Alta disponibilidad de los servicios en la SGTIC del MEH

Emilio Raya López

Marcos Llama Pérez

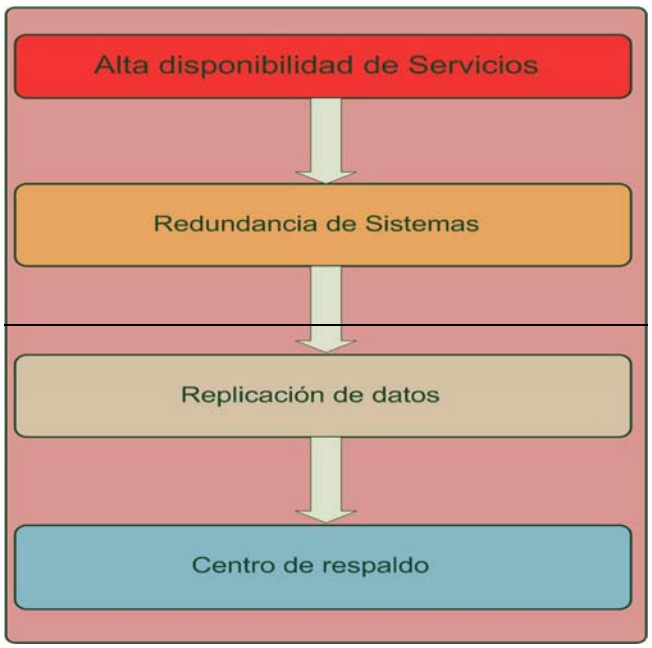
Índice

1. Introducción

La Ley 11/2007, de 22 de Junio, en su artículo 26.2, establece la obligación de permitir, desde los registros electrónicos, la presentación de solicitudes, escritos, y comunicaciones todos los días del año durante las veinticuatro horas.

Por ello aparece la necesidad de crear planes de recuperación ante desastres en los que se identifiquen los servicios que deben prestarse en régimen de alta disponibilidad, así como los elementos necesarios a los distintos niveles (centros de proceso de datos, hardware, software, datos, personal, etc…) que deben ser tenidos en cuenta para asegurar la continuidad de dichos servicios.

El compromiso de mantener determinados servicios en un nivel de disponibilidad de 24x7 lleva aparejada la necesidad de contar con elementos de respaldo a distintos niveles:



