
	Tirada: 30.000	Sección: -	
	Difusión: 19.000	Espacio (Cm_2): 433	
Nacional	Audiencia: 66.500	Ocupación (%): 71%	
Informática	01/04/2007	Valor (€): 1.728,12	
Mensual		Valor Pág. (€): 2.404,50	
		Página: 14	Imagen: Si

Soluciones de recuperación ante desastres

Alhambra-Eidos y HP organizan el Primer Foro Disaster Recovery Plan en las Administraciones Públicas

Tanto las Administraciones Públicas como la empresa privada tienen las mismas necesidades en la puesta en marcha de planes de recuperación ante desastres, debido a la importancia de su información y de la cada vez mayor dependencia de las TIC. Esta ha sido una de las conclusiones del primer Foro DRP en las AAPP que han organizado de forma conjunta Alhambra-Eidos y HP. El evento tenía como objetivo analizar qué situaciones se pueden producir y cuáles pueden poner en peligro los activos TIC y servir de foro donde compartir la experiencia con las instituciones públicas. Según Manuel Monterrubio, CEO de Alhambra-Eidos, "en la administración pública, en caso de desastre o incidente, no se pierde negocio, sino servicio". Actualmente, la dependencia de la informática es casi total tanto en el ámbito público como en el privado, lo que implica que los planes de recuperación son necesarios. "El plan dependerá de la dependencia de las TIC y del impulso de los máximos cargos, así que para que funcione es necesario que en la administración pública la clase política se comprometa", declara el máximo responsable de Alhambra-Eidos.

El principal problema de las organizaciones en el momento en que se produce un incidente es el poder disponer y recuperar la información crítica para poder proseguir con la actividad y no llegar a una caída del servicio o de la continuidad del negocio. Adelantarse a las incidencias y emergencias, planear cómo actuar si ocurren, establecer políticas de seguridad y llevar a cabo pruebas periódicas son las principales claves para los responsables de la administración pública.

Además, una de las cuestiones importantes para las organizaciones es el diseño de su propio test de evaluación, lo que permitirá saber si tienen diseñado un buen plan de recuperación ante desastres que pueda responder a cuestiones tales como: saber si los usuarios guardan información crítica en local, si se almacenan las cintas de back up en



Manuel Monterrubio (segundo por la izquierda) junto a los ponentes del Foro DRP (Disaster Recovery Plan)

la oficina, si se lleva a cabo la comprobación de las cintas de back up, si las cintas de back up se guardan en un bunker ignífugo...

Otro de los invitados en el Foro fue Javier Hernández del Castillo, Jefe de Departamento de Informática y Comunicaciones del Instituto de Salud Pública de la Comunidad de Madrid, que destacó en su intervención que cuando se habla de desastre o incidencia también es necesario pensar en los errores humanos o en los problemas técnicos como principales causas de pérdida de información. En palabras de Hernández, "la Administración Electrónica crea también un factor importante ante la puesta en marcha de este tipo de planes, ya que desde las AAPP estamos obligando al empresario y al ciudadano a establecer contacto con nosotros desde fuera a través de la red y de la tecnología. Si la AAPP ya ha empezado a dar ese servicio, es necesario entonces poner en marcha medidas que hagan que no se produzca ningún corte del mismo y hay que hacer que haya continuidad en esa comunicación". La administración electrónica implica también interdependencia entre organismos, mayor control, cumplimiento de normativas y servicio óptimo al ciudadano así que cada vez tiene más importancia implantar el plan. Es importante conseguir aspectos como la confidencialidad, la integridad y la disponibilidad. ■

IMPLANTACIÓN DEL DRP

La implantación de las soluciones DRP (Disaster Recovery Plan) está precedida por una fase de consultoría en la que se tratará de identificar la información y los servicios críticos, determinar los tiempos de respuesta y recuperación, recoger datos para la fase de diseño y definir una solución teórica que en la fase de implantación tomará forma.

Es básico definir el intervalo de tiempo entre la invocación del DRP y el momento en que se considera operativo, así como establecer la fecha y hora hasta la que será posible recuperar la información (cuántas transacciones se han perdido, frecuencia de copias de seguridad, retraso en la replicación...)

La compañía también trata de garantizar la disponibilidad de las comunicaciones, basándose en su infraestructura multioperador y en su equipo de monitorización de líneas, así como la puesta en marcha de un centro de trabajo alternativo para un equipo definido de personas con todo lo necesario (PCs, material de oficinas, sala de reuniones) y una infraestructura de movilidad que pueda contemplar que los usuarios trabajen desde sus hogares o cualquier otro lugar, utilizando soluciones de SBC (Citrix, TS...).

Finalmente, como parte del mantenimiento del DRP habrá que establecer los criterios de activación, y una serie de procedimientos: rollback, puesta en marcha y validación del DRP.