Inversiones en seguridad y amortización

Diciembre 2005

Agustín López

Ing. Informático

Lead Auditor BS7799 certificado por BSI

www.iso27000.es

Desde un tiempo a ésta parte, podemos asegurar que la palabra “seguridad” se ha puesto definitivamente de moda y está siendo consecuentemente explotada en la comercialización de productos, especialmente en el ámbito de la tecnología y de tratamiento de la información.

En la mayoría de productos y sistemas de seguridad, fabricantes y distribuidores finalizan sus demostraciones técnicas con modelos de costes adaptados para destacar las ventajas del producto, convirtiendo características técnicas en cantidades económicas que alcanzan rápidamente su amortización en un corto espacio de tiempo.

Sin embargo, éste tipo de modelos no suelen ayudar más allá de las obligadas comparaciones entre productos similares, ya que cualquier adquisición conlleva a nuestra empresa unos costes variables asociados a una formación, adquisición de hardware o software, servicios de implantación y/o integración, asistencia y/o mantenimiento, que son específicos y diferentes para cada entorno específico.

Una vez contabilizados los gastos totales y las nuevas medidas implantadas, nos enfrentamos, por tanto, en cada caso, al reto de contrastar la inversión económica y los nuevos niveles de seguridad alcanzados mediante un sistema al estilo “antes/después” que permita una evaluación racional de la amortización.

A pesar que es un proceso lógico y necesario podemos comprobar, sin embargo, que en muchos casos no se llega a realizar finalmente por falta de modelos definidos dentro de la empresa o de capacidad técnica y/o de personal que el propio proceso necesita, siendo finalmente encontrados como suficientes los procesos estándar de comprobación de las compras y de la gestión controlada del presupuesto asignado, justificaciones de por sí necesarias, pero que poco o nada evidencian de la efectividad de las mejoras y su estudio de amortización correspondiente.

“¿Realmente era inevitable?, ¿Podría haber sido menor el daño?, ¿Se invierte adecuadamente en seguridad?”. Éstas son, sin duda, las preguntas más frecuentes derivadas de cada incidente que afecta a la disponibilidad, confidencialidad o integridad de la información crítica relacionada con el desarrollo de las actividades propias de la organización.

Si los gastos en seguridad se realizan con la mejor intención y claridad posible y la Dirección no duda en apuntar que el esfuerzo económico es el mayor que la organización puede permitirse, ¿no queda alternativa para conocer en detalle cuándo es necesario dedicar más o menos presupuesto y dónde es más efectivo o más urgente aplicarlo?

Comparando la inversión y los resultados en seguridad.

Cualquier inversión en Euros que realiza la empresa está justificada en relación a unos resultados evaluados finalmente en Euros y las inversiones en seguridad no deberían ser una excepción.

Pero, ¿cómo podemos cuantificar una posible pérdida de reputación de la empresa, el daño en las decisiones de negocio basadas en información crítica adulterada o la violación y propagación más allá de su círculo de confidencialidad (planes de reducción de personal o colectivos, estratégicos, financieros o nóminas por ejemplo)?.

En sectores como las compañías de seguros, un agente de seguros debe enfrentarse a diario a estimaciones de éste tipo, llegando al extremo de asignar un valor monetario a la vida humana para poder aplicar una política de beneficios. El análisis “coste-beneficio”, en este caso, está expuesto al conocido riesgo que suponen los resultados finales con numeradores infinitos o divisiones por cero.

