VII JORNADAS SOBRE TECNOLOGÍAS DE LA INFORMACIÓN PARA LA MODERNIZACIÓN DE LAS ADMINISTRACIONES PÚBLICAS
A CORUÑA
15, 16, 17 y 18 de octubre de 2002
Palacio de Congresos y de la Ópera
www.tecnimap.com
Ponencias

Seguridad, Respaldo, Continuidad y Alta Disponibilidad en el ámbito de la Administración Electrónica: Diseño del Centro de Respaldo y Hospedaje de la Junta de Andalucía

José F. Quesada
Gabinete de Sistemas Informáticos Horizontales
Servicio de Coordinación Informática
Dirección General de Organización, Inspección y Calidad de los Servicios
Consejería de Justicia y Administración Pública
Junta de Andalucía

Jesús Porras
PROFit

1. Seguridad, Respaldo, Continuidad Informática y Alta Disponibilidad ante Desastres

El Centro de Seguridad, Respaldo y Continuidad Informática de la Junta de Andalucía surge como una solución de carácter general y como servicio de aplicación horizontal en el ámbito de la infraestructura, aplicaciones y servicios propios o relacionados con las Tecnologías de la Información y las Comunicaciones de la Junta de Andalucía.

1.1. Motivación Funcional y Tecnológica

No cabe duda que en el marco de una administración pública involucrada en un proceso de informatización de la mayor parte de los servicios que presta al ciudadano y de su propio funcionamiento interno, las tecnologías de la información y las comunicaciones juegan un papel principal como infraestructura tecnológica vertebradora.

Pero este mismo papel crucial hace que las posibles vulnerabilidades de esta infraestructura tecnológica la conviertan en un objetivo crítico en cuanto a su protección. La información, su almacenamiento y tratamiento a través de servicios y aplicaciones, y el propio flujo de la misma por distintas redes de telecomunicación, hace que tanto los datos como las aplicaciones y las redes constituyan bienes que requieren una especial atención en cuanto a la gestión de su seguridad.

1.2. Convergencia de las Estrategias de Seguridad

Recientemente se ha producido una convergencia en la planificación de los mecanismos de seguridad (respuesta ante incidentes de seguridad informática) tanto de índole natural (tolerancia ante desastres tales como terremotos, inundaciones, etc.) como de índole tecnológica (ciber-ataques y sus consecuencias en una administración pública, tales como denegación de servicios, fraude, etc.).

Además se pretende lograr la integración de estos enfoques con la planificación general de seguridad ante alteraciones propias de los sistemas informáticos (deterioro físico de los componentes hardware y errores de funcionamiento de los componentes software).

1.3. Hacia un Enfoque basado en la Seguridad Activa

Por otro lado, una planificación coherente de un sistema general y horizontal de seguridad informática para una institución con la dimensión de la Junta de Andalucía necesita incorporar no sólo un enfoque reactivo o de seguridad pasiva orientado hacia la recuperación ante incidentes, sino además un enfoque proactivo o de seguridad activa orientado hacia la prevención.

Es decir, será necesario contemplar todos los aspectos relacionados con la gestión de incidentes de seguridad.

A este nivel, resulta útil utilizar como hilo conductor el ciclo de incidentes de seguridad (prevención, detección, respuesta y corrección) para llevar a cabo el estudio de los principales objetivos que se deben abordar así como la planificación general del Centro de Seguridad, Respaldo y Continuidad Informática.

1.4. El CSRC:
Un compromiso de calidad en la gestión de los servicios por parte de la Administración de la Junta de Andalucía

Como resumen de esta sección dedicada al estudio del marco de implantación es importante resaltar que el CSRC surge como una propuesta de un servicio que se podría catalogar dentro del ámbito de las tecnologías avanzadas de información y telecomunicaciones.

La propuesta, coordinada desde el Servicio de Coordinación Informática, pretende abarcar funcionalmente a todo el ámbito de la Administración de la Junta de Andalucía.

Teniendo en cuenta el carácter crítico de la información, su gestión a través de servicios y su transmisión a través de redes de comunicaciones, el CSRC pretende dotar de una estructura coordinada en cuanto a políticas de seguridad, respaldo y continuidad informática, así como de la infraestructura tecnológica necesaria para cubrir dichas políticas.

2. Gestión Global de la Seguridad: Prevención, Detección, Respuesta y Corrección

Un modelo canónico de ciclo de incidentes de seguridad que una organización necesita gestionar consta de cuatro fases o elementos:

1. La amenaza,
2. El incidente (como por ejemplo, un ataque),
3. El daño producido como resultado del incidente, y
4. La recuperación.

