tecnimap Murcia 2004

17

PROYECTO FÉNIX: RESPALDO Y CONTINUIDAD INFORMÁTICA PARA LA JUNTA DE ANDALUCÍA

José Francisco Quesada Moreno
Jefe Gabinete de Sistemas de Información Horizontales. Dirección General de Administración Electrónica y Calidad de los Servicios
Consejería Justicia y Administración Pública. Junta de Andalucía

1. INTRODUCCIÓN

Durante los últimos años, todas las administraciones públicas, en mayor o menor grado, han acometido ambiciosos planes de automatización de sus procedimientos. De forma paralela, estamos inmersos en un proceso creciente de implantación de la "Administración Electrónica", la cual exige una presencia continua de la administración a través de distintos canales, especialmente Internet.

La informatización de su funcionamiento junto con la necesidad de una presencia continua en la Web son algunas de las principales razones que han motivado que las administraciones públicas se planteen seriamente los problemas relacionados con el respaldo y continuidad informática.

Tradicionalmente se han planteado estrategias dirigidas hacia lo que podríamos denominar seguridad pasiva. Es decir, medidas que de acuerdo con las metodologías para análisis y gestión de riesgos de los sistemas de información (por ejemplo, MAGERIT) tienden a reducir la vulnerabilidad de los sistemas de información. No obstante, las amenazas, por su propio carácter, siguen persistiendo, por lo que se hace necesario abordar estrategias de seguridad activa. Es decir, estrategias dirigidas a la eliminación o mitigación del impacto en los sistemas una vez que se ha materializado la amenaza.

Teniendo en cuenta este escenario, en el ámbito de la Junta de Andalucía se decidió abordar la implantación de una solución de respaldo y continuidad informática para todos los sistemas de información críticos. El resultado ha sido el "Proyecto Fénix", cuya implantación se está iniciando durante 2004, y estará en pleno funcionamiento a inicios de 2005.

Este artículo describe las líneas principales de este proyecto. En primer lugar se describe la planificación del proyecto como parte del Plan Director de Organización para la Calidad de los Servicios de julio de 2002. De acuerdo con las directrices de este plan, el proyecto de creación de un centro de respaldo comenzó abordando las tareas relativas al análisis de riesgos, y en particular se abordó un estudio sistemático de los sistemas de información críticos que debían quedar cubiertos en el centro de respaldo.

El diseño del proyecto parte de la división funcional de la operativa del centro de respaldo y continuidad informática en dos servicios básicos: la salvaguarda de datos y la recuperación ante desastres. Estos servicios se organizan asimismo atendiendo a la criticidad de los propios sistemas de información. Los niveles de criticidad afectan a dos parámetros básicos: RPO (relacionado con el servicio de salvaguarda de datos) y RTO (relacionado con el servicio de recuperación ante desastres.

Por último, el artículo describe la situación actual del proyecto Fénix, una vez que ha finalizado la fase de licitación, se ha producido la adjudicación del proyecto, y se ha comenzado con la fase de transición o de incorporación de los distintos organismos al Centro de Respaldo.

2. PLANIFICACIÓN: EL PLAN DIRECTOR DE ORGANIZACIÓN PARA LA CALIDAD DE LOS SERVICIOS

La necesidad de creación de un centro de respaldo para la Junta de Andalucía se formuló inicialmente en el Plan Director de Organización y Calidad de los Servicios, aprobado en Consejo de Gobierno de la Junta de Andalucía con fecha 23 de julio de 2002.

De dicha formulación se pueden destacar los objetivos propuestos, los cuales delimitan estratégicamente las áreas funcionales y operativas en las que centraría la actuación este Centro:

- Coordinación de las políticas de seguridad.
- Custodia o almacenamiento de datos.
- Respaldo telemático remoto.
- Alta disponibilidad y continuidad informática de servicios críticos.

