353

IMPLANTACIÓN DE UNA SOLUCIÓN DE RESPALDO, ALTA DISPONIBILIDAD Y CONTINUIDAD EN EL ÁMBITO DE LOS ENTORNOS CRÍTICOS

Manuel Escudero Sánchez
Director General de Informática
Consejería de Economía y Hacienda.
Comunidad Autónoma de la Región de Murcia.

Elena González Arnal
Jefe de Servicio de Sistemas Informáticos
Dirección General de Informática. Consejería de Economía y Hacienda.
Comunidad Autónoma de la Región de Murcia.

Joaquin Matás Gambín
Técnico de Gestión Informática
Dirección General de Informática. Consejería de Economía y Hacienda.
Comunidad Autónoma de la Región de Murcia.

Manuel Frutos Mirete
Subdirector General de la Inspección General y Calidad de Servicios
Dirección General de Informática. Consejería de Economía y Hacienda.
Comunidad Autónoma de la Región de Murcia.

Manuel Escudero Sánchez
Elena González Arnal
Joaquin Matás Gambín
Manuel Frutos Mirete

Palabras clave

Almacenamiento, salvaguarda, seguridad, fiabilidad, disponibilidad, robustez, continuidad, plan de contingencias.

Resumen de su Comunicación

La Dirección General de Informática está desarrollando una estrategia de modernización y unificación de las infraestructuras para dar respuesta a las necesidades en el manejo de la información de los sistemas corporativos del Gobierno Regional.

La clara apuesta hacia una estrategia de e-administración conlleva dotarse de infraestructuras robustas y fiables, que permitan continuidad del servicio y una disponibilidad de 24x7.

La Dirección General ha planteado un proyecto de ***integración de los servicios*** *críticos en un sistema unificado de almacenamiento, salvaguarda y seguridad, que permita una solución de alto valor, que garantice los requisitos planteados por estos sistemas de información y permita una flexibilidad y escalabilidad adecuadas para el funcionamiento, desarrollo y crecimiento de dichos entornos .*

La solución planteada ha constado de los procesos de estudio de la información crítica y sus necesidades de manejo, definición y diseño de un sistema de almacenamiento de alta disponibilidad, adecuación y redefinición de las estrategias de seguridad (políticas de backup, planes de contingencia) e integración y migración de los sistemas críticos al nuevo entorno.

El proyecto ha permitido, no solo, conseguir los objetivos planteados, sino fijar las bases para futuras acciones en la implantación efectiva de un CPD de respaldo y en la consolidación y gestión del ciclo de vida de la información.

Manuel Escudero Sánchez
Elena González Arnal
Joaquin Matás Gambín
Manuel Frutos Mirete

IMPLANTACIÓN DE UNA SOLUCIÓN DE RESPALDO, ALTA DISPONIBILIDAD Y CONTINUIDAD EN EL ÁMBITO DE LOS ENTORNOS CRÍTICOS

La Dirección General de Informática, de la Consejería de Economía y Hacienda, de la Comunidad Autónoma de la Región de Murcia tiene atribuidas las competencias en materia de Sistemas de Información y Aplicaciones Informáticas Corporativas. Dentro de su política técnica, se plantea el acotar los niveles de servicio ofrecidos a los usuarios (disponibilidad, confiabilidad, ...) mediante el diseño de actuaciones tendentes a conseguirlos. Uno de los aspectos fundamentales que se identificó fue la mejora del sistema de respaldo de la información, para conseguir una mayor disponibilidad de los mismos y mejorar el sistema de backup.

1. Identificación de los objetivos

Durante el análisis del problema para la búsqueda de soluciones adecuadas a las cuestiones planteadas se identificaron una serie de objetivos:

• Continuidad de servicio. La puesta en servicio de aplicaciones de administración electrónica obligan a acercarse a un servicio con disponibilidad cercana al 24x7. Esta disponibilidad podría verse comprometida por caída o fallo en alguno de los nodos. En la actualidad se afectada por los fallos ya mencionados y por paradas programadas debido a la necesidad de realizar copias de seguridad. El sistema objetivo implicará necesariamente que, para los sistemas de información identificados como críticos, haya una garantía de no interrupción del servicio durante el proceso de back-up (copias de seguridad).