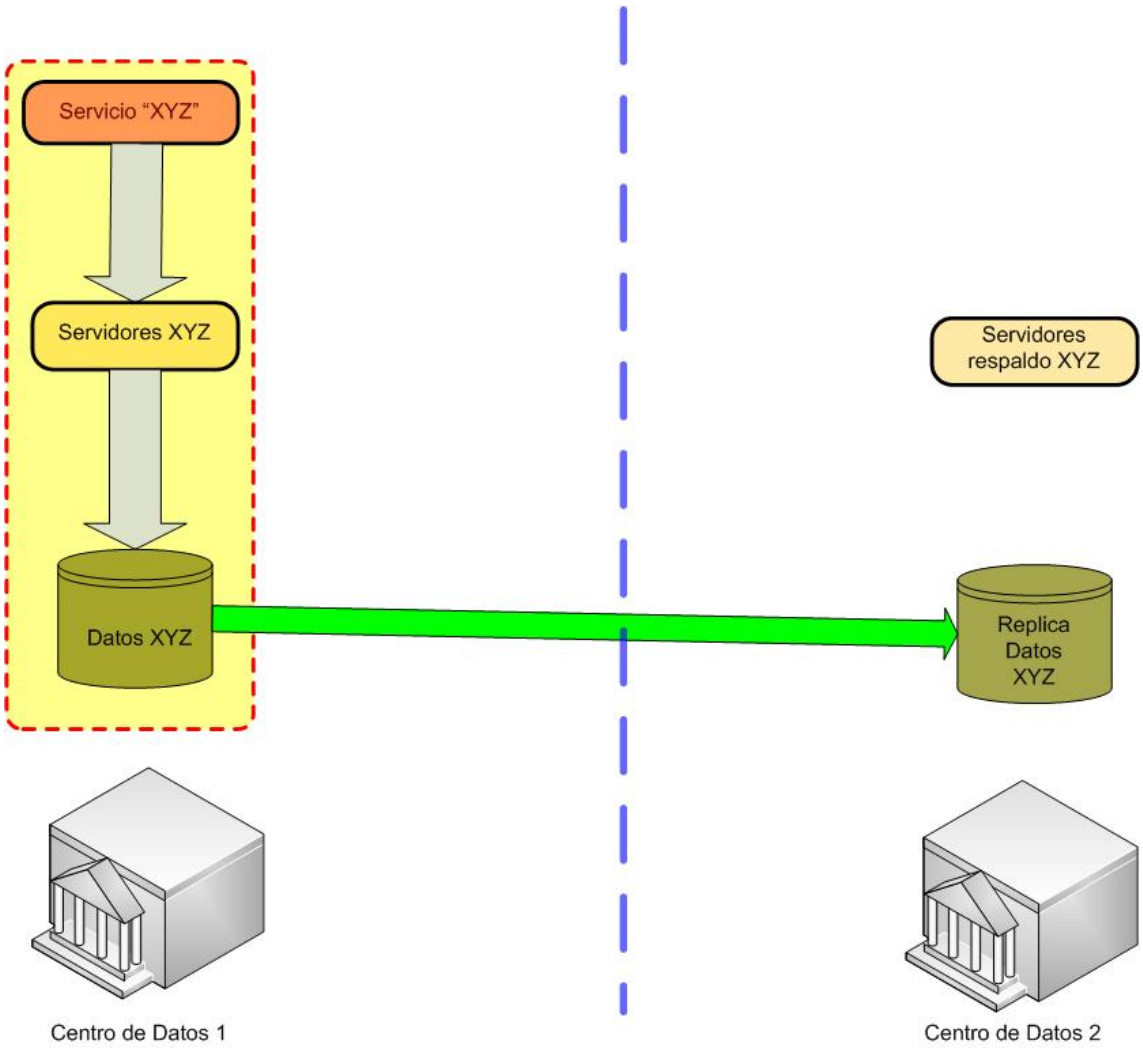
Para asegurar la disponibilidad de un servicio en 24x7, será necesario contar con sistemas redundantes, distribuidos en distintas ubicaciones físicas lo suficientemente separadas entre sí para poder dar respuesta a situaciones de contingencia, como por ejemplo incendios o inundaciones.

No menos importante que la disponibilidad de los servicios es la disponibilidad e integridad de los datos asociados a dichos servicios: Estos deben estar convenientemente replicados entre las distintas ubicaciones físicas, y se debe garantizar que en caso de desastre se dispone de una copia fiable y actualizada de los mismos, lista para poder trabajar con ella.