De forma paralela a estas fases de un incidente de seguridad aparecen otras cuatro medidas de seguridad:

2.1. Prevención

Básicamente el objetivo de esta medida de seguridad es prevenir que una amenaza se convierta en realidad o reducir la probabilidad de su ocurrencia. En este apartado se pueden situar:

- Los sistemas de cortafuegos (firewall),
- Los mecanismos de escaneo de vulnerabilidades conocidas en un sistema de información en red,
- La instalación de parches, y
- Otras medidas de reducción de riesgos orientadas a la minimización de los posibles daños derivados de un ataque, como la realización de copias de seguridad (back-ups).

2.2. Detección

Por su propia naturaleza, la prevención no excluye la ocurrencia de posibles incidentes. Por tanto, se deben definir procedimientos para lograr la detección e identificación de cualquier incidente (intrusión, ataque, etc.) tan pronto como sea posible con el objetivo de activar las acciones necesarias de respuesta.

2.3. Respuesta

Una vez que un incidente ha ocurrido y ha sido detectado, la organización debe poner en funcionamiento las acciones pertinentes que minimicen los posibles daños que el incidente pueda causar. Por ejemplo, una respuesta podría ser aislar los sistemas computacionales de la organización de la red pública. Las medidas de respuesta pueden incluir asimismo la realización de trazas del incidente así como la recopilación de todas las evidencias en torno al propio incidente.

2.4. Corrección

Cuando como consecuencia de un incidente se produce un daño en la integridad, confidencialidad o disponibilidad de la información o servicios contenidos o manejados a través de la red y los sistemas de información, el siguiente paso se

debe centrar en la ejecución de medidas correctivas que aseguren la continuidad de los servicios y la restauración de los daños sufridos.

2.5. Ciclo holístico de gestión y respuesta ante riesgos

Las principales acciones a nivel europeo (por ejemplo, el *eEurope Action Plan*) se han centrado tradicionalmente en algunos aspectos del ciclo de gestión y respuesta ante riesgos presentado en los apartados anteriores. Por ejemplo, los denominados CERTs (*Computer Emergency Response Teams*) y CSIRTs (*Computer Security Incident Response Teams)* se han centrado en la anticipación y reacción ante incidentes y ataques a redes de ordenadores. Tanto los CERTs como los CSIRTs tienen una función especialmente importante en la detección de incidentes y la generación de avisos y alertas que permiten iniciar el ciclo de respuesta y prevención.

De forma similar, el *eEurope Action Plan* se ha centrado en "la estimulación pública y privada para la cooperación sobre la fiabilidad de infraestructuras de información (incluyendo el desarrollo de sistemas de alerta rápida o temprana) y el refuerzo de la cooperación entre los CERTs nacionales."

No obstante, los últimos proyectos europeos están insistiendo en la necesidad de adoptar un enfoque holístico o general de gestión y respuesta ante riesgos que incluya las fases de prevención, detección, respuesta y corrección.

En el marco de este objetivo global ha surgido la propuesta EUROPEAN WARNING & INFORMATION SYSTEM (EWIS), promovida inicialmente por el Joint Research Centre de la Comisión Europea y el proyecto DDSI (Dependability Development Support Initiative Project – IST-2000-29202) financiado por el programa IST (Information Society Technologies) del 5º Programa Marco Europeo de Investigación.

Entre las conclusiones de la reunión celebrada los días 25 y 26 de Octubre de 2001 relativa a EWIS merecen la pena citar las siguientes: *"Compartir información es un tema crítico para asegurar la fiabilidad de la infraestructura de información de Europa y las infraestructuras globales más amplias en las que las primeras están basadas. Compartir información es algo necesario para lograr una alerta temprana de fallos, vulnerabilidades y amenazas e incidentes pero debe ser parte de una respuesta holística. Sobre esto se deben montar las buenas prácticas y relaciones ya existentes, pero el entorno nuevo e interdependiente requerirá nuevos paradigmas que permitan que la información traspase los límites sectoriales".*

3. Planificación

Con carácter general, todas las metodologías relacionadas con el diseño e implantación de sistemas de información han venido prestando una mayor anterior a las tareas relacionadas con la propia planificación de los proyectos.