• Mejora del sistema de backup. Minimizar las amenazas a la disponibilidad de los sistemas y en caso de caída o fallo de alguno de los elementos que impliquen almacenamiento aplicar medidas para que el tiempo de "no-disponibilidad" del servicio se reduzca a intervalos de tiempo acotados y predeterminados. Siendo este intervalo de tiempo un indicador del nivel de servicio perseguido.

• Reducción en la ventana de recuperación de los servicios. En caso de que se produjera una situación que llevara a la recuperación desde copia de seguridad de alguno de los servicios, es necesario que la ventana temporal de restauración del servicio se reduzca a un intervalo temporal y una posible pérdida de información aceptable por el responsable del sistema de información.

2. Sistemas críticos

Una vez planteadas las grandes líneas de actuación se procedió a la identificación de los sistemas críticos y a la recogida de datos que permitiera acotar el alcance y dimensionamiento de la solución buscada, con respecto al nivel de servicios que esperaban los responsables de las aplicaciones.

2.1 Identificación de los Sistemas Críticos

De todos los sistemas que se gestionan desde la Dirección General de Informática, se destacaron aquellos que tenían una mayor importancia en cuanto al impacto en caso de no disponibilidad.

Los sistemas críticos que se identificaron fueron cinco: Plataforma de Administración Electrónica, Gestión de Personal, Gestión Económico Presupuestaria, Correo Electrónico, Soporte a la red local.

2.2 Formulario de definición de planes de continuidad

Se identificaron un conjunto de preguntas básicas que debían ser respondidas por los responsables funcio-

Volver

nales de cada uno de los Sistemas de Información, al objeto de poder diseñar la infraestructura de back-up necesaria.

Para la realización de estas preguntas se diferenciaron los conceptos de COPIA de la información y de RESTAURACIÓN de la misma.

Se entiendo por procesos de COPIA aquellos que tienen como objetivo salvaguardar la información de forma que tengamos posibilidad de recuperación en caso de pérdida accidental, rotura de equipos o catástrofe, o así sea requerido por otros motivos.

En cuanto a los procesos de RECUPERACIÓN tendrán como objetivo la restauración de la información previamente copiada de forma que un sistema pueda estar operativo y funcional a una hora/fecha anterior a la actual, o al instante en que se produjo un incidente.

Proceso de copia. Las preguntas que se plantearon fueron las siguientes:

a) Cuanto tiempo puede estar parado el Servicio para realizar una copia de su información de forma consistente.

Esta pregunta incide en la necesidad que existe en algunos casos de parar un servicio para poder asegurar que la copia que vamos a realizar sea consistente y ofrezca garantías de ser recuperada con éxito.

b) Cuando se puede parar el Servicio.

Con esta pregunta se obtiene la idea de la franja horaria en que se debe realizar la copia de la información en el caso que sea necesaria una parada del servicio.

c) Cuanto tiempo deberían conservarse las copias.

En algunos casos, motivos legales pueden ser condicionantes importantes en este sentido. La respuesta a esta pregunta, entre otras cosas, hace reflexionar sobre temas de archivado de información poco o nada accedida, ciclo de vida de la información, información online/offline, etc.

Otro aspecto a cubrir con esta pregunta será, obviamente, la determinación de hasta donde vamos a estar dispuestos a retroceder en caso de restauración.

Proceso de restauración. En este apartado se distinguen dos escenarios diferentes susceptibles de generar respuestas distintas para las mismas preguntas. Nos vamos a plantear la restauración de un sistema teniendo en cuenta que hubiera que realizarla sobre el mismo sistema donde está funcionando habitualmente o sobre un sistema diferente.
• Restauración sobre el mismo equipo. Se refiere a la motivada por un error lógico, degradación del Sistema Operativo u otro tipo donde no exista un error grave de hardware.

a. Ventana posible de vuelta atrás.
Se quiere averiguar hasta donde se va a necesitar dar marcha atrás en el tiempo. Será necesario afinar bien en la contestación, siendo recomendable plantear simulaciones apropiadas.

b. Tiempo máximo permitido para reestablecer el servicio.
Se refiere al tiempo de inactividad del servicio que se está dispuesto a asumir hasta de su restauración y puesta en funcionamiento.
c. Asumible pérdida parcial de información.
Se evalúa la posibilidad de que en caso de incidente se pueda asumir la pérdida de información de un inter-

valo de tiempo.