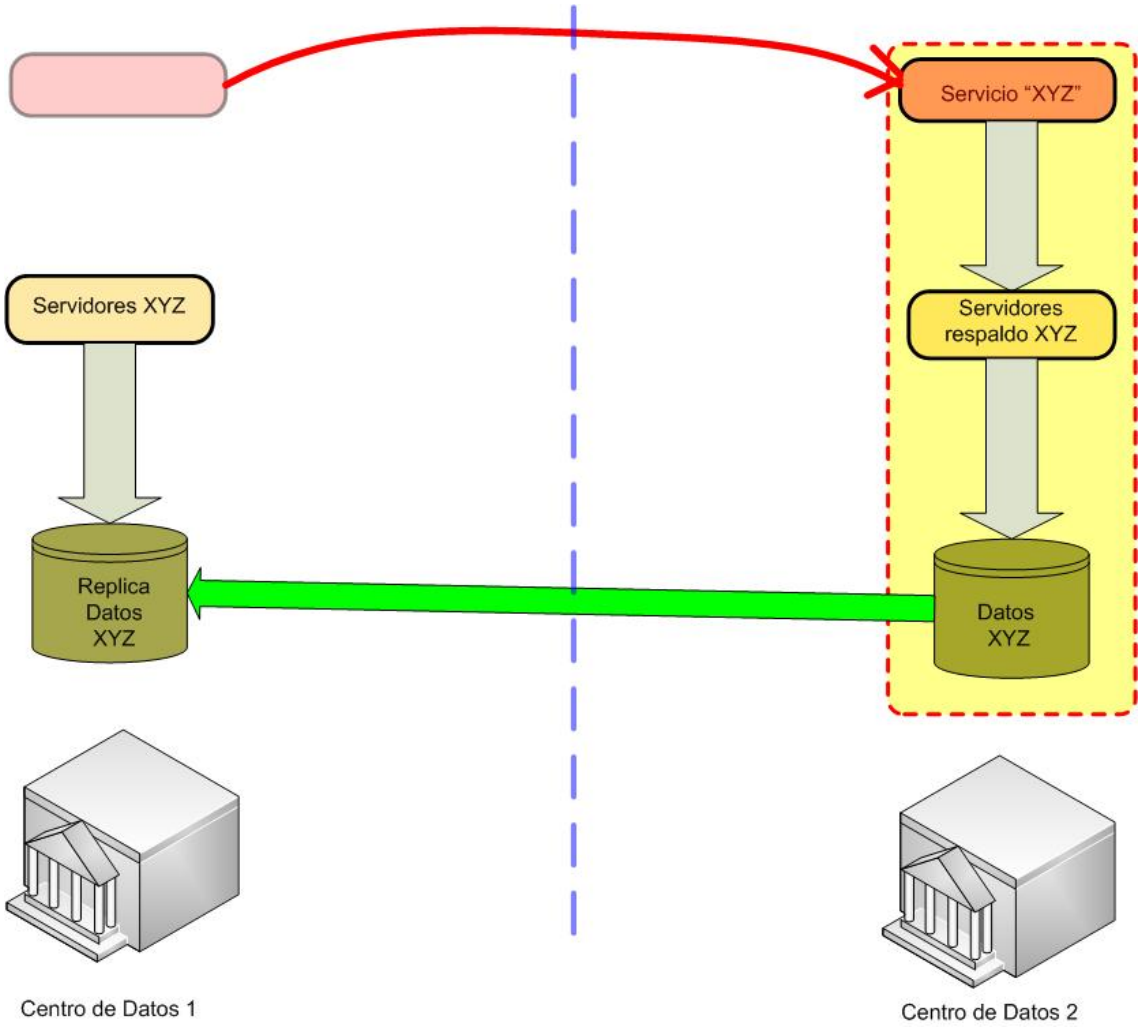
Además es necesario automatizar los trabajos de recuperación de los servicios para minimizar los tiempos de indisponibilidad. Estos trabajos incluyen no solo operaciones en los servidores como detectar fallos y arrancar y parar servicios, sino también la coordinación con los sistemas de almacenamiento de datos: Se trata de asegurar, además de la disponibilidad del servicio, que los datos se están replicando de forma adecuada, y que una copia válida de los mismos estará lista para ser utilizada de forma automática (o cuasi-automática) en caso de desastre.

En definitiva, si se debe dar un servicio en régimen de disponibilidad de 24x7, en un escenario que incluye múltiples ubicaciones físicas, se debe contemplar la alta disponibilidad de forma integrada, gestionando en bloque las operaciones relacionadas con los servicios, sistemas y almacenamiento de datos.

En el ejemplo de la página siguiente, el servicio XYZ se presta en el Centro de Datos 1, y tiene asociados una serie de servidores y de discos de datos, que se replican contra los discos situados en el Centro de Datos 2. En este centro de datos hay servidores preparados para dar servicio en caso de fallo en el Centro de Datos 1.



