SEGURIDAD Y NEGOCIO: UN MISMO LENGUAJE

La comunicación entre dos o más partes no siempre resulta fácil; depende de varios factores, pero sin lugar a dudas tenemos mucho terreno ganado si los que intentan comunicarse disponen de un mismo lenguaje. Sólo tenemos que pensar en el pasaje bíblico de la Torre de Babel...

La dificultad en la comunicación con el negocio en aspectos de seguridad no está relacionada con el propio término **seguridad**. La seguridad (o la falta de ella, según se mire) es algo cotidiano en nuestros días. Seguridad física sobre todo: protección de nuestro hogar, del vehículo que nos transporta, seguridad de las personas que, por su papel en la sociedad, se encuentran en situación de riesgo, etc. Somos todos cada vez más conscientes de la aportación de la seguridad a nuestras vidas: entendemos la necesidad de medidas contra el terrorismo, que los fabricantes de automóviles mejoren continuamente las medidas de seguridad y utilicen este hecho como un argumento de venta (el que no tiene no sé cuantos *airbags*, ABS, ESP y demás siglas raras, se queda atrás). Puede ser incluso que los clientes no comprendamos técnicamente algunos de los mecanismos de seguridad, pero sí entendemos los beneficios potenciales que suponen: el producto final es más seguro. La tarea machacona de bombardeo de información ha conseguido impregnar al cliente de una **cultura de seguridad**, porque además, la comunicación le ha transmitido en un **lenguaje entendible**, a veces muy duro, lo que nos estamos jugando: la propia vida.

El concepto seguridad, por tanto, está muy presente en el día a día de todos nosotros pero, ¿qué ocurre con la **seguridad de la información** o de los activos de información, según queramos precisarlo, utilizados por los negocios? En este ámbito la cuestión ya resulta más difusa y es preocupación de los responsables de seguridad de la información explicar y hacer entender a los responsables del negocio hasta qué punto es importante la seguridad, **hasta qué punto forma parte del propio negocio**.

Nuestro reto está en saber comunicarnos con el negocio en términos que le resulten familiares, de negocio en definitiva: **rentabilidad de la inversión**, **reducción de costes**, **beneficios**, como consecuencia de dotar de más seguridad a sus activos de información. En esta situación, los responsables de seguridad de la información hemos de ser capaces de determinar y dar a conocer al negocio el valor añadido que una adecuada seguridad le aporta.

Análisis

La evolución del negocio y el objetivo por alcanzar cada vez mayores cotas de competitividad hacen que surjan nuevas necesidades de sistemas de información en los que apoyarse. Ante la gran complejidad tecnológica existente y las arquitecturas cada vez más abiertas, la seguridad de la información debe convertirse, desde los primeros pasos de concepción y durante el resto del ciclo de vida de estos sistemas, en un compañero de viaje inseparable.

El método a utilizar para establecer el nivel de seguridad adecuado es el **análisis de riesgos**, sistemática que al negocio le resulta muy conocida. Aplicar esta metodología sobre los activos de información forma parte del cálculo del riesgo operativo, componente a su vez del análisis de riesgos global del negocio.

El análisis de riesgos dará como resultado la determinación de las amenazas, las vulnerabilidades y el impacto previsible en el negocio, caso de materializarse alguna de las amenazas. El propio negocio será parte fundamental en la valoración del posible impacto en términos cuantificables y será el que decida cuál será el riesgo residual a admitir como asumible.

La información de gestión que hay que suministrar al negocio para conseguir las inversiones necesarias en protección, debe plasmarse en un conjunto reducido de indicadores revelador de cuál es el nivel de seguridad de su información.

Gestión

Posteriormente, la **gestión del riesgo** definirá las contramedidas técnicas, organizativas o de cualquier otra índole a implantar con el objetivo de reducir el riesgo hasta la cota admisible por el negocio. En esta fase habrá de establecerse la relación **coste / beneficio** (coste de las contramedidas, beneficio conseguido por su implantación). Como podemos observar, toda esta terminología es perfectamente conocida por el negocio.

Informes

No debemos descuidar otro aspecto fundamental en la comunicación a mantener con el negocio: el *reporting*. El negocio necesita saber "cómo estamos en seguridad". La información de gestión que hay que suministrar al negocio para, entre otras cuestiones, conseguir las inversiones necesarias en seguridad, debe plasmarse en un conjunto reducido de indicadores (**cuadro de mando**) revelador de cuál es el nivel de seguridad de su información. Debemos ser muy cuidadosos en la selección de estos indicadores y no informar de cuestiones llamémosle técnicas, por ejemplo, del número de ataques que estamos detectando a través de los diferentes cortafuegos, antivirus, detectores de intrusión y demás "cachivaches". Esta información es más interna al equipo de gestión de la seguridad, útil para valorar quizás el correcto funcionamiento de esos mecanismos, pero no es entendible por el negocio.

Para que el negocio nos entienda habremos de informarle mediante un lenguaje que le permita observar fácilmente el nivel de **confidencialidad**, **integridad** y **disponibilidad** de sus activos de información: intentos de acceso no autorizados fallidos y exitosos, tiempo de indisponibilidad de los servicios de información ocasionado por problemas de seguridad, fraudes, intentos de suplantación de personalidad y de aplicaciones, el impacto en su negocio, si lo ha habido. Los valores comparativos de los diversos indicadores a lo largo del tiempo reflejarán la evolución de la seguridad y si se están consiguiendo las metas marcadas por el negocio.

A modo de conclusión final, conviene recalcar la tremenda importancia de hablar con el negocio en su mismo lenguaje cuando tratamos cuestiones de seguridad de la información, demostrando que no se trata simplemente de algo incómodo y que supone un coste adicional, sino todo lo contrario: se traducirá en una ventaja competitiva para su negocio. Así, poco a poco, conseguiremos ganar confianza y aumentar la conciencia de seguridad a lo largo de la organización, base para el establecimiento de la cultura necesaria para extender el proceso de seguridad de manera inseparable en los procesos de negocio. ■

> **Ramón Montes Ortega**
Responsable de Seguridad Informática

ENDESA