

|  |  |  |  |  |  |  |  |  |  |
|--|--|--|--|--|--|--|--|--|--|
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |

## ¿Estamos preparados para un desastre?

**Manuel Monterrubio**

*Miembro de la Comisión de Seguridad de ASIMELEC*

*Alhambra-Eidos*

Podríamos empezar diciendo que nunca estamos preparados para un desastre, ¿quién puede imaginar que le toque a su empresa? Sin embargo, ocurre y el 60 por ciento de las organizaciones que sufren un desastre, cierra en los tres años posteriores. (Cummings, Haag y McCubbrey, 2005).

Hoy en día, el acceso a la información es fundamental para la continuidad de los negocios (aunque parezca obvio, hace tan sólo 15 años no era así en la mayoría de las empresas, siendo los activos físicos la clave exclusiva); por tanto, es necesario garantizar la disponibilidad de los datos críticos en caso de desastre. Lo primero, para ello, es aceptar que en cualquier momento se pueden producir. No tiene por qué tratarse de un incendio como el acaecido en el Windsor hace ya tres años. Nos valen otros hechos mucho más cotidianos como: cortes de energía eléctrica -típico en época estival-, caídas de líneas telefónicas, inundaciones, ataques de virus, empleados desleales, sabotajes, etc.

En cada organización -privada o pública, multinacional o pyme- el nivel de alerta, la severidad y el impacto en los distintos casos es diferente, así como el tipo de actuación requerido para la protección, pero el objetivo es el mismo: recuperar el acceso a la información de negocio y reiniciar la actividad de la empresa en el menor tiempo posible.

En definitiva, para evitar ser parte de esta estadística, cada empresa debe poner en marcha políticas y estrategias claras de: seguridad, actuación ante emergencias y recuperación ante desastres.

No se trata de poner en marcha proyectos enormes con cuantiosas inversiones, sino de medidas adaptadas a las necesidades y capacidad de cada organización. El objetivo principal: evitar o minimizar en la medida de lo posible el impacto negativo de la pérdida de datos e infraestructuras tecnológicas sensibles para el negocio y, sobre todo, estar operativo de nuevo cuanto antes al máximo nivel posible.

En resumen, si el lector tiene influencia en los accionistas (o es uno de ellos) que será el que pierda valor cuando el desastre se produzca, no lo deje para mañana, realice un Plan de Recuperación de Desastres cuanto antes.