En caso de contingencia, las operaciones relacionadas con servicios, aplicaciones, servidores y replicación de datos deben estar automatizadas y coordinadas, de forma que se pueda dar servicio desde el centro de respaldo en el menor tiempo posible. En la figura siguiente, el servicio pasa a ser prestado desde el centro de respaldo, implicando el inicio de las correspondientes aplicaciones en los servidores de respaldo, y el cambio del sentido de la replicación de los datos, cuyo origen está ahora en los antiguos discos de réplica:

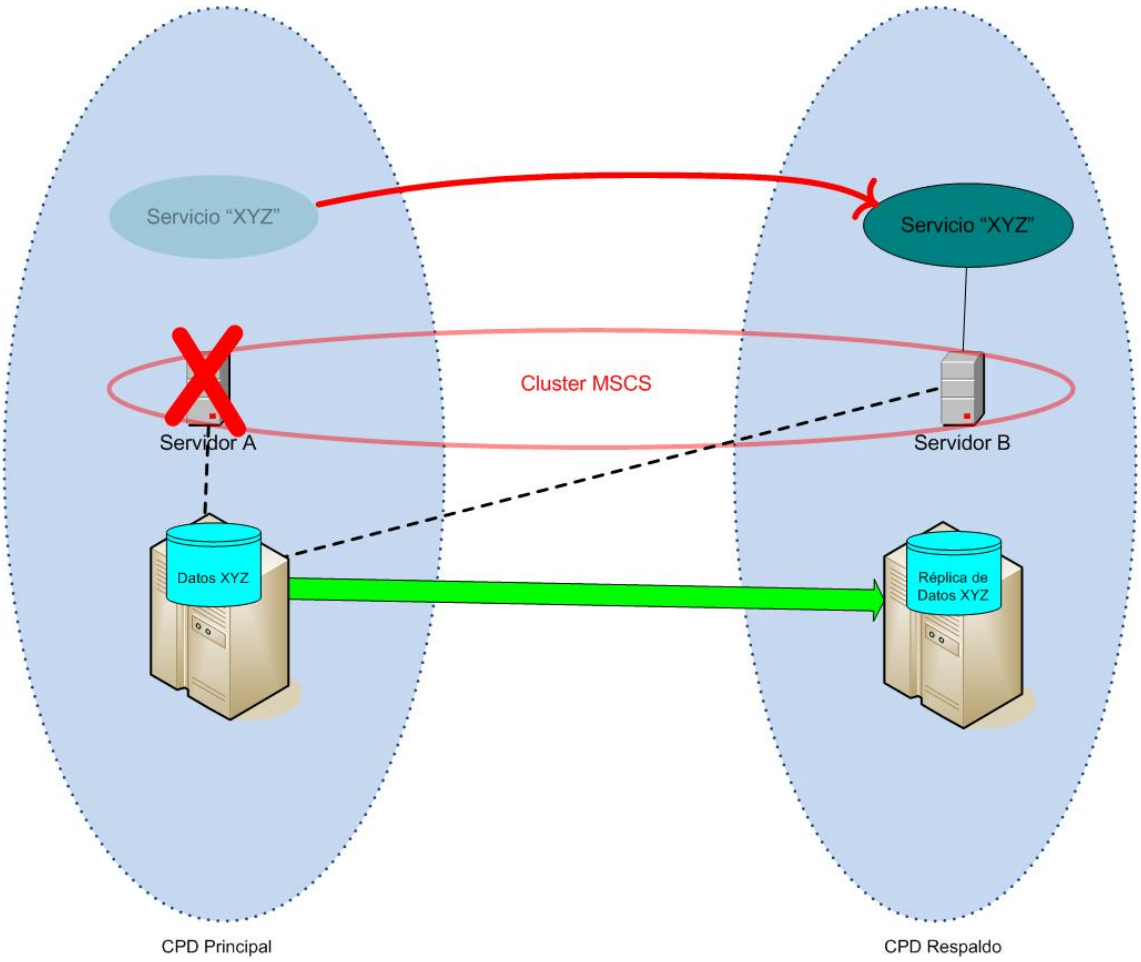


Para poder automatizar estas operaciones y dar una respuesta fiable y rápida a los distintos escenarios de fallo que pudieran plantearse, se requiere implantar soluciones de *clustering* geográfico que integren los distintos niveles: A nivel de servidor y aplicación, se utilizan servicios de *clustering* como por ejemplo Microsoft MSCS. A nivel de datos, se