En particular, la principal metodología aplicable a nivel nacional para el ámbito de la seguridad informática (*MAGERIT: Metodología de análisis y gestión de riesgos de los sistemas de información*) insiste claramente en la importancia de la fase o etapa inicial de planificación.

Para el proyecto CSRC se ha diseñado una etapa primera centrada en la planificación del proyecto en la que se abordan cuatro frentes fundamentales de trabajo o grandes actividades en torno a las cuales se han estructurado las tareas concretas que se llevarán a cabo.

3.1. Dirección y Coordinación

La primera actividad (***Dirección y Coordinación***) aborda las tareas relacionadas con la dirección y coordinación del proyecto durante la etapa de planificación.

Esta actividad incluye la definición y el control del **plan de trabajo** que se va a desarrollar durante la etapa completa.

Asimismo se define detalladamente el **cronograma**.

Una de las principales tareas de esta actividad es el análisis y determinación de los **objetivos** del CSRC.

Asimismo esta actividad incluirá la recopilación de la **normativa legal vinculante** en cuanto a seguridad informática.

Por último, esta actividad culmina los trabajos realizados en esta etapa proponiendo una **planificación de la siguiente etapa** del proyecto, básicamente dirigida al análisis de riesgos, y que supondrá el estudio de los planes de contingencia y continuidad a implementar en el Centro de Seguridad, Respaldo y Continuidad Informática.

3.2. Análisis y Valoración de Sistemas, Aplicaciones y Servicios Críticos

Además de las tareas relacionadas con el control, dirección y coordinación de la planificación, un aspecto crucial en esta fase del trabajo es conocer los servicios de informática que actuarán como centros de producción y gestión de

cara a la labor de seguridad, respaldo, continuidad, hosting y housing. Es evidente que una buena planificación del CSRC exige conocer las necesidades de los organismos a los que prestará sus servicios. Para lograr este objetivo se ha diseñado la segunda actividad: **Análisis y Valoración de Sistemas, Aplicaciones y Servicios Críticos.**

Además de la necesaria coordinación que esta actividad requiere debido a la complejidad intrínseca que presenta, esta actividad incluye la **elaboración de un cuestionario específico para la recogida de datos** en todas las consejerías e institutos de la Junta de Andalucía, así como la **organización de las entrevistas.**

La labor más compleja de esta actividad será la realización de las propias **entrevistas,** y tras la realización y recogida de datos se llevará a cabo un **análisis y valoración de la información** obtenida.

Esta información permitirá abordar un **estudio de los planes de contingencia y continuidad** necesarios, aunque el análisis detallado de estos se abordará en la etapa 2 del proyecto.

3.3. Prospección Tecnológica

La tercera actividad tiene como objetivo estudiar y analizar la tecnología disponible actualmente. Se trata por consiguiente de un trabajo dirigido a la **prospección tecnológica** que permita conocer detalladamente los productos principales disponibles por las empresas del sector.

Esta tarea incluye la realización de entrevistas con responsables de distintas empresas en distintos sectores tecnológicos, y especialmente en sistemas de almacenamiento, software de backup, estrategias de virtualización de datos e información, sistemas gestores de bases de datos, relación entre comunicaciones y estrategias de respaldo y continuidad, etc.

Asimismo como parte de esta actividad se incluye una tarea dirigida al estudio y análisis de **centros similares**.

3.4. Diseño y Marco de Implantación

Esta actividad incluye todas las tareas relacionadas con el diseño mismo del Centro de Seguridad, Respaldo y Continuidad Informática como resultado de todo el trabajo en la etapa. Es decir, la etapa en su conjunto finaliza con una propuesta de diseño del Centro.

Este diseño parte de un estudio inicial de las **políticas de implantación** aplicables al centro, específicamente las políticas de seguridad, respaldo, continuidad y alta disponibilidad, hosting y housing. Esta tarea depende en gran medida de los resultados obtenidos en la tarea I.2.5 (*Análisis y valoración de sistemas, aplicaciones y servicios críticos*), y por otro lado constituye, junto con el resultado de la tarea I.2.6 (*Análisis de planes de contingencia y continuidad*), el punto de partida para el diseño y puesta en funcionamiento de los planes de contingencia y continuidad correspondientes a las etapas II (*Análisis de riesgos para los sistemas de información*) y III (*Gestión de riesgos*) del proyecto.

