



## La responsabilidad responsable



José de la Peña Sánchez

Antes de entrar en el asunto que en esta entrega nos ocupa, esto es, el del responsable de seguridad en informática y comunicaciones, conviene reflexionar acerca de algunos aspectos que aluden al marco en el que ha de desarrollar su actividad.

Desde luego, se debe de reconocer que nuestra ley de leyes –nos referimos a la Constitución de 1978, y concretamente a su artículo 18.4: «La ley limitará el uso de la Informática para garantizar...»–, ha sido un caso atípico de previsión legislativa, poco usual en la normativa de las TIC. El de la derogada LORTAD (1992) también fue un interesante caso de previsión a efectos de seguridad. Sin embargo, la desesperante lentitud en la aparición del Reglamento de medidas de seguridad (1999), todavía hoy no implantado en su totalidad, puede considerarse como un ejemplo histórico de las pocas prisas existentes en ciertos ambientes por hacer las cosas bien y mejor. Este texto legal, del que disfrutamos en España, ha sido y es uno de los motores del despegue de la seguridad y de la actividad profesional correspondiente.

Hay un aspecto de marco, el cambio social, que interesa mencionar: el desequilibrio existente entre sus tres vectores, el tecnológico, que tiene un desarrollo incontenible; el legislativo, que últimamente marcha con excesivo retraso, y el ético, la escala de valores, que no está adaptado en absoluto al actual estado del arte de las TIC.

Es interesante recordar a estas alturas, en las que tanto se habla de confianza, que «en confiar no hay más que esperanza, en fiarse hay seguridad». Como quiera que disponer de cierta 'seguridad' técnica medianamente verificable –y de una organización de seguridad– se ha convertido en una exigencia legal, la alternativa que queda es cumplir, y ya se sabe que en este tiempo de hoy (quizá también en el de ayer), lleno de OPAs/OPVs y fusiones/absorciones, definido por la existencia de una mezcla asimétrica entre la 'antigua' economía –basada en el trabajo físico y los recursos materiales– y la 'nueva' –aquella que hace énfasis en

el conocimiento y la comunicación en el entorno de la Red–, las normas se cumplen por atrición (para que no nos pillen) en vez de por contrición (por convencimiento).

Pues bien, en este ambiente confuso, turbulento y cambiante se encuentran las entidades pública y privadas donde prestan sus servicios los responsables de seguridad en informática y comunicaciones.

### ¿QUÉ DEBEMOS ENTENDER POR RESPONSABLE DE SEGURIDAD?

¿Qué debemos entender por responsable de seguridad? Sencillo, no hay que inventar nada. El Reglamento lo define como «Persona o personas a las que el responsable del fichero

### *En las entidades dirigidas por aficionados, no se entiende lo difícil que es llegar a saber con la exactitud suficiente qué riesgos de seguridad TIC hay que ir gestionando*

ro ha asignado formalmente la función de coordinar y controlar las medidas de seguridad aplicables». Esto afecta exclusivamente al tratamiento de datos personales, pero si aceptamos la opinión reputada del profesor Arturo Ribagorda cuando indica, acerca del Reglamento, que «Donde dice datos personales, léase datos», la figura del responsable de seguridad queda bastante bien dibujada en la definición, salvedad hecha del término fichero, puesto que a efectos reales –y como es sabido–, una organización en algo más que responsable de un conjunto de ficheros con y sin datos personales. Si a lo dicho le sumamos la expresión gestión de riesgos, la cosa empieza a tener forma.

Esto de la gestión del riesgo, que ya es asunto antiguo y conocido, presupone la realista aceptación de la inexistencia de la seguridad total, lo que por otra parte debería llevar a la idea de mejora continua en todos los órdenes de la eficiencia del sistema de seguridad, incluyendo la función interna o externalizada de intrusos buenos. Desgraciadamente, en las entidades dirigidas por aficionados, no se entiende lo difícil

que es llegar a saber con la exactitud suficiente qué riesgos de seguridad TIC hay que ir gestionando (porque esto es un proceso), y como mucho, implantan tres productos y no consideran necesario disponer de una función específica y concreta de seguridad. Obviamente, el tratamiento de datos personales lo entienden como algo exótico que no va con ellos. Afortunadamente, cada vez hay menos de esto.

Antes de seguir con el asunto, merece la pena puntualizar que la función de auditoría, tanto interna como externa, continúa teniendo razón de ser. Y no sólo eso, sino que se está viendo reforzada. Eso sí, nadie regala duros a cuatro pesetas: la formación del auditor de seguridad TIC debe ser tremendamente

completa, profunda y especializada, a tenor de la cada vez mejor formación de los responsables de seguridad, y del perfeccionamiento y complejidad de las tecnologías aplicables a la seguridad técnica, cada vez más utilizadas por el auditado.

### UBICACIÓN

Hasta el momento se han expuesto algunas ideas sobre el responsable de seguridad TIC, pero no hemos dicho cosa alguna acerca de un asunto esencial: a saber: su ubicación dentro del organigrama formal de la entidad. Hay alternativas, desde hacer que ocupe una posición de directa dependencia del primer ejecutivo, hasta la adscripción a la estructura gestora del sistema de información.

En mi opinión, y como norma general para entidades a partir de un cierto volumen y dependencia tecnológica, un gestor de riesgos (de seguridad) en el contexto de las TIC debe ser un directivo de alto nivel, versado en TIC y en organización, con equipo humano multidisciplinar, presupuestado, dotes de persuasión y especialmente preparado para

colaborar, sobre todo si la 'organización' en la que presta sus servicios es un grupo formado por muchas empresas y, obviamente, muchos sistemas de información tecnológicos. (Dejaremos el caso específico de las fusiones para otro artículo).

Una fuente de problemas en este escenario es la relacionada con las guerras y tensiones entre las estructuras formales e informales que existen en cualquier entidad. La estructura formal es un «sistema artificial creado ex profeso», en tanto que la informal nace como consecuencia de las tensiones lógicas provocadas por la estructura formal. Las llamadas agrupaciones informales, variopintas y complejas, son hasta cierto punto inevitables y asumibles; pero no en materia de seguridad TIC, especialmente si presentan una geometría vertical y de naturaleza parasitaria. (Las hay de otros tipos: horizontales, verticales simbióticas, complejas...).

En todo caso, está muy claro: la existencia y desarrollo de las TIC y su función de seguridad inciden profundamente en las estructuras de las corporaciones actuales; no obstante, los trabajos y actividades relativos a la propia seguridad –y a la calidad– son tareas de toda la entidad y deben impregnarla, independientemente de que haya responsables funcionales específicos.

En entregas posteriores intentaremos tratar aspectos que aquí se han obviado por no hacer la exposición demasiado larga: dirección y gestión por competencias y capacidades (tecnológicas, estratégicas, personales, organizativas..., estructuras del poder y estilos de dirección); los efectos de la existencia de *hackers*, *crackers* y grupos organizados antisistema, y la existencia «real» de la empresa «virtual», o lo que es hoy casi lo mismo, el cuchillo sin hoja que no tiene mango.

Para terminar, y en atención al papel de la seguridad TIC en el contexto mercantil contemporáneo, recordemos al gran Drucker, cuando dijo aquello de que el primer FIN de la EMPRESA no ha de ser obtener un BENEFICIO, sino ASEGURAR su SUPERVIVENCIA, de la cual resulta condición indispensable dicho beneficio. n

### JOSÉ DE LA PEÑA SÁNCHEZ

Auditor Censor Jurado de Cuentas y Licenciado en Informática  
Correo-e: coda2@jet.es