

Nota de Prensa

Alhambra-Eidos y HP proponen a las AAPP adoptar cuanto antes soluciones de Recuperación ante Desastres.

Ambas compañías han organizado de forma conjunta el Primer Foro DRP en las Administraciones Públicas.

Madrid, 26 de febrero 2007.- Una de las conclusiones del primer Foro DRP en las AAPP que han organizado de forma conjunta Alhambra-Eidos, empresa especializada en facilitar soluciones a las necesidades empresariales en el ámbito de las Tecnologías de la Información y las Comunicaciones, y HP en las instalaciones de esta empresa en Madrid, es que tanto la Administraciones Públicas como la empresa privada tiene 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.

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 – principales asistentes al encuentro. Según Manuel Monterrubio, CEO de Alhambra-Eidos, *“las principales diferencias entre admón. Pública y empresa privada son los encargados de tomar las decisiones y que en la AAPP no se pierde negocio, sino servicio en el caso de que se produzca un desastre o incidente. Si se perdiera la información de la seguridad social, ¿qué supondría?”*

En estos momentos, tanto en el ámbito público, como en el privado, la dependencia de la informática es casi total o – en algunos casos, total - , lo que hace que los planes de recuperación sean 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.

Acceso a la información

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. *“Ante un desastre – además de las personas - uno de los aspectos fundamentales a tener en cuenta es la capacidad de acceder a la información, incluso más que la mayoría de los activos de una fábrica o de un organismo.”*, comenta Monterrubio.

Prever las incidencias y emergencias que pueden afectar a la entidad, 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 la

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

Administración Pública y compromiso

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. Según sus datos, el error humano es en el 55% de los casos uno de los principales causantes, mientras que los problemas técnicos y los empleados movidos por ánimo de lucro pueden llegar a representar el 20% y el 10%.

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.

Si a esto se añade la importancia de los datos que las distintas organizaciones públicas pueden guardar en sus instalaciones (datos tributarios, salud, ...) una pérdida de información global, puede suponer un grave perjuicio para múltiples actores de la sociedad (ciudadanos, profesionales y empresas).

Implantación del DRP

La implantación de las soluciones DRP 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: roll-back, puesta en marcha y validación del DRP.

Sobre Alhambra-Eidos

Alhambra-Eidos es una compañía especializada en proporcionar Soluciones a las necesidades empresariales en el ámbito de las Tecnologías de la Información y las Comunicaciones. Contamos con un fuerte bagaje técnico en distintas áreas especializadas, así como con un numeroso conjunto de clientes de renombre. También gozamos del prestigio ante los fabricantes con los que colabora habitualmente. Así, por ejemplo, fuimos la primera compañía en España que obtuvo la homologación como Microsoft Gold Certified Partner for Learning Solutions, y CISCO nos ha premiado en el año 2003 como el reseller más innovador, aplaudiendo así la dedicación de nuestra corporación.

<http://www.alhambra-eidos.es>

Para más información:

Alhambra-Eidos

Miguel Ángel Gombau

91 787 23 00

mangel.gombau@a-e.es