• Restauración sobre equipos diferentes. Serán roturas irreparables de equipos e incluso desastres naturales o incendios del propio Centro de Proceso de Datos. Aunque las preguntas a plantear serían las mismas que en apartado anterior, hay que ser conscientes de que se hace referencia a incidentes graves que podrían justificar que se asumieran tiempos mayores que en el apartado anterior.

a. Ventana posible de vuelta atrás.
b. Tiempo máximo permitido para reestablecer el servicio.
c. Asumible pérdida parcial de información.

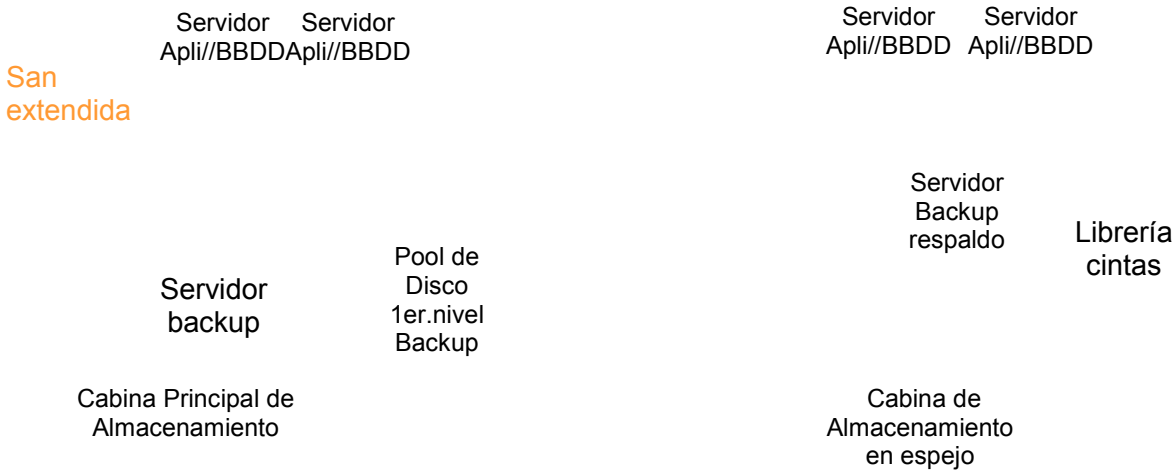
El formulario, para cada servicio crítico, a rellenar quedó de la siguiente manera.

3. Análisis del sistema

Con toda la información recopilada de los servicios críticos se empezó a trabajar el análisis de la solución de deseada.

Se identificaron una serie de premisas, que condicionaban las posibles alternativas. Así se partía de la posibilidad de tener dos ubicaciones físicas separadas, dos centros de proceso de datos (CPD en adelante), con las condiciones adecuadas de espacio, condiciones eléctricas, de aire acondicionado, etc. Se disponía además de una serie de elementos físicos (como una librería de cintas) que por su funcionamiento y reciente adquisición, se deseaba que formaran parte de la configuración final.

El estudio de los requisitos planteados llevó a la definición del siguiente esquema:



Volver

San Extendida: Será la base de toda la infraestructura para conseguir una mejora en los tiempos de "backup" y "restore". Así mismo, aislará el tráfico pesado de backup de las redes de negocio. Asumirá todo el tráfico para las copias y restauraciones. Los equipos de la solución planteada estarán conectados a esta red (dispondrán de los adaptadores FibreChannel correspondientes).

Cabina principal de almacenamiento: Todo el almacenamiento estará consolidado aquí. Estará situada en el CPD Principal. Para los datos críticos con necesidades de copia y restauración muy rápidos, proporcionará herramientas para la realización de copias instantáneas. Será lo suficientemente potente y escalable para soportar la carga necesaria. Las copias instantáneas tendrán que ser convenientemente desarrolladas y procedimentadas para su uso en caso de necesidad.

Gestor de backup: Gestionará los procesos de copia y restauración de la información a excepción de los relativos a la estrategia de copias instantáneas que estarán implementados a través de la tecnología que nos proporcione la cabina principal de almacenamiento. Se integrará con las copias instantáneas de forma que, para los servicios críticos, lleguemos a conseguir soluciones de copias desatendidas, sin ventana de tiempo y sin impacto en el rendimiento normal de dichos servicios.