emplean sistemas de replicación de datos entre cabinas de discos como SRDF en el caso de EMC Symmetrix o Continuous Access en el caso de HP XP/EVA. Para coordinar las operaciones de aplicaciones y servidores con las operaciones de almacenamiento, habitualmente se implantan soluciones de integración como SRDF/CE (EMC) o MetroCluster XP/EVA (HP). Si además se requiere automatizar las operaciones relacionadas con entornos virtuales, existen soluciones como VMWare SRM (Site Recovery Manager).

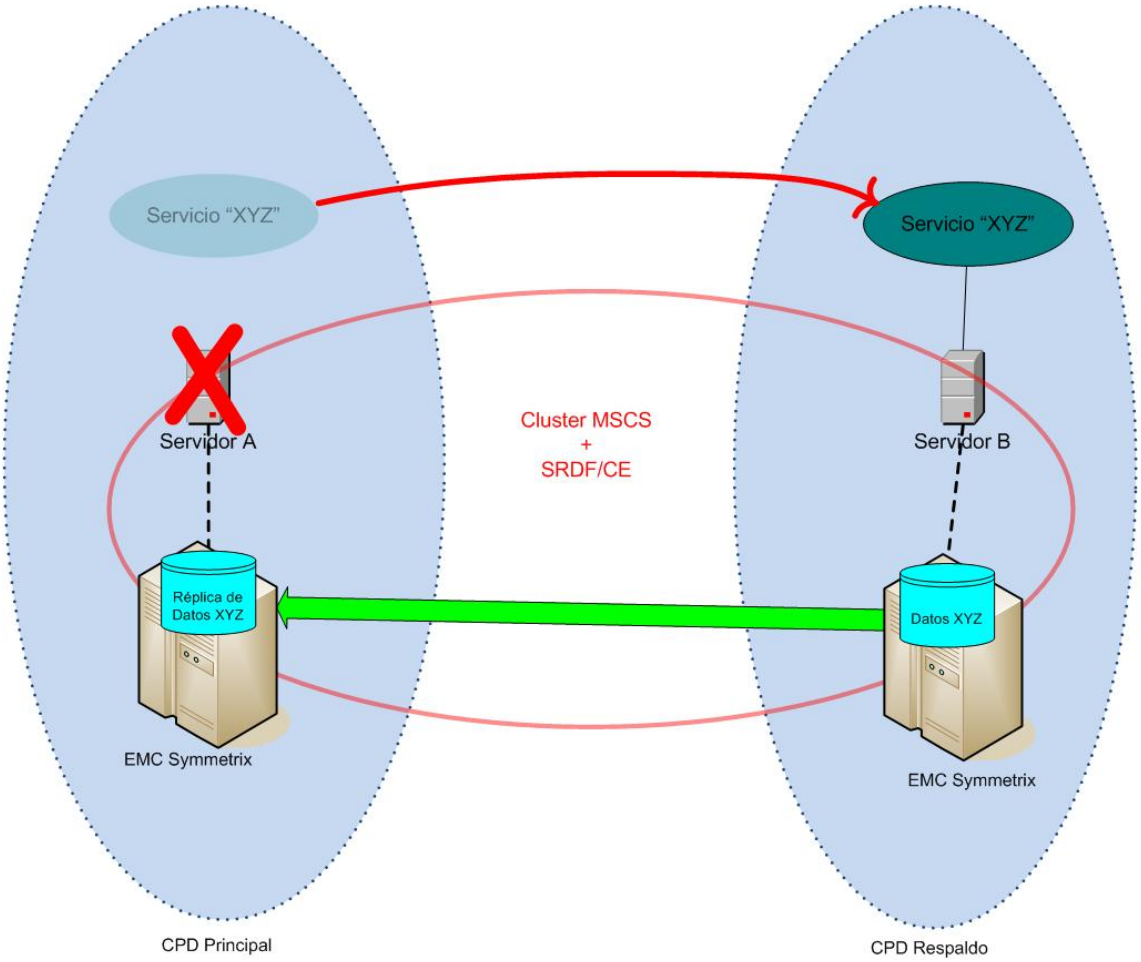
A continuación se detallan 2 ejemplos prácticos del Ministerio de Economía de Hacienda, en los que se utilizan clusters geográficos. El primero trata de la implantación de clusters geográficos de máquinas físicas con Microsoft MSCS y SRDF/CE. El segundo, actualmente en estudio, trata de la automatización de operaciones de recuperación de entornos virtuales geográficamente distribuidos con VMWare SRM.

