El 'ROSI' o hasta el rabo todo es toro

José de la Peña Sánchez

No quisiera que esta entrega se convirtiera en el apunte para un *vademecum* de contabilidad y finanzas para no financieros -en primera redacción salío algo así-, pero me parece que en los tiempos que corren en el mundo de la protección de la información, marcados por la necesidad de incrementos presupuestarios para invertir en planes y no tanto por la justificación de la necesidad de proteger los sistemas de información, algunos profesionales de la seguridad TIC –siempre hay excepciones– deberían de familiarizarse con determinados conceptos de gestión de las empresas, el tan traído ROI entre otros.

Antes de entrarle al asunto, y para centrar expectativas, merece la pena citar al profesor Tamames, cuando dice que "Las previsiones económicas son aún menos verosímiles que las metereológicas".

Bien, al grano: ¿qué se entiende por el ROI, *Return on Investment* (retorno de la inversión)? Pues según Andersen es el "Ratio financiero que compara el **beneficio neto** obtenido en determinado **proyecto de inversión** con el **capital total** invertido en él". El ROSI (*Return on Security Investment*) es un ROI sobre seguridad TIC, y *tutti contenti*.

Y, ¿qué es inversión (*Investment*)? Pues continuando con Andersen, la "Colocación de fondos en un **proyecto** (de explotación, financiero, etc.) con la intención de obtener un **beneficio** en el **futuro**".

Creo oportuno recordar que en todas las empresas existe un sistema de **planificación** (largo plazo)/**presupuestación** (corto plazo)/**control** (permanente), una estructura organizativa, y las cuentas de resultados, tanto histórica o real como previsional, dentro del sistema de control.

Esto es importante tenerlo muy en cuenta para encajar un proyecto de inversión en seguridad TIC, tema muy concreto que forma parte de la planificación de la empresa –uno más–, que entra dentro del proceso de fijación del presupuesto.

Al respecto y en el caso de la seguridad TIC, procede determinar su grado de libertad, primero de la inversión en TIC, y después, de otra u otras inversiones. Estos son dos frentes cruciales en el contexto organizativo de los que la seguridad TIC depende casi al completo.

Quizás resulte ilustrativo evidenciar que el desarrollo de las TIC se inició con el impacto sobre los procesos en lo tocante a **eficacia** y después sobre la **eficiencia**; posteriormente, se amplió a la transformación del **negocio**, esto es, capacidad de generación de **nuevos productos, nuevos canales, nuevos mercados**. ¿Algo que ver hoy con la seguridad?

Un CISO –cargo directivo de muy nuevo cuño en estos lares– debe conocer el medio ambiente del entorno decisor en su compañía, sobre todo en lo que atañe al proceso de la selección de inversiones.

Por otra parte, los **proyectos de inversión** pueden clasificarse por su objetivo en mantenimiento o incremento de la capacidad, productividad, obligatorios por imperativo legal, estratégicos y sociales o suntuarios. Y como todo requiere una **estimación** (cálculo aproximado o hipótesis que se hace sobre algo, según Andersen), bien puede decirse que la determinación del ROSI de un proyecto multifuncional resulta muy arriesgada. Un marrón, vamos.

Antes de entrar en el proceso de selección de inversiones, traigo a colación un hecho: que de cara al futuro, las empresas bien gestionadas tratan de orientarse en un medio compuesto de **certeza/riesgo/incertidumbre** en el que "Sólo se puede saber si se ha tomado una buena decisión cuando se conocen los resultados de la misma".

Resulta obvio que las decisiones se toman en un ambiente de racionalidad limitada; la racionalidad absoluta y el óptimo no son posibles debido a la imperfecta adaptación de los modelos.

Visto lo visto, ahondemos en lo mencionado: el proceso de selección de inversiones. Y nada mejor, para ello, que enumerar los criterios de selección que deberían tenerse en cuenta; a saber: **rentabilidad, evaluación de riesgos, impacto de la financiación.** Ni qué decir tiene que los aspectos técnicos, económicos y financieros están interrelacionados.

Hoy por hoy, los ciclos económicos existen –como nos recuerda lo sucedido con las punto.com–, por tanto resulta necesario evaluar la sensibilidad de las inversiones a las oscilaciones del mercado, de la tecnología, de la disponibilidad de los recursos financieros..., principalmente.

Y a todo esto, el Responsable de Seguridad TIC con su *hot potato*: su proyecto de inversión, solo o en compañía de otros. Para él, y desde un punto de vista de la calidad, el resto de la empresa son sus clientes internos, a los que tiene que vender su producto, la seguridad TIC.

La inversión, indudablemente, es un problema de empresa y condiciona su futuro, por lo que la decisión se convierte en un acto estratégico. En consecuencia, la aprobación del presupuesto de inversión implica un acto de gran transcendencia en la elección de los objetivos y de cómo se pretende configurar lo que será la empresa.

Este circuito creará tensiones, puesto que algunos proyectos de inversión serán desestimados, de forma total o parcial, transitoria o definitivamente.

La selección de inversiones es un problema de toma de decisiones, que deberá estar debidamente argumentada y evaluada, para lo cual existen diversas técnicas. Dicha toma de decisiones está condicionada, además, por lo que con un exceso de tacto llamaremos superestructura de poder/decisión en la empresa. Existen, como es sabido, los *stakeholders* (grupos de interés), implicados en y por la actividad empresarial, por lo que resulta normal la existencia de coaliciones, tanto internas como externas. Esto genera asimetrías y/o equilibrios entre grupos y/o personas. Un CISO –cargo de muy nuevo cuño en estos lares– debe conocer el medio ambiente del entorno decisor en su compañía en el contexto en el que lo estamos tratando: la selección de inversiones.

No parece que sobre el ROSI y aledaños pueda decirse mucho más con rigor y sin recurrir a planteamientos algo esotéricos, aunque al CISO, que presumiblemente en este estadio evolutivo actual procede de los escenarios técnicos de las tecnologías de la información, y más que nada para no quedar descolocado, sí le vendrá bien familiarizarse con terminos como IRR (*Internal Rate of Return*) o TIR (*tasa interna de rentabilidad*), NPV (*Net Present Value*) o VAN (valor actual neto) y DCF (*Discounted Cash Flow*) o flujo neto de caja... Recuerdo ahora que en determinados ambientes profesionales, el *Cash Flow* es un totem, y en otros, "las pelas son las pelas". Y no sería honrado concluir esta caterva de terminajos sin traer a colación el Ebitda, lucubración de moda en ámbitos de la economía mágica.

Antes de concluir esta entrega nada mejor que incidir en lo serio: que el área de seguridad TIC debería de ser el proveedor interno de seguridad TIC, y el resto de la empresa sus clientes internos; en consecuencia, si se dispone de un mapa de amenazas/riesgos, cada cliente interno, con apoyo de seguridad TIC, analizará sus fortalezas/debilidades y actuará en consecuencia. Este es el mejor modelo posible hoy.

Como broche final diremos dos cosas: que el Informe de Gestión de la empresa debe incluir el cumplimiento de empresa en funcionamiento, y que no hay que olvidar en el presupuesto anual la inclusión sistemática de la actualización del Plan de Recuperación de Desastres. Así de fácil. ■

José de la Peña Sánchez
Auditor Censor Jurado de Cuentas y Licenciado en Informática
info@codasic.com