presentations/C32_Presentation.pdf

[4] ”Outsourced IT Environments Audit/Assurance Program”, ISACA, acceso el 31 de Octubre del 2016, http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Outsourced-IT-Environments-Audit-Assurance-Program.aspx