DIRECCIÓN VS. SISTEMAS: TRATADO DE PAZ

Recibido: 03/07/07
Aceptado: 23/07/07

MANAGEMENT VS SYSTEMS: TREATY OF PEACE

Joseba Enjuto Gozalo
Ingeniero Superior de Telecomunicaciones
Consultor Senior
Nextel, S.A.

RESUMEN

En muchas empresas es frecuente que los gerentes y los técnicos no se pongan de acuerdo. Pero es posible acercar la tecnología al negocio a través de los riesgos, un término que ambos mundos comparten. Un análisis de los riesgos tecnológicos a alto nivel puede ser el nexo de unión entre uno y otros de forma que todos caminen en la misma dirección.

Palabras clave: Análisis, riesgos, estrategia, seguridad, tecnología.

ABSTRACT

In many companies it's usual that the managers and the technicians do not agree themselves. But it's possible to approach the technology to the business through the risks, a term that both worlds share. A technological risks assessment carried at high level can be the nexus of union between one and others so that all walk in the same direction.

***Key words**: Assessment, risks, strategy, security, technology.*

Aunque, como consultor de seguridad, conozco muchas empresas, cada una con sus particularidades, la mayor parte de ellas comparten un problema que se repite continuamente y que habitualmente es la causa de muchos desencuentros. La dirección y el área de sistemas de información nunca se ponen de acuerdo. Las prioridades de unos a los otros les parecen secundarias. Lo que para unos es evidente, los otros son incapaces de asimilarlo. Sencillamente es como si no fueran capaces de entenderse. Como diría un conocido *best-seller,* parece que unos son de Marte y los otros, de Venus… ¿Cómo se puede lograr que ambos grupos trabajen de forma coordinada? ¿Es posible dirigir los esfuerzos de ambos mundos en una misma dirección? Sí, es posible y a continuación vamos a ver cómo se puede conseguir.

La principal preocupación de la dirección es, evidentemente, el negocio. Estrategia, costes o beneficios son palabras habituales en su discurso y, sin embargo, es en otro concepto en el que nos tenemos que centrar: el riesgo Todos los directivos son conscientes de los riesgos a los que está sujeto su negocio: sus financieros, competitivos, de mercado… Sin embargo, hay un tipo de riesgo que no suelen conocer con detalle y es el riesgo asociado a la tecnología. En general, la dirección es consciente de que la introducción de tecnología en sus procesos de negocio puede constituir una ventaja competitiva, pero, en muchos casos, no conoce los riesgos que supone esa introducción. Es un mundo desconocido, complejo y difícil de asimilar cuando no se conoce. Por tanto, éste es el punto de partida: resolver esa complejidad.

Para conseguir nuestro objetivo, tenemos que partir de algo sencillo y conocido como es el mapa de procesos de negocio. La dirección lo conoce, es sencillo de entender y muy útil si se sabe trabajar con él.

A partir del mapa, tenemos que ir profundizando en cada proceso, revisando en qué consiste. Tenemos que analizar qué se hace y qué se obtiene en cada uno de ellos. Conocerlos, saber cuál es su función, cuáles son las entradas y cuáles las salidas de cada uno, y entender sus interrelaciones. Al menos, a nivel general.

Cuando tengamos claro cada proceso (y siempre se puede pedir ayuda a los correspondientes responsables), habrá que pensar qué necesitamos para llevar a cabo esas tareas, identificar los recursos asociados a cada proceso. Y es aquí donde aparece la tecnología, pero con una particularidad: está ligada a uno (o varios) procesos de negocio.

En este primer paso de identificación de recursos no hay que ser muy exhaustivos. A los directivos les basta saber que hay una aplicación que les permite llevar la contabilidad. No les interesa saber si es una aplicación cliente - servidor o si está desarrollada en Java. Y, menos aún, si está soportada por un único servidor o por varios. Y, en este momento, a nosotros tampoco. Es suficiente saber con que existe una "plataforma" de contabilidad.

Llegados a este punto, podemos empezar a pensar en un sencillo análisis de riesgos, que debe ser más sencillo que análisis. Lo suficiente como para que la dirección esté dispuesta a ejecutarlo.

Recordemos que hemos partido del mapa de procesos de negocio. Y, en el análisis de riesgos, la labor de la dirección es valorar estos procesos, priorizarlos. Analizar su importancia para la empresa, evaluando aspectos

como la disponibilidad de los procesos, la confidencialidad de la información que se procesa en ellos o su integridad. Ellos, mejor que nadie, conocen su negocio y tienen que ser capaces de valorar estos aspectos.