2. Implantación de clusters geográficos con Microsoft MSCS y SRDF/CE

Actualmente se están implantando en la S.G.T.I.C. del Ministerio de Economía y Hacienda soluciones de *clustering* geográfico basadas en Microsoft MSCS y SRDF/CE. Antes de la implantación de SRDF/CE, se utilizan clusters MSCS sin posibilidad de coordinación de las operaciones relacionadas con la replicación del almacenamiento: Dichas operaciones deben ser gestionadas manualmente de manera independiente. Ello implica que para dar servicio desde el CPD de respaldo, deben realizarse manualmente complicadas tareas de reconfiguración a nivel de almacenamiento y sistema operativo, que inevitablemente dilatan los tiempos de recuperación del servicio en caso de desastre y están expuestas a errores humanos. Los servicios de cluster MSCS por sí solos son capaces de dar respuesta automatizada a fallos de servidor y comunicaciones, pero no a fallos de cabinas de discos o de replicación de datos que impliquen tener que usar la copia remota de los mismos, y mucho menos a situaciones extremas como la destrucción de un centro de datos por desastres como incendios e inundaciones. En la figura de la página siguiente se muestra el fallo de un servidor, que forma parte de un cluster MSCS. El servicio conmuta automáticamente al servidor ubicado en el centro de datos remoto; sin embargo, los discos utilizados siguen siendo los del centro de datos original, y el sentido de la replicación de los datos no se altera:



Con la implantación de SRDF/CE en los clusters MSCS, se consigue integrar y automatizar todas las operaciones necesarias a realizar en caso de contingencia –incluyendo aquellas relacionadas con la replicación de datos entre cabinas de almacenamiento-. En la mayoría de los escenarios de fallo, dichas operaciones se realizarán de forma completamente automática. En la siguiente figura se muestra el mismo caso de fallo de un servidor, en un entorno con MSCS y SRFD/CE; el servicio conmuta al servidor remoto, y automáticamente pasan a utilizarse los datos ubicados en la cabina remota, y se invierte el sentido de replicación de los datos:



Ante ciertos casos de fallo, como la destrucción de un centro de datos o la pérdida total de comunicaciones -incluyendo comunicaciones entre servidores y replicación de datos entre cabinas de discos-, la recuperación del servicio será semiautomática, requiriendo la intervención del administrador de sistemas.

Esta intervención es necesaria para evitar el síndrome de "Split-brain": En estos casos SRDF/CE y MSCS son incapaces de determinar en qué estado se encuentra el centro de datos remoto, y el administrador debe tomar la decisión de levantar el servicio en uno o en otro para evitar que pueda llegar a darse el caso de que en ambos centros se levanten los servicios de manera simultánea, trabajando cada uno por su lado con copias de los datos que se actualizarían de manera independiente, lo cual podría desembocar en una situación de corrupción de datos.

