La formación de los directivos de seguridad de la información

José de la Peña Sánchez

En la pasada entrega opinábamos que la función de seguridad en una empresa típica debería depender de su Consejero Delegado, en tanto que ejecutivo de máximo nivel, esto es, lo que en EEUU se entiende por CEO, *Chief Executive Officer*. Dábamos también algunas breves pinceladas sobre la ubicación de la función específica de seguridad TIC, y dejábamos apuntadas algunas ideas sobre qué tipo de profesionales parecen adecuados para cumplir dicha función específica.

Sin entrar en discusiones sobre la estratificación y los niveles profesionales y operativos alrededor de la actividad de protección de la información, bien merece la pena aseverar que el perfil más alto y el que es necesario potenciar por su escasez es el de directivo, cuyas habilidades no le deberían distinguir de las prescritas para sus colegas del mismo nivel en otras áreas, y cuyos conocimientos habrían de abarcar un amplio abanico de campos, desde el conocimiento profundo de los negocios/actividades de su entidad, hasta el escenario legal y normativo completo en el que ésta se desenvuelve, pasando por el dominio a nivel general de su sistema de información y de comunicaciones. Añadamos como indispensable que ha de ser un experto en la gestión de riesgos tecnológicos y en seguridad técnica.

Dicho perfil no es fácil de encontrar hoy, ya que su necesidad en grandes organizaciones se ha manifestado desde hace relativamente poco tiempo, y de todos es sabido que los buenos directivos no se crían espontáneamente, sino que necesitan el periodo justo de maduración.

Así pues, nos encontramos con que hoy ese perfil antedicho, orientado al *IS Governance* (gobierno de la seguridad de la información), se empieza a necesitar/demandar, justo en un momento de la historia en que el *Governament Corporate* (gobierno corporativo) ha contagiado su tremenda crisis al *IT Governance* (gobierno de las tecnologías de información).

> *En una sociedad sana el contenido de la formación que se ofrece da una idea muy aproximada de los perfiles profesionales que se buscan.*

En este punto, quizá convenga traer a colación, por sus implicaciones con los tres gobiernos mencionados y con la práctica de auditoría, el concepto de **Sistema de Tecnología de Información Financiera" (FITS)**, integrado o independiente, que está mereciendo últimamente gran atención en el terreno normativo a ambos lados del charco. No está definido lo que es un FITS, ni integrado ni independiente, aunque habrá que hacerlo, y cuanto antes mejor.

Pero volvamos al tema que nos ocupa más directamente; a saber, el relativo a los profesionales de la seguridad de la información en las empresas, a los que en el mundo anglosajón denominan CISO (*Chief Information Security Officer*) e ISO (*Information Security Officer*).

CISM

Bien puede decirse aquí que por su formación los conocerás. Efectivamente, en una sociedad sana el contenido de la formación que se ofrece da una idea muy aproximada de los perfiles profesionales que se buscan.

Si nos creemos este envenenado pensamiento, la formación extrauniversitaria existente en materia específica de seguridad, basada en la obtención de certificaciones de reconocido prestigio, es decir las proporcionadas por Sans Institute (GIAC) y por (ISC)2 (CISSP), principalmente, cubren un espectro de conocimiento muy técnico, dejando los ámbitos profesionales de gestión y dirección tal vez desasistidos.

Los primeros en reaccionar han sido los colegas de ISACA (*Information System Audit and Control Association*), la entidad certificadora de personas que concede el CISA (*Certified Information System Audit*). Y lo han hecho proponiendo la credencial CISM (*Certified Information Security Manager*).

Esta credencial se obtendrá tras superar un examen en los siguientes dominios o áreas:

– *Information Security Governance* (gobierno de la seguridad de la información).

– *Risk Management* (gestión del riesgo).

– *Information Security Program Development* (desarrollo del programa de seguridad de la información).

– *Information Security Management* (gestión de la seguridad de la información).

– *Response Management* (gestión de respuesta).

Si se llega a buen fin, hay que adherirse al Código Profesional de ISACA y aceptar la verificación de la evidencia de:

– Un mínimo de 5 años de trabajo en seguridad de la información.

– Un mínimo de 3 años de trabajos en tres o más de las áreas precitadas de gestión de seguridad de la información.

– Experiencia en sustituciones certificadas en seguridad de la información.

– Certificaciones relativas (incluso CISA) y titulaciones con experiencia en gestión de sistemas de información.

ISACA también ofrece el proceso "abuelo" o promoción cero, aceptando experiencia verificable de:

– Un mínimo de 8 años de trabajo en seguridad de la información.

– Un mínimo de 5 años de trabajo en cuatro o más áreas precitadas de gestión de seguridad de la información.

Con este repaso de la propuesta uno puede hacerse una idea del tipo de profesional que ISACA busca certificar, quizá impelida por la "enronitis" aún no superada en la sociedad americana y en la economía global a buscar expertos que ayuden al regreso del control interno, un elemento fundamental para el buen gobierno de la corporación y de todos los sistemas que la componen, más específicamente los de información, integrados o independientes, soportados por TIC.

Hay otras razones que sin duda pueden explicar este movimiento de ISACA, y una firme candidata es la que alude a la demanda del mercado, que parece empeñada en recordarnos que se necesitan directivos de seguridad de la información. n

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