Será capaz de abarcar toda la problemática de copias necesaria para una buena solución de backup general:

- Sistemas Operativos: Fundamentalmente Windows 2000-2003, Linux RedHat.

- Copias incrementales para restauraciones totales o parciales.

- Aportará soluciones específicas para copias y restauraciones de productos concretos: BBDD Oracle, SAP, correo (notes, exchange), novell.

El servidor de backup estará instalado en alta disponibilidad.

La instalación del servidor de backup contemplará la posibilidad de recuperación de información en caso de un desastre en el CPD Principal y que pueda suponer la destrucción del servidor de backup ubicado en dicho centro.

Complementando una solución de backup típica, se contemplará la gestión de creación de imágenes en caliente para restauraciones rápidas de todo el sistema. (solución disaster recovery rápida de un servidor).

El gestor de backup tendrá que soportar redes SAN, de forma que los clientes puedan utilizarla para enviar información a cualquier dispositivo de backup integrado en la misma.

Pool de disco: Rapidez en la realización de las copias de seguridad.
Supondrá una cabina de discos conectada directamente a la San extendida (o podrá estar ligada físicamente al servidor de backup)

Librería de cintas: Estará situada físicamente en un CPD Secundario, conectada a la San extendida. Será el medio de almacenamiento de siguiente nivel al pool de disco utilizado por el servidor de backup.

Cabina de almacenamiento en espejo: Estará ubicada en un CPD Secundario y actuará como espejo de la información crítica almacenada en la cabina principal de almacenamiento del CPD Principal.
Con tres objetivos claros:

• Actuar como almacenamiento principal en caso de caída de la cabina de almacenamiento situada en el CPD Principal. La presentación de sus unidades a los Servidores de Aplicaciones y BBDD tendrá que estar

Manuel Escudero Sánchez
Elena González Arnal
Joaquin Matás Gambín
Manuel Frutos Mirete

convenientemente documentada y procedimentada. Dichos Servidores tendrán acceso a este almacenamiento haciendo uso de la San extendida.

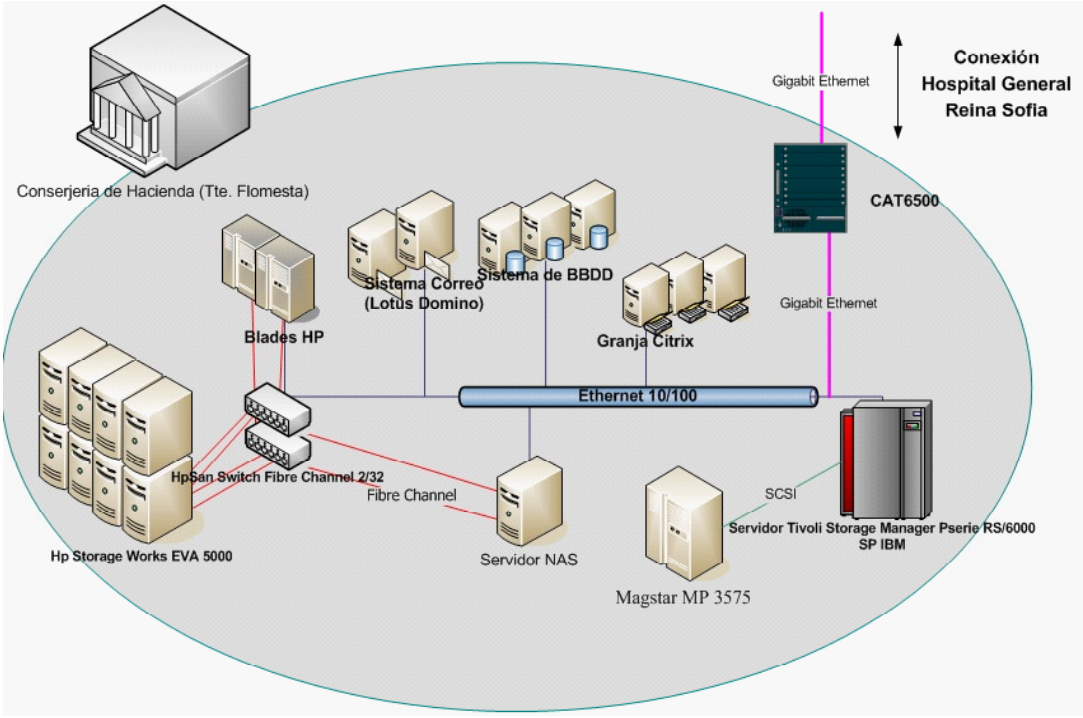
• Actuar como almacenamiento principal en caso de desastre del CPD Principal. Para que esta solución tenga sentido, asumimos que existen Servidores de Aplicaciones y BBDD preparados en el CPD Secundario.

