



¿QUÉ
PREOCUPA?

... LA ADECUADA GESTIÓN DEL RIESGO

Tengo la firme creencia y convicción de que la principal misión que se me encomienda al ser responsable de seguridad informática es la de realizar una adecuada gestión del riesgo tecnológico; mi empresa pone a mi disposición una serie de medios, tanto técnicos como humanos, y espera que con los mismos aporte la capacidad y el criterio necesarios para gestionar de manera eficiente el riesgo asociado a los sistemas de información.

Hace ya algún tiempo quise hacer un pequeño sondeo sobre el concepto que tenían, personas allegadas a mí, del trabajo que desarrollaba; tras preguntar a diversos amigos, encontré tres grupos de respuestas que se resumen de la siguiente manera:

"¿Tú? Eres programador y responsable de equipos informáticos". En este grupo se encuadran los que no tienen ni idea y la seguridad les suena simplemente a algo relacionado con la informática.

"Eres como la policía informática del Banco". A una respuesta similar a ésta acudieron los que aplican la lógica y lo comparan con otras actividades cotidianas.

"Tu misión es controlar que la informática no tenga intrusos, ni virus y que los equipos informáticos funcionen". Los que realizan una definición así, asocian la seguridad con aspectos específicos que conocen y relacionan con la misma.

ción causa/efecto por incidentes ocurridos, debe fijarse de acuerdo a una planificación derivada de un análisis exhaustivo y con el total apoyo y comprensión de la dirección de las empresas.

Riesgos

Normalmente, en las grandes compañías se habla a menudo de riesgos financieros, que son fácilmente entendibles y asimilables por la dirección, pero se desconoce o se minusvalora la existencia de un tipo de riesgo que es inherente al uso de sistemas de información, elementos imprescindibles para el desarrollo de las actividades de negocio. La visión de la seguridad como gestión del riesgo informático facilita la comunicación con la alta dirección de las empresas al utilizar un lenguaje cercano y familiar a los interlocutores y, a través de ello, hacer comprensibles las funciones y responsabilidades del área de seguridad.

La gestión empresarial hace hincapié en emplear todos los recursos disponibles en conseguir los objetivos estratégicos definidos por la empresa, tendiendo a ser eliminada toda aquella actividad o función que no aporte valor para la consecución de los objetivos. Por ello, se deben redoblar los esfuerzos para dar una visión de la seguridad como inversión y no como gasto; algo tangible que

El riesgo tecnológico debe ser considerado un exponente fundamental del riesgo operacional asociado a cualquier actividad de una empresa que utilice un sistema de información como soporte básico de su actividad o como medio para conseguir sus objetivos.

Si partimos de la base de que la seguridad absoluta es imposible, y los estadios cercanos a la misma tienen un coste infinito, la concepción de la seguridad como gestión del riesgo es la vía que permite al responsable de seguridad saber las medidas que debe aplicar, de forma que se evite la pérdida de visión global y la tendencia a aplicar medidas de seguridad de manera compulsiva, sin reparar en el coste de las mismas o el retorno de la inversión que producirían en términos de reducción del riesgo.

Tan importante como aplicar las medidas necesarias para reducir o mitigar el riesgo tecnológico es el conocimiento y la asimilación del riesgo remanente existente en las compañías; es importante saber calibrar el mismo y que la dirección lo asuma.

La gestión del riesgo tecnológico debe estar basada en un soporte metodológico que junto a profesionales especializados y herramientas de soporte, permita una reducción del mismo con medidas de índole organizativo y procedimental, además de aquellas estrictamente asociadas a seguridad.

Como resumen, se podría decir que la gestión del riesgo es la herramienta que permite la comunicación de forma inteligible de la seguridad con la dirección de las empresas, y su difusión y concienciación por parte del personal de las mismas, permite gestionar los medios a disposición de los responsables de seguridad y determinar las medidas a adoptar para obtener un nivel de riesgo adecuado a las necesidades de la empresa y que el mismo sea asumido por la dirección.

En definitiva, entiendo la seguridad como una labor fundamentalmente preventiva y la gestión del riesgo como la vía inequívoca para dilucidar dónde y qué medidas de seguridad se deben aplicar, de ahí que mi principal preocupación sea el gestionar adecuadamente el riesgo asociado a los sistemas de información de mi empresa. ▢

«La adecuada gestión del riesgo aporta un carácter de inversión a la seguridad y dota de criterio y justificación a los costes de implementación de medidas de seguridad»

Mi primera preocupación surgió del hecho de extrapolar estas respuestas al pensamiento de la dirección de mi empresa: ¿qué conocerían de la seguridad?, ¿qué sabrían del trabajo que desarrollamos?, ¿cómo podrían valorarlo? Probablemente si preguntásemos a altos directivos, su definición de seguridad iría más orientada hacia el tercer tipo de respuesta que, en definitiva, habla de amenazas concretas y de la posibilidad de que las mismas se plasmen en realidad, es decir de riesgos específicos asociados a los sistemas de información.

Ningún programa serio de seguridad puede ser desarrollado sin el apoyo de la dirección de la empresa, de ahí la gran importancia de hacer comprensibles las funciones y responsabilidades del área de seguridad. La motivación para la inversión en seguridad, que normalmente viene dada por una reac-

aporte valor añadido a la empresa, parte de la estrategia de la misma como una ventaja competitiva o una necesidad para la consecución de ciertos objetivos. La adecuada gestión del riesgo aporta un carácter de inversión a la seguridad y dota de criterio y justificación a los costes de implementación de medidas de seguridad; es la vía para que la dirección pueda calibrar la inversión que debe realizar en materia de seguridad.

El riesgo está presente en la mayoría de las actividades de la empresa, desde el lanzamiento de un nuevo producto hasta la concesión de un crédito, y de su adecuada gestión depende en gran parte el cumplimiento de los objetivos; por ello es importante calibrar los riesgos tecnológicos en función de los objetivos de negocio. De tal forma que la seguridad pueda ser considerada como un componente estratégico para la consecución de los objetivos de la empresa.



> José Antonio Castro González
Director de Seguridad Informática
Santander Central Hispano