

Tirada: <b>7.306</b>		Superficie: <b>354,00 cm<sup>2</sup></b>		
Difusión: <b>7.082</b>				
(O.J.D)	Nacional	Mensual	Valor: <b>2.243,42</b>	
Audiencia: <b>24.787</b>	Tecnología/Informática		Página: <b>21</b>	
Ref: <b>1203021</b>	1 <sup>a</sup> Edición	01/12/2006	1 / 1	

## TRIBUNA

# Más vale prevenir que lamentar

■ **Manuel Monterrubio**

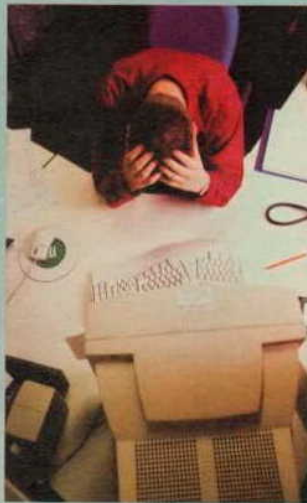
CEO de Alhambra-Eidos

Según algunos estudios realizados a empresas norteamericanas, el 40% de las compañías que sufren un desastre no vuelven a abrir nunca. Y del 60% que reabren, más de un tercio cierra en los siguientes tres años. En resumen, el 60% de las organizaciones que sufren un desastre desaparece en los tres años posteriores al mismo. Una cifra escalofriante. Para no ser parte de esta estadística, cada empresa debe poner en marcha políticas y estrategias claras de seguridad y de recuperación de datos ante desastres.

En estos momentos, se encuentra en fase de tramitación un nuevo Reglamento de Protección de Datos que potenciará los planes de Disaster Recovery (DRP) dentro de las organizaciones. De la misma forma, impulsará la incorporación de proyectos específicos de seguridad en las compañías, tanto grandes –aunque éstas en gran medida ya cuentan con algunas medidas de este tipo– como medianas y pequeñas. Aunque la nueva normativa, que previsiblemente entrará en vigor a principios de 2007, no obliga a las organizaciones a implantar planes de contingencia y recuperación de información en caso de desastres, sí ayudará a que se tome conciencia de un problema importante y más común de lo que muchos sospechan.

En muchas empresas, nos encontramos con aspectos tan chocantes y arriesgados como la realización de back-ups que nunca se comprueban o que se almacenan en la misma oficina donde está ubicado el centro de proceso de datos. Debemos tener en cuenta que, hoy en día, en todas o casi todas las compañías las Tecnologías de la In-

formación y las Comunicaciones son un elemento crítico para la marcha del negocio. En algunas, de hecho, si los sistemas fallan, la empresa se paraliza totalmente. El nuevo reglamento obligará, por ejemplo, a revisar que las copias de seguridad funcionan cada seis meses. De poco sirve una copia de seguridad que no recupera datos o que se guarda en la oficina, si se produce un incendio precisamente en estas instalaciones...



Lo más adecuado para establecer un DRP, una vez decidida su implantación, será programarlo como un plan en espiral, en el que las áreas cubiertas y las competencias se vayan ampliando poco a poco. Tendrá que basarse a su vez en la metodología PDCA o "Plan-Do-Check-Act" (planear-realizar-comprobar-actuar), lo que se resume en aprobar el plan preliminar, implantarlo, realizar la auditoría y revisar los procedimientos (desde el mantenimiento, hasta la formación o la puesta en marcha de acciones preventivas o correctoras), y así sucesivamente.

El coste de su implantación obedece a muchos factores, pero tampoco tiene por qué requerir una inversión desmesurada. Las compañías deben buscar la solución a sus necesidades específicas y los procedimientos más adecuados a su tipo de organización, avanzando poco a poco en la protección.

Si, además, aplicamos las ventajas de disponer de redundancia en determinados sistemas y comunicaciones, estaremos ayudando a la eficiencia de la organización, al incremento de la seguridad y a la reducción del coste de propiedad de las tecnologías de la información y las comunicaciones. ■