De acuerdo con estos objetivos, se abordó una fase inicial de planificación para el estudio del proyecto. Esta primera fase permitió obtener una planificación detallada de acuerdo con las principales metodologías para el análisis y gestión de riesgos en sistemas de información, especialmente para entornos relacionados con las Administraciones Públicas. En concreto, se hizo un especial esfuerzo para lograr una adecuación total al marco propuesto por las recomendaciones MAGERIT (Metodología de Análisis y Gestión de Riesgos de Sistemas de Información).

3. ANÁLISIS DE RIESGOS: ANÁLISIS Y VALORACIÓN DE LOS SISTEMAS CRÍTICOS

A continuación se abordó un estudio centrado en el "Análisis y Valoración de los Sistemas, Aplicaciones y Servicios Críticos, desde el punto de vista del Respaldo y la Continuidad Informática, en la Junta de Andalucía." El objetivo de este estudio se centró en la obtención de un dimensionamiento global de las necesidades en cuanto a respaldo y continuidad informática de los Servicios de Informática de los distintos organismos (consejerías e institutos) que forman la administración de la Junta de Andalucía.

Dado el amplio espectro de los sistemas objetivo de este estudio y la profundidad de la información necesaria para su realización, se propuso abordar en primer término una evaluación de la situación general de la Junta de Andalucía en los aspectos relacionados con el aseguramiento de la continuidad informática. Esta evaluación permitió obtener una visión general sobre los sistemas de los que dispone la Junta, su magnitud y su estado y permitió crear un plan de acción ajustado para la elaboración de un futuro análisis de riesgos de cada Consejería, atendiendo a su magnitud relativa y a la criticidad de los servicios que presta.

Esta evaluación recogió la información proporcionada por cada uno de los organismos acerca de:

- Configuraciones hardware y software de los sistemas de información.
- Aplicaciones y servicios que proporcionan al ciudadano y al propio personal de la administración.
- Volumen y tipos de datos.
- Medidas adoptadas para el aseguramiento de la continuidad

Además de los objetivos específicos de este estudio, como resultado de la realización del mismo se obtuvieron una serie de conclusiones de especial relevancia:

En cuanto administración, la Junta de Andalucía debe cumplir un conjunto de medidas acerca de seguridad informática, tales como mantenimiento de copias de seguridad, algunas de las cuales ya vienen exigidas por el propio tratamiento de ficheros con datos personales (de acuerdo con la LOPD). Además, las funciones propias de la sociedad de la información imponen nuevos requerimientos tanto en el ámbito del respaldo como la continuidad (servicios a ciuda-

danos disponibles las 24 horas del día durante todo el año, integración de estrategias multi-administraciones, etc.), lo que implica planes más sofisticados y ambiciosos de contingencias y continuidad en todos los sistemas de información.

En cuanto a tipos de servicios que las distintas consejerías necesitan se obtuvo una clasificación global en tres grandes apartados:

- Custodia de datos, es decir, almacenamiento seguro de los datos en una instalación distinta a la propia de la consejería donde se lleva a cabo la explotación y producción de la aplicación. Este servicio posee una motivación legal evidente que surge de la Ley Orgánica de Protección de Datos de Carácter Personal.
- Respaldo telemático de datos, es decir, estrategias que aseguren la no pérdida de datos durante la propia explotación de la aplicación. Esto exige no una mera custodia de los datos (generados mediante copias mensuales, semanales o diarias), sino la copia casi inmediata de los datos tal y como se generan.
- Continuidad ante contingencias. La dependencia funcional que crean los sistemas de información junto con las tendencia hacia una administración electrónica hacen que determinados servicios sean tan críticos que requieren una estrategia de continuidad (recuperación del servicio) ante una contingencia.

Además de obtener una imagen genérica de las necesidades en cuanto a respaldo y continuidad y un modelo operativo claro (tal y como se ha indicado en el punto anterior), éste estudio nos permitió obtener una primera valoración en cuanto a órdenes de magnitud en sistemas que requieren cada uno de estos servicios.