A continuación, la segunda tarea aborda una propuesta detallada de las **características básicas, funciones y servicios** del Centro. Evidentemente, esta tarea actúa como vértice de fusión del trabajo sobre *Análisis y determinación de objetivos* (Tarea I.1.3), *Análisis y valoración de sistemas, aplicaciones y servicios críticos* (Tarea I.2.5) y *Análisis y prospección de tecnología, empresas y productos* (Tarea I.3.1).

A continuación se detallará tanto el **marco tecnológico** que se utilizará como referencia para el diseño del centro como el **marco normativo y acuerdos de participación y co-financiación**.

La tarea I.4.5 (**Marco de implantación**) aborda básicamente la selección de la sede para el CSRC, su acondicionamiento para albergar las funciones asignadas, una valoración de inversiones en cuanto a infraestructuras, así como una estimación de las necesidades de personal.

Por último, como resultado final de toda la etapa se aborda el Diseño del Centro de Seguridad, Respaldo y Continuidad Informática. Dentro de esta fase de Diseño, se han realizado dos estudios dirigidos a un dimensionamiento detallado de las necesidades en cuanto a seguridad, respaldo, continuidad y alta disponibilidad en toda la Junta de Andalucía. Las siguientes secciones describen los objetivos y líneas de trabajo de estos dos subproyectos.

4. Análisis y valoración de los Sistemas, Aplicaciones y Servicios críticos, desde el punto de vista del respaldo y continuidad informática, en la Junta de Andalucía

Para la primera etapa de Análisis y valoración de los Sistemas, Aplicaciones y Servicios críticos, desde el punto de vista del respaldo y continuidad informática, en la Junta de Andalucía, se confeccionaron una serie de cuestionarios, que permiten obtener gran cantidad de información de forma paralela. Dichos cuestionarios fueron entregados, y debidamen-

te explicados, a los responsables de su cumplimentación designados por cada Consejería/Instituto.
Básicamente, la información solicitada a dichos responsables se puede agrupar en torno a dos áreas:

- Entorno Tecnológico
- Servicios, Aplicaciones y Datos

En concreto, la información requerida fue la siguiente:

Entorno Tecnológico de cada Consejería, donde figure:

- Hardware de Proceso, de Almacenamiento, de Interfaz, Servidores, Terminales y otros.
- Software de Base, de Gestión, de Monitorización, Programas-Producto y otros.
- Topología de Comunicaciones (Redes Propias y Servicios Contratados).

Especificando la Denominación y Ubicación de cada uno de los elementos del Entorno, así como:

- Características técnicas principales (capacidad de proceso, de almacenamiento, de respuesta, etc.).
  - Criticidad y Redundancia del elemento.
  - Procesos soportados.
  - Incidentes sufridos por el elemento (causas y tiempos de reparación).
  - Proveedor del elemento y existencia de Contrato de Mantenimiento.

Servicios, Aplicaciones y Datos proporcionados por cada una de las Consejerías, donde figure:

- Servicios actualmente prestados por la Consejería, y su ámbito.
- Aplicaciones de Negocio, especificando:

  - Responsable, usuarios y ámbito de actuación de las mismas.
  - Criticidad en el tiempo y Restricciones de Uso/Seguridad.
  - Existencia de Acuerdos de Nivel de Servicio.
  - Alternativas al aplicativo en caso de indisponibilidad total del mismo.
  - Volumen de operaciones realizadas por la Aplicación (transacciones, altas/bajas, etc).
  - Incidencias más reseñables detectadas y tiempo de resolución.

- Datos, especificando:
  - BBDD y relación con las Aplicaciones de Negocio y/o áreas usuarias.
  - Entorno Tecnológico que soporta dichas BBDD.
  - Existencia de Catálogo de Datos y Procedimientos de Backup (frecuencia y calidad).

Los cuestionarios se estructuraron conforme al siguiente esquema:

- NIVEL DE ENTORNO
  - Ubicación
  - Accesos
  - Suministros
- NIVEL DE SERVICIOS
  - Externos (al ciudadano)
  - Internos
  - Contingencia
- NIVEL DE COMPONENTES
  - Tecnológicos
    - Hardware
      - Proceso
      - Almacenamiento
      - Servidores
      - Comunicaciones
      - Terminales/Impresoras
      - Puestos Personales
    - Software
      - Sistema Operativo
      - Almacenamiento
      - Comunicaciones
      - Gestores de BBDD
      - Utilidades
      - Correo Electrónico
      - Backup/Restore
    - Topología de Comunicaciones
      - Redes Propias
      - Servicios Contratados
  - Aplicaciones y Datos
    - Aplicaciones
      - Externas
      - Internas
    - Datos
      - Externos
      - Internos