Con esta valoración, el trabajo puede seguir avanzando y ahora hemos de pensar en las amenazas que pueden sufrir esos procesos. Y tenemos que pensar en ellas a todos los niveles. Unas serán externas y otras, internas. Algunas, intrínsecas, y otras, debidas a la tecnología. Por fin, la primera aproximación. Sin embargo, no hay que tener prisa. Estamos pensando en plataformas tecnológicas, genéricas y, por lo tanto, las amenazas a las que están sujetas serán igual de abstractas. Podemos pensar en errores de usuario o quizás en *hackers*, pero jamás seremos capaces de evaluar la amenaza de corrupción de la base de datos a este nivel. No importa, todo llegará.

Después tenemos que analizar las vulnerabilidades, discutirlas y razonarlas, tratando de establecer, lo más claramente posible, por qué las plataformas son vulnerables a las amenazas contempladas. Y, una vez lleguemos a un acuerdo, está dado el primer paso. El cálculo del nivel de riesgo es automático como resultado de los tres factores analizados. Será tan sencillo como combinar los valores que se han dado a cada activo, a cada amenaza y a cada vulnerabilidad. Y, como consecuencia del análisis, tendremos una serie de riesgos tecnológicos que afectan a los procesos de negocio. Valorados y definidos.

A partir de este punto, es probable que la dirección se preocupe. Aparecen ciertos riesgos de los que hasta este momento no eran conscientes. Y probablemente quieran conocer mejor el problema o, al menos, sus soluciones.

En este momento, la tarea es desgranar el análisis de riesgos estratégico que hemos realizado. Expandir el concepto de plataforma en cada uno de sus componentes, desmenuzar cada una de las amenazas contemplada en sus múltiples elementos. Una vez que lleguemos a identificar la base de datos, podremos analizar su riesgo de corrupción. Pero no tenemos que

perder de vista que el análisis exhaustivo tiene que partir del estratégico y, por tanto, habrá que poner mucho empeño en que quede claro cómo se llega de los riesgos estratégicos a los riesgos técnicos. Evitando que los riesgos identificados a nivel estratégico se diluyan o pierdan al llegar al nivel operativo.

Una vez tengamos el análisis de riesgos a bajo nivel, será relativamente sencillo identificar los activos a proteger. Y probablemente también será fácil identificar el modo de hacerlo ya que los riesgos serán técnicos y sus soluciones, también. Así que tendremos que comenzar a gestionar el riesgo. Habrá que definir las contramedidas técnicas y operativas a implantar, y evaluar su coste. Y nadie mejor que el propio departamento de sistemas para llevar a cabo esta tarea.

Luego habrá que asociar esas soluciones técnicas a los riesgos estratégicos. Para ello, habrá que identificar las ventajas de alto nivel que presentan las soluciones técnicas planteadas. Un antivirus corporativo se convertirá en una mayor protección para los datos financieros, mientras que un CPD* replicado pasará a ser una garantía de disponibilidad frente a catástrofes naturales. Quedará claro que, si necesitamos una nueva cabina de discos, es para mejorar la competitividad de la empresa. Tendremos soluciones de negocio para los riesgos tecnológicos. Soluciones diseñadas y cuantificadas desde el departamento de sistemas, parametrizadas y en tiempo, dinero y esfuerzo para que sean entendibles por la dirección. Y así habremos llegado a la solución del problema.

De este modo, hemos llevado a cabo un análisis de riesgos estratégico y hemos sido capaces de traducirlo en un plan de tratamiento de riesgos de carácter técnico que sea entendible por la dirección. Ahora, el área de sistemas sabe expresar proyectos a nivel estratégico y la dirección es capaz de identificar riesgos a nivel tecnológico. Por fin, hemos conseguido que directivos y técnicos se entiendan. No parece complicado, ¿verdad? Con unos resultados tan prometedores, merece bien la pena el intento. Y, de todas formas, si a la hora de la verdad el trabajo se complica, siempre se puede recurrir a una ayuda externa especializada…

BIBLIOGRAFÍA

- BS 7799-3:2006, *Information technology -Security techniques -Part 3: Guideline for information security risk management.*

- BIERY, Ken Jr. *Aligning an information risk management approach to BS 7799 -3:2005*. © SANS Institute 2006, -

- ISO / IEC. -13335-1:2004 *Information technology -Security techniques -Management of information and communications technology security -Part 1: Concepts and models for information and communications technology security management.* ■

** Centro de Procesos de Datos*