4. MAPA DE SERVICIOS CRÍTICOS Y CATÁLOGO DE CRITICIDAD.

A partir de los datos obtenidos mediante el estudio anterior, se realizó un estudio centrado en la obtención del "Mapa de Servicios Críticos y Catálogo de Criticidad" de los servicios prestados por la Junta de Andalucía.

Un primer objetivo de este estudio se centró en la obtención de un conjunto de índices de criticidad que pudiese ser utilizado como vector de parámetros para medir la criticidad de las distintas aplicaciones en particular y de las consejerías en general. Estos parámetros debían adaptarse a las características de una administración pública como es la Junta de Andalucía.

Se seleccionaron 3 criterios o parámetros básicos de criticidad:

- Tiempo máximo de indisponibilidad de los servicios / aplicaciones.
- Volumen de información crítica almacenada.
- Impacto del servicio. Este parámetro a su vez se divide en dos apartados, impacto en la propia administración en impacto en el servicio que la administración presta al ciudadano.

A continuación se llevó a cabo una catalogación de todas las consejerías y organismos autónomos analizando la infraestructura tecnológica. Esta línea de trabajo pretendía obtener un dimensionamiento objetivo para las necesidades del Centro de Respaldo. En concreto se analizaron tres dimensiones básicas:

- Capacidad de proceso
- Capacidad de almacenamiento

- Ancho de banda del sistema de comunicaciones

Por otro lado, se analizaron los distintos servicios prestados por las consejerías determinando su grado de criticidad (obtenido según el tiempo máximo de indisponibilidad especificado por los propios organismos responsables de los sistemas en cuestión).

El resultado de este estudio fue un mapa global de las necesidades de proceso, almacenamiento y comunicaciones de las distintas consejerías. Este mapa de infraestructuras tecnológicas, puesto en relación con el nivel de criticidad de cada una de ellas, permitió obtener un mapa de servicios críticos en la Junta de Andalucía.

Este mapa nos ha permitido obtener dos resultados cruciales. En primer lugar, el propio mapa nos da una indicación objetiva de los sistemas que actualmente requieren estrategias avanzadas de respaldo y continuidad. En segundo lugar, el nivel de criticidad de los distintos sistemas permitió abordar una estrategia de implantación por fases del Centro de Respaldo.

Los estudios relativos al análisis de sistemas críticos, mapa de criticidad, y el estudio de niveles de servicio y acuerdos contractuales para el Centro de Respaldo han sido realizados en colaboración con la empresa Profit Informática S.A.

5. DISEÑO DEL PROYECTO

El diseño del proyecto parte de la división funcional de la operativa del centro de respaldo y continuidad informática en dos servicios básicos: la salvaguarda de datos y la recuperación ante desastres. Estos servicios se organizan asimismo atendiendo a la criticidad de los propios sistemas de información. Los niveles de criticidad afectan a dos parámetros básicos: RPO (relacionado con el servicio de salvaguarda de datos) y RTO (relacionado con el servicio de recuperación ante desastres.

5.1 Salvaguarda de datos y recuperación ante desastres

El servicio de salvaguarda de datos incluye el transporte, la custodia y almacenamiento de datos a través de procesos de backups a cinta, para los Organismos de la Junta de Andalucía que requieran estos servicios y el respaldo telemático remoto para el resto de Organismos.

Por su parte, el servicio de recuperación ante desastres abarca el diseño, la implantación y la realización de los procedimientos necesarios para la recuperación y continuidad de las aplicaciones y sistemas informáticos de la Junta de Andalucía calificados como críticos de acuerdo a las diferentes modalidades de criticidad de los procesos.

Las actividades que se desarrollarán en el ámbito de este servicio son las siguientes:

- Recuperación de la operativa de los servicios en caso de desastre en el centro de Respaldo. Para ello, este centro debe disponer del número de servidores, capacidades de almacenamiento en disco y líneas de comunicaciones necesarias para dar servicio en situaciones de desastre en el plazo de tiempo definido por la Junta de Andalucía y recogidos en los ANS.
- Ejecución de pruebas anuales del Plan de Recuperación ante Desastres. Se contemplan dos pruebas anuales para cada Organismo dentro del ámbito del proyecto.
- Plan de Contingencia del Centro de Respaldo: diseño y realización de los procedimientos y herramientas para operar los sistemas informáticos en alta disponibilidad.