3. Recuperación ante desastres con VMWare SRM

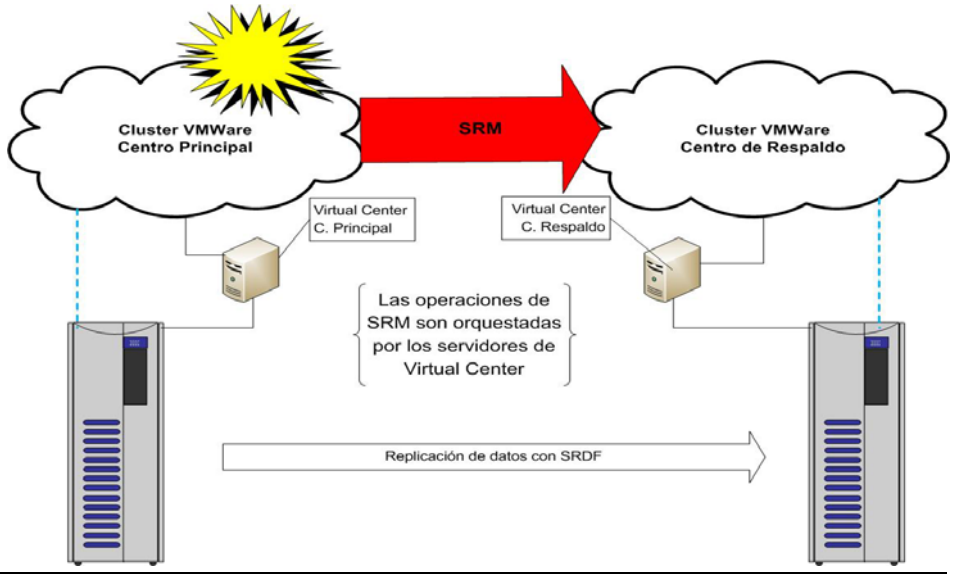
En la S.G.T.I.C. del Ministerio de Economía y Hacienda se está estudiando implantar VMWare SRM con el objetivo de dotar a la plataforma de virtualización VMWare de un mecanismo de recuperación frente a desastres. SRM automatiza las operaciones a realizar en caso de contingencia, incluyendo el reinicio de máquinas virtuales en el centro de datos de respaldo y el control de la replicación de datos en las cabinas de disco.

Actualmente se cuenta con un cluster ESX en el centro principal, al que se desea dotar de un mecanismo de protección frente a desastres. El primer paso será la creación de un cluster similar en el centro de respaldo. Los discos de sistema operativo de las máquinas virtuales residen en las cabinas de almacenamiento, y se replican contra las cabinas remotas a través de los mecanismos de replicación habituales (SRDF en Symmetrix).

Al implantar SRM, se automatizan las siguientes tareas:

- Traspaso de configuración de máquinas virtuales del cluster principal al cluster de respaldo.
- Conexión con cabinas de discos para configurar la copia de respaldo como copia principal en caso de contingencia e invertir el sentido de la replicación.
- Actualización de la configuración de discos de máquinas virtuales en cluster de respaldo para que se utilicen los datos ubicados en el centro de respaldo.
- Configuración de parámetros de sistema operativo de máquinas virtuales, tales como direccionamiento IP, licencias, arranque y parada de servicios, etc…

Adicionalmente, SRM permitirá la creación y mantenimiento de planes de recuperación ante desastres de la infraestructura virtual.



4. Conclusión

En resumen, las soluciones descritas permiten la automatización de las tareas necesarias para la recuperación del servicio en el mínimo tiempo posible, integrando y coordinando los diferentes elementos implicados, en un entorno geográficamente distribuido para la protección ante desastres.

A nivel operativo, el objetivo que se pretende conseguir es tener centros de proceso de datos desde los que puedan prestarse los servicios más críticos de forma autónoma, con una gestión ágil que permita realizar de forma sencilla, rápida y segura las operaciones de recuperación ante desastres.

En definitiva, desde la S.G.T.I.C. del Ministerio de Economía y Hacienda se pretende a través de estas soluciones conseguir una infraestructura informática robusta y fiable, dando así respuesta a las exigencias de disponibilidad de los servicios electrónicos introducida por la Ley 11/2007.