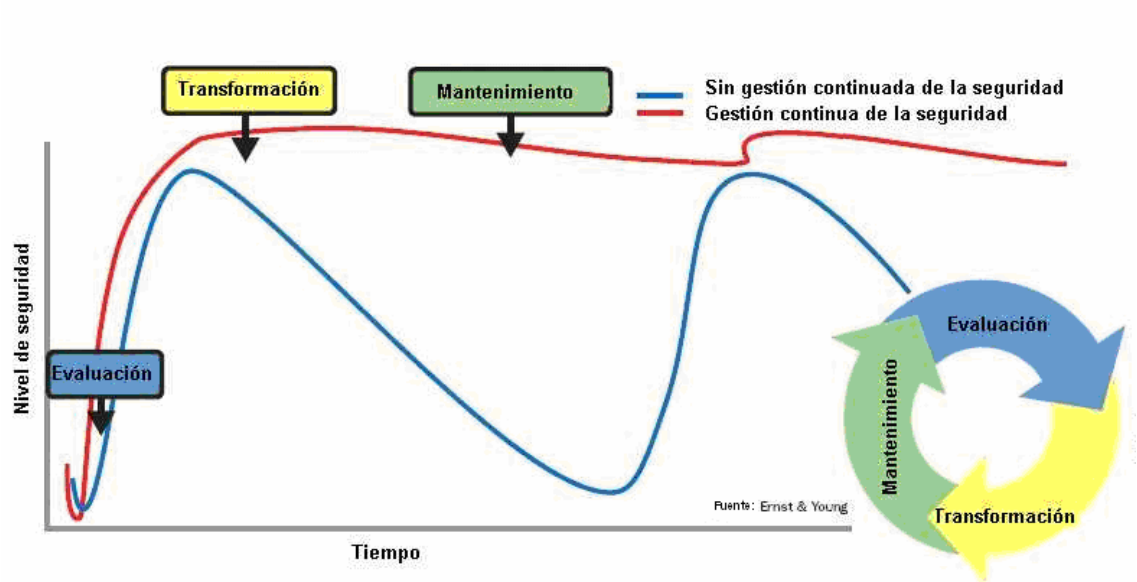
Por este motivo y la complejidad y riesgos relacionados de un modelo similar para nuestros fines, debemos evitar la pregunta “¿Cuánto es lo máximo que puedo obtener invirtiendo X Euros?” (Análisis de coste y beneficios), sustituyéndola por una efectividad en los costes determinada por la pregunta básica: “¿Tengo inevitablemente que gastarme X Euros?”.

Para ayudarnos a desarrollar éste enfoque, disponemos de las buenas prácticas en seguridad del estándar ISO27000, que sirven de referencia útil para conocer y contrastar regularmente el nivel de seguridad que hemos implantado mediante medios técnicos, procesos organizacionales y guías directivas.

Con ayuda del estándar, las medidas de seguridad pueden guiarse efectivamente siguiendo un grado de detalle sostenible por la propia empresa, capacitándola para responder de modo concreto a toda la organización a las preguntas clave:

- ¿Es la empresa segura en un grado aceptable?
- ¿Están las inversiones en seguridad justificadas?
- ¿Contra qué riesgos mayores, medios y menores se enfrenta la empresa?
- ¿Está garantizada la disponibilidad mínima de los servicios mediante indicadores de los factores críticos (p.ej. volumen crítico de transacciones)?
- ¿Cómo son identificados y establecidos los requisitos de seguridad?
- ¿Qué importancia tienen las medidas individuales de seguridad?
- ¿En qué estado está la empresa en comparación con la competencia?

Un análisis básico de la situación actual de la seguridad y sus potenciales repercusiones para el negocio no conduce a respuestas reales para este tipo de preguntas, si no se desarrolla una comparación continuada y acorde con las “mejores prácticas”. El estudio realizado mediante la simulación de Monte Carlo muestra la diferencia de los niveles alcanzados con una gestión continua de la seguridad.



La evaluación de las medidas de seguridad debe confirmar a la empresa unas necesidades concretas de gestión y la importancia de cada una de ellas en el tiempo, que sirva finalmente para determinar la inversión final derivada que debemos considerar en la organización.

De este modo no queda ninguna duda posible: la efectividad de los costes en seguridad se origina mediante la consecución de aquellas medidas de seguridad en el grado que demuestran ser realmente imprescindibles para la empresa.