- Gestión de la actualización de la infraestructura HW-SW de Contingencias de manera que el Plan este vigente en todo momento.
- Gestión de los cambios necesarios en el Plan de Contingencias, en función de las actualizaciones HW-SW.
- Mantenimiento y actualización de los procedimientos de actuación incluidos en el Plan de Contingencias.
- Mantenimiento y actualización de la información de cada elemento identificado: ubicación o estado actual, posibles incidencias a las que esté expuesto, elementos relacionados a los que pueda repercutir la incidencia, descripción de actividades a realizar para maximizar la seguridad, y elaboración de un plan de controles específicos.

5.2 Perfiles de criticidad

Se han establecido 4 perfiles o niveles generales en cuanto a la criticidad de los servicios.

Es importante tener en cuenta que el proyecto exige dos funcionalidades básicas: salvaguarda de datos y recuperación ante desastres.

- La salvaguarda de datos minimiza la pérdida de datos implantando estrategias para el traspaso de datos desde los organismos respaldados hasta el Centro de Respaldo.
  Para cada nivel de criticidad se fija un tiempo máximo correspondiente al RPO *(Recovery Point Objective)*: antigüedad de los datos con los que se quiere ser capaz de recuperar un sistema en el caso de un desastre. Por ejemplo, si el RPO es de 4 horas, se pretende ser capaz de restaurar el sistema hasta un estado nunca anterior a 4 horas.
- La recuperación ante desastres minimiza el impacto de una pérdida de servicio posibilitando que el Centro de Respaldo asuma la funcionalidad del servicio que ha sufrido un desastre.
  Para cada nivel de criticidad se fija un tiempo máximo correspondiente al RTO *(Recovery Time Objective)*: tiempo necesario para llevar a cabo la recuperación de un servicio ante un desastre, o de otra forma, tiempo máximo de indisponibilidad del sistema.

De acuerdo con estos criterios, los niveles o perfiles fijados son:

- Servicio de Criticidad Muy Alta
  - RPO: 1 hora (Copia remota por un periodo nunca superior a una hora)
  - RTO: 4 horas (Recuperación del servicio con un tiempo máximo de cuatro horas)
- Servicio de Criticidad Alta
  - RPO: 4 horas (Copia remota por un periodo nunca superior a cuatro horas)
  - RTO: 12 horas (Recuperación del servicio con un tiempo máximo de doce horas)
- Servicio de Criticidad Media
  - RPO: 12 horas (Copia remota por un periodo nunca superior a doce horas)
  - RTO: 24 horas (Recuperación del servicio con un tiempo máximo de veinticuatro horas)
- Servicio de Criticidad Baja
  - RPO: 24 horas (Copia remota por un periodo nunca superior a veinticuatro horas)
  - RTO: 48 horas (Recuperación del servicio con un tiempo máximo de cuarenta y ocho horas)

Estos criterios aplicados sobre los servicios marcarán la criticidad de las aplicaciones y las plataformas que las ejecutan.

6. ESTADO ACTUAL DEL PROYECTO FÉNIX

Desde el punto de vista administrativo, la fase de licitación de este proyecto se realizó durante el último trimestre de 2003. Una vez adjudicato el proyecto a la empresa Telvent Interactiva S.A., la ejecución efectiva del proyecto se inició en marzo de 2004.

Teniendo en cuenta la envergadura del proyecto (en total quedan incluidos 129 servicios críticos), el proyecto prevée un plan de transición o integración de los distintos organismos que se desarrollará fundamentalmente durante 2004, con el objetivo de que a principios de 2005 todos los sistemas críticos identificados queden integrados con el proyecto.