• Seguridad, al disponer de un segundo almacenamiento en línea con la información crítica de la organización.

4. Situación Inicial

La situación de partida era que el sistema de backup se encontraba en fase de migración del Sistema de Copias de seguridad, desde un entorno en el que se encontraba un sistema de copias basado en una librería de cintas y un servidor de copias, ubicados en el mismo CPD, junto con los diferentes entornos (clientes) a copiar, hacia un sistema de copias donde la librería de cintas y el servidor de copias se encuentran ubicados en una localización diferente.

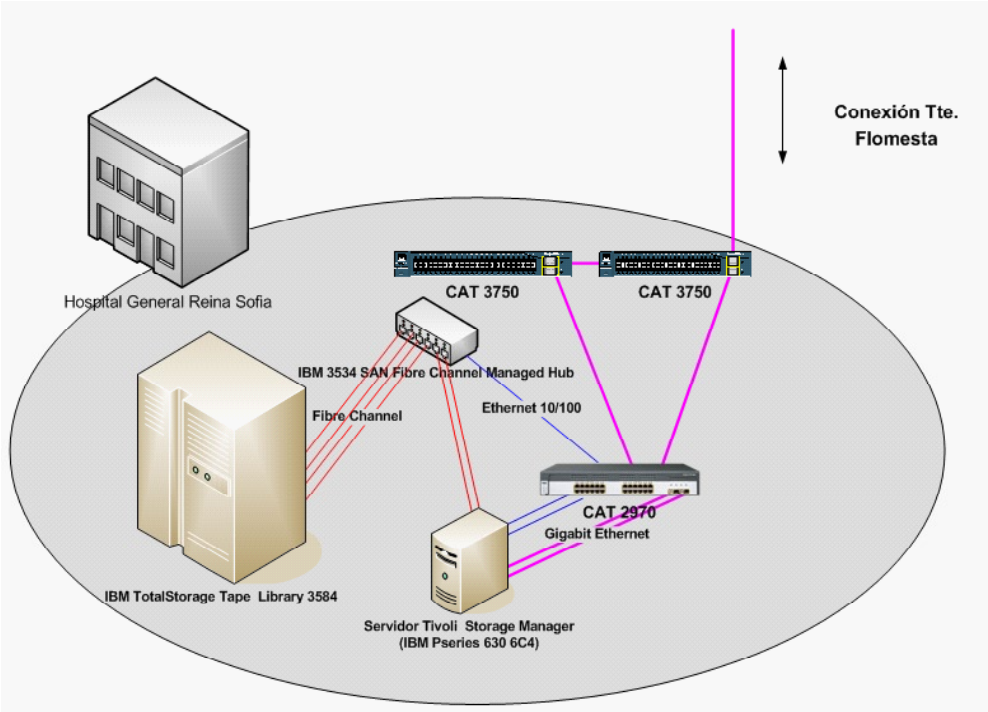
La ubicación del CPD con el antiguo sistema de copias se encontraba en la Consejería de Economía y Hacienda en el edificio de Teniente Flomesta (CPD 1 en adelante).



En el diagrama se observa la existencia de una librería (Magstar MP 3575), conectada mediante una conexión SCSI a servidores dentro de un sistema SP de IBM.
El sistema de copias al que estaba produciendo la migración se sitúa en el Hospital General Reina Sofía (HGRS) (CPD2 en adelante) según el siguiente diagrama

Volver

Manuel Escudero Sánchez
Elena González Arnal
Joaquin Matás Gambín
Manuel Frutos Mirete



Como se aprecia en el esquema, existe una biblioteca de cintas (IBM 3584), junto con un servidor de copias dedicado (IBM PSerie 630 6C4) en el CPD2 conectado a la sala CPD1, mediante una conexión Gigabit Ethernet de 1 GB.