5. Mapa de Criticidad para Servicios y Aplicaciones

La evaluación efectuada tras la anterior Propuesta de Colaboración ("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") ha permitido obtener una visión general sobre los Sistemas de los que dispone la Junta, su magnitud y su estado. Como resultado de la mencionada colaboración, se recogió la siguiente información de cada uno de los Organismos (Consejerías e Institutos) dependientes de la Junta:

- Configuraciones Hardware y Software de los Sistemas de Información.
- Aplicaciones y Servicios que proporcionan dichos Organismos al ciudadano y al propio personal de la administración.
- Volumen y tipo de datos.
- Medidas adoptadas, con respecto a los puntos anteriores, para el aseguramiento del respaldo y la continuidad.

Tras la evaluación de dicha información, y tomando como base los comentarios surgidos en las entrevistas personales con los responsables técnicos de cada Organismo, se resaltaron los siguientes factores como determinantes a la hora de catalogar los distintos Servicios y Aplicaciones:

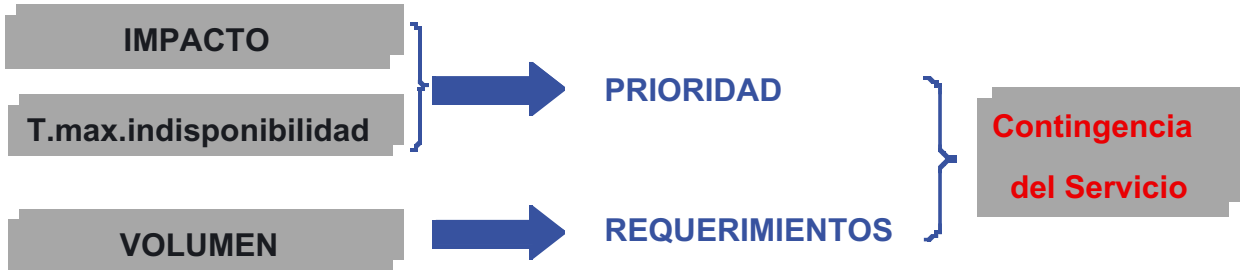
- Impacto del Servicio sobre el usuario (administrado), para los Servicios de tipo vertical (Servicios Externos).
- Impacto del Servicio sobre la Administración, para los Servicios de tipo horizontal (Servicios Internos).
- Para ambos tipos de Servicios, tiempo máximo de indisponibilidad admisible.
- Igualmente, para ambos tipos de Servicios, volumen de la información gestionada y almacenada por los mismos.

Esto ha facilitado identificar aquellos Indicadores que mejor definirán el grado de criticidad que caracterizará a cada uno de los Servicios críticos inventariados.

En relación con los factores reseñados, vamos a considerar pues los siguientes Indicadores de Criticidad (IC) :

- Impacto del Servicio (externo, interno).
- Tiempo máximo de indisponibilidad admisible (< 1 hora, < 1 día, < 1 semana).
- Volumen de la información (con respecto a los datos almacenados, capacidad de proceso necesaria y ancho de banda requerido para el transporte de estos datos).

Los IC de Impacto y de Tiempo máximo de indisponibilidad establecerán la prioridad de inclusión del Servicio en el Plan Marco de Continuidad. El IC de Volumen (procesador, almacenamiento más comunicaciones) determinará los requerimientos técnicos a tener en cuenta para el rearranque del Servicio en situación de contingencia.



Con el fin de facilitar el estudio de los resultados, hemos procedido a tipificar la gran cantidad de datos obtenidos basándonos, en primer lugar, en el IC de Volumen, por su utilidad en el dimensionamiento del futuro Centro de Seguridad,

Respaldo y Continuidad Informática. Así pues, para cada Consejería e Instituto, se mostrara:

- Unidades mínimas de Proceso necesarias.
- Almacenamiento mínimo necesario.
- Ancho de Banda mínimo para soportar el entorno de Comunicaciones.

Además de este indicador, consideramos imprescindible reseñar también los Servicios críticos prestados por cada Consejería e Instituto, ya que su determinación y valoración fue el objetivo central de las entrevistas para la recogida de los Cuestionarios, y cuantificar la criticidad de dichos Servicios, según el criterio de los entrevistados, tomando como primer IC el Impacto (vertical y horizontal) del Servicio y como segundo IC el máximo Tiempo de indisponibilidad admisible para el mismo.