>> DOBLE FONDO

José de la Peña Muñoz
Director
jpm@codasic.com

El plan de continuidad provisional permanente

A muchos responsables de sistemas de información se les reverdece el miedo a la indisponibilidad cada vez que tienen noticia de un desastre en casa ajena. Lamentablemente, ese miedo, tan agudo como arrítmico, no es lo suficientemente persistente como para provocarles un subidón de conciencia empresarial que les anime a hacer el titánico esfuerzo –plenos de habilidad y con conocimiento del medio: sus empresas– de llevar a buen puerto (pruebas y actualizaciones incluidas) ese dichoso plan de contingencias informático y de comunicaciones que desde hace años está a medio hacer, y sin el cual no es posible construir un plan de continuidad de negocio, del que es pieza capital.

Ya se sabe que a la disponibilidad, cuyo mantenimiento –junto con el de la integridad y la confidencialidad– constituye el objetivo de la seguridad de la información, sólo se la toman en serio –salvo excepciones– los que han sufrido en sus carnes el ataque de la bestia, ya en forma de fuego, en el caso de Deloitte hace muy poco, ya en forma de agua, en el caso del Banco Guipuzcoano hace años, ya en forma de *bits* envenenados –hay muchos candidatos en esta familia de modalidades–, puesto que ataques a la disponibilidad hay muchos, bien directos, bien indirectos. Y por lo que se observa, es un terreno tan abonado o más para la comisión de delitos como el del robo de identidades y la suplantación.

Por otra parte, no hay cosa peor para la buena imagen y, por ende, para el negocio –sobre todo en algunos sectores– que la indisponibilidad en sus distintas gradaciones de los sistemas y de los servicios que éstos soportan, la pérdida de datos y de información, y el incumplimiento de contratos que pudiera derivarse de esa caida de servicios y/o pérdida de datos.

Y ojo: ya puestos, los sistemas de seguridad del sistema de información tecnológico pueden constituir, mal implantados y mal gobernados, una amenaza a la disponibilidad de los sistemas y servicios de una organización (también a la integridad y confidencialidad de la información), y, por ende, a sus negocios y actividades. En esto, como en todo, el uso de la tecnología entraña riesgos, y la de protección no iba a ser menos. Este epígrafe, cuya criticidad aumenta a medida que se incrementa el uso de herramientas tecnológicas con diversas finalidades de seguridad, entra dentro de las responsabilidades específicas de los directores del área, unos profesionales cuya formación permanente no se puede improvisar.

Conviene, pues, estudiar con urgencia todos los riesgos asociados a la disponibilidad del sistema de información tecnológico, e intentar mitigarlos con profesionalidad. Al fin y al cabo, una buena labor en ese punto contribuirá a alejar más el fantasma de la quiebra, algo que muy pocos directivos discutirán. ●