De esta manera en caso de desastre en la sala de sistemas CPD1, una copia de toda la información se encuentre en un lugar distante que garantice la salvaguarda de la información.

Se cuenta con Tivoli Storage Manager como software de copias de seguridad, mediante el cual se realizan copias de los diferentes sistemas, tanto en el ámbito de sistema operativo (AIX, Linux, Windows) como en el ámbito de aplicaciones (SAP R/3, Oracle y Domino).

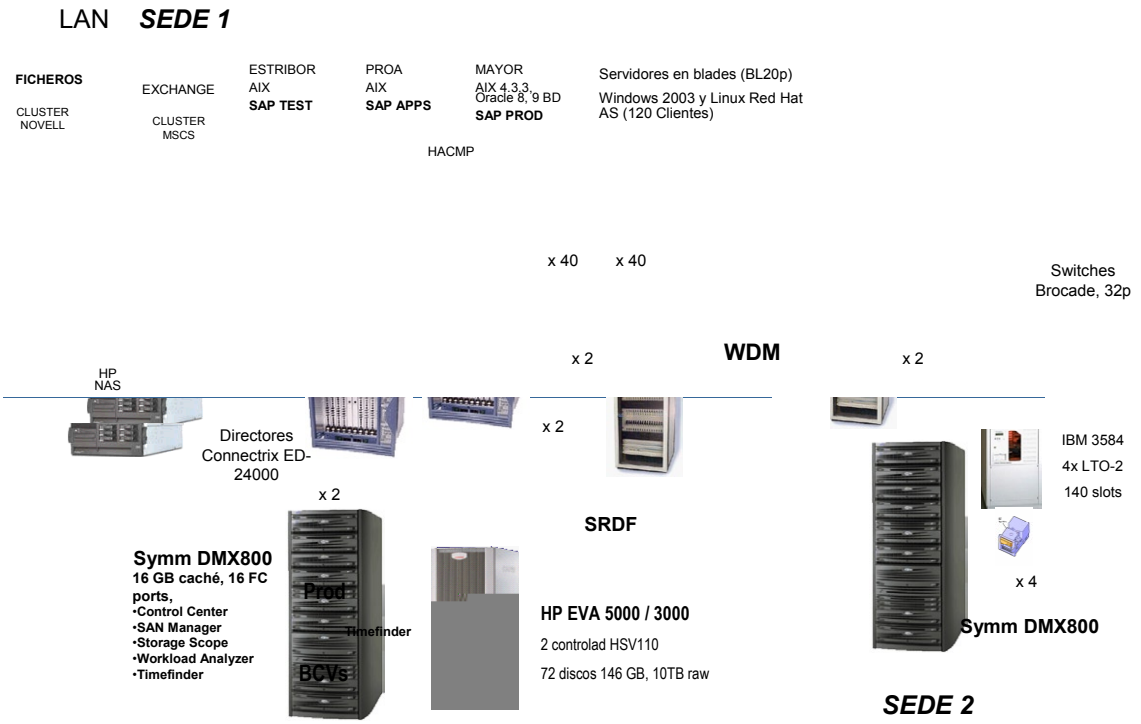
Por otro lado, existe un sistema de servidores Novell de la Consejería de Economía y Hacienda repartidos en tres localizaciones: edificio ASEInfante, Foro y CPD1. La copia de seguridad de estos servidores se encontraba también en proceso de integración desde una solución inicial con ArcServe 9.0 sobre Windows 2000, en la que se hacía una copia de los volúmenes de datos sobre discos FATA dentro de la misma SAN (una EVA3000) y posterior copia a cinta; a una solución final de copia de los volúmenes de datos por TSM a la librería de cintas ubicada en el CPD2.

5. Diseño de la solución.

Una vez estudiadas las distintas alternativas tecnológicas y de diversos fabricantes que daban respuesta al análisis indicado en el punto tercero, se abordó un proyecto cuyos objetivos eran el diseño, instalación y puesta en marcha de la infraestructura de almacenamiento y gestión, que permitiera consolidar los procedimientos de la Dirección General de Informática en materia de salvaguarda y restauración de datos.
La solución propuesta sigue el siguiente esquema.

Volver

Manuel Escudero Sánchez
Elena González Arnal
Joaquin Matás Gambín
Manuel Frutos Mirete



En el proyecto para el diseño, instalación y puesta en marcha se establecieron los siguientes objetivos:

- Implementación de la Solución de Backup en el entorno de Producción de DGI, robusta y avanzada sobre múltiples niveles de almacenamiento: 1° Nivel Symmetrix DMX 800, 2° Nivel HP EVA 5000 y 3° Nivel Cinta.

- Integración de la infraestructura de almacenamiento actualmente instalada en la DGI.

- Implantación de la infraestructura centralizada de almacenamiento necesaria para mejorar el grado de disponibilidad, rendimiento y funcionalidad de los entornos SIGEPAL, GESPER, Netware, e-Administración y Correo electrónico (sistemas identificados como críticos).

- Migración de los elementos y parámetros de la SAN actual a la nueva SAN.

- Creación, integración y parametrización de una SAN extendida, mediante la conexión de los switches y/o directores a dispositivos WDM.

- Conexión a la SAN o en directo de los servidores asociados a los entornos anteriormente citados y el sistema de almacenamiento suministrado.

- Ampliación de la librería de cintas IBM 3584 de 4 a 8 drives LTO-2 para soportar la nueva demanda de escritura.

- Instalación en un centro secundario de un sistema de almacenamiento de respaldo, con réplicas remotas síncronas y mediante en uso de otro sistema de almacenamiento y la funcionalidad SRDF

- Diseño, definición, instalación, configuración e integración de los sistemas de almacenamiento en la SAN.

- Soporte a la migración de los datos almacenados actualmente en discos SSA al nuevo sistema de alma-

Volver

cenamiento.

- Instalación, parametrización y evaluación de las nuevas licencias de usuario, en los servidores de la DGI, e integración de las mismas dentro del entorno de replicación general (Replication Manager).

- Instalación, parametrización y evaluación del software de tercera copia Timefinder en modo BCV's para el backup, en modo snap para prevención de corrupciones lógicas y/o en modo clone para entonos de testing.

- Ajuste y realización de pruebas de scripting para la realización de BCV's para el entorno de Correo sin disrupción de servicio.

- Ajuste e integración de los módulos de automatización necesarios (Replication Manager) para la realización de ciclos de snaps y/o BCV's sobre los entornos de la DGI.

- Ajuste y realización del scripting para la sincronización de clones de producción para los entornos de Testing.

- Implantación del sistema de administración; consola, agentes y sus módulos asociados de reporting, alertas y rendimiento

- Optimización y recomendaciones de implantación que puedan incidir sobre el rendimiento global del sistema.

- Seguimiento mediante actas de reunión y entrega de la documentación asociada al proyecto.

- Se prestará especial atención a la documentación de los procedimientos de salvaguarda/restauración de la información.

5. Conclusiones y futuro del proyecto.

Desde la Dirección General de Informática se ha podido constatar en la realización de este proyecto, que es muy interesante la opción de abordar soluciones de salvaguarda, copia de datos, restauración y continuidad de servicios de una manera integral, ya que es una buena forma de conseguir un sistema robusto en el que los Acuerdos de Calidad de Servicio que se pueden ofrecer no se ven limitados por el "eslabón más débil de la cadena", cuestión que puede suceder en los enfoques realizados por la integración de sistemas independientes, sino que se pueden definir de una manera global.

En cuanto al futuro del proyecto, hay que mencionar que la implantación de la solución que se ha presentado en este artículo, es la fase I de un proyecto más ambicioso que pretende convertir al CPD que se utiliza como segunda ubicación de los elementos de almacenamiento de datos, en un auténtico CPD de respaldo con la incorporación de sistemas servidores de aplicaciones en cluster, con los que residen en la actualidad en el CPD principal.

Así mismo, el estudio de la información que se ha llevado a cabo para la integración en el sistema de almacenamiento, y el hecho de tenerla toda unificada, ha abierto el camino para poder tratar de manera efectiva el ciclo de vida de la información (ILM). Se abordará un proceso de identificación de la información a archivar en cada uno de los sistemas críticos y se buscará la solución más adecuada para crear la jerarquía de almacenamiento que se adapte a las necesidades del sistema.