Departamento de Informática

PROYECTO FIN DE CARRERA

PLAN DE CONTINGENCIA DE TECNOLOGIAS DE LA INFORMACIÓN EN ENTORNOS DISTRIBUIDOS

Autor: Jose Ignacio Verdú Fernández

Tutor: Jose Luis Lopez Cuadrado

Leganés, Octubre 2015

Título: Plan de contingencia para tecnologías de la información en entornos distribuidos
Autor: Jose Ignacio Verdú Fernández
Director: José Arturo Mora Soto

EL TRIBUNAL

Presidente:

Vocal:

Secretario:

Realizado el acto de defensa y lectura del Proyecto Fin de Carrera el día 14 de Octubre de 2015 en Leganés, en la Escuela Politécnica Superior de la Universidad Carlos III de Madrid, acuerda otorgarle la CALIFICACIÓN de 7,0.

VOCAL

SECRETARIO PRESIDENTE

AGRADECIMIENTOS

Agradecerle principalmente a mi familia porque sin su apoyo y ayuda me hubiera sido imposible llegar hasta este punto, especialmente a mi mujer y mis hijos porque cada día me dan la luz necesaria para poder cumplir mis objetivos.

Por supuesto también a Jose Arturo por su ayuda y su insistencia en apoyarme para que lograra este objetivo que tanto tiempo y esfuerzo me ha costado. Estaré eternamente agradecido.

Y por último y no menos importante, a mis compañeros de trabajo que con sus conocimientos y experiencias me han puesto el camino muy fácil para tanto laboralmente como en este proyecto haya cumplido mis objetivos.

Resumen

Un porcentaje muy alto de los incumplimientos de los acuerdos a nivel de servicio[i] (SLA) del servicio en proyectos de TI es debido a la caída de infraestructura Hardware o Software, la cual supone una afectación en el servicio sin previo aviso. De forma proactiva se establecen planes y herramientas que mejoren la capacidad del entorno, pero de forma reactiva, están los llamados Planes de Contingencia para tecnologías de la información (TI).

Un plan de contingencia es un instrumento de gestión para el buen gobierno de las Tecnología de la Información y las comunicaciones en el dominio del soporte y desempeño. Estos planes de contingencia contienen las medidas técnicas, humanas y organizativas necesarias para garantizar la continuidad del negocio y las operaciones de un proyecto. Es un caso particular de plan de continuidad del negocio, pero dada la importancia actual de las tecnologías modernas, el plan de contingencias es el más relevante.

El objetivo de este documento es explicar que es un plan de contingencia, el porqué de su importancia y el cómo de su preparación, poniendo como ejemplo un caso práctico de proyecto TI en el cual se plantea la mejora de un plan ya creado para una Entidad Bancaria Nacional con más de 13 millones de clientes . La mejora de dicho plan se basa principalmente en la automatización de las acciones, es decir, disminuir todo lo posible la acción humana y sobre todo la acción humana especializada, para disminuir al máximo, sin restar rendimiento, el consumo de recursos del proyecto.

Abstract Resume

A very high percentage of service level agreements (SLA) breaches in IT projects are because hardware or software infrastructure failure, that causes instant and unannounced interruption of service. We make plans and tools that improve the capacity of the environment proactively, but reactively, provide contingency plans for information technology (IT).

A contingency plan is a management tool for good governance of information technology and communications in the area of support and performance. These contingency plans contain technical, human and organizational measures to ensure business continuity and operations of a project. It's an element of business continuity plan, which is particularly relevant in the light of modern technologies become more important.

The purpose of this document is to explain: what a contingency plan is, why it's important and how we prepare it. We do this with the example of an IT project. We propose to improve the existing contingency plan of a National Bank with over 13 million customers. The improvement of this plan is primarily based on automating actions, reducing to minimum human intervention and the use of the project resources, without affecting the project performance.

Índice

1. Introducción

Este trabajo se desarrolló en un entorno empresarial como parte de las actividades profesionales del sustentante en una multinacional bancaria con una plantilla de 32.625 empleados, en la cual, se le solicitó al sustentante el diseño de un plan de contingencia TI para entornos distribuidos.

Una multinacional bancaria con una plantilla de 32.625 empleados y más 13 millones de clientes, necesita realizar una revisión exhaustiva de su plan de contingencia TI de sistemas para la infraestructura correspondiente al servicio Intranet. Este servicio consta de más unos 20 servidores de aplicaciones, 15 servidores de BBDD y varios servidores de software dedicado a otras funcionalidades.

El actual plan de contingencia está obsoleto, con una utilización de recursos y de tiempo que ya no es soportable para un procedimiento de recuperación de un servicio caído. El valor que se aporta actualmente al usuario está muy por encima de las posibilidades de los recursos materiales y técnicos con los que se cuenta en el departamento encargado de la administración de la Intranet.

El documento presente, expondremos una primera aproximación y explicación del estado del arte actual del contexto de un plan de contingencia conjuntamente con las metodologías y recursos utilizados para la elaboración de este plan. Explicando brevemente el uso y la descripción de las tecnologías manejadas que cada departamento del servicio de Intranet administra.

Analizaremos el problema que nos encontramos más en profundidad y que nos ha llevado a realiza este proyecto de mejora, el cual no hay que olvidar que se trata de un proyecto de mejora continua, ya que este plan se debería ir adaptando a los cambios que surjan en la infraestructura presente. Expondremos los puntos débiles del plan en vigor previamente habiendo explicado la infraestructura a la que nos referimos.

Una vez puestos en el marco actual, explicaremos el proceso de elaboración del plan con la estrategia y diseño a seguir previos. Este punto es muy importante ya que es del que se parte y del cual nos basaremos para la construcción e implementación del plan. Quiero remarcar la importancia, ya que como hemos indicado anteriormente, el proyecto no es de finalización inmediata, sino que se quiere que sea de mejora continua, y cada cambio o mejora que se realice tendrá que ser siempre basada en este diseño y estrategia para mantener una estabilidad.

Por último, haremos una explicación ampliada y detallada del nuevo plan de contingencia. Este punto tendrá las responsabilidades y competencias de cada departamento, los flujos de los diferentes escenarios que pueden darse en el proceso de contingencia y demás características principales del plan.

Este trabajo ha sido elaborado tomando como base la metodología ITIL (INFORMATION TECNOLOGY INFRASTRUTURE LIBRARY), formado por personas, equipos y procedimientos. Al conjugar una serie de elementos como hombres y servidores se hace imprescindible tomar medidas que nos permitan una continuidad en la operatividad de los sistemas para no ver afectados los objetivos de las mismas y no perder la inversión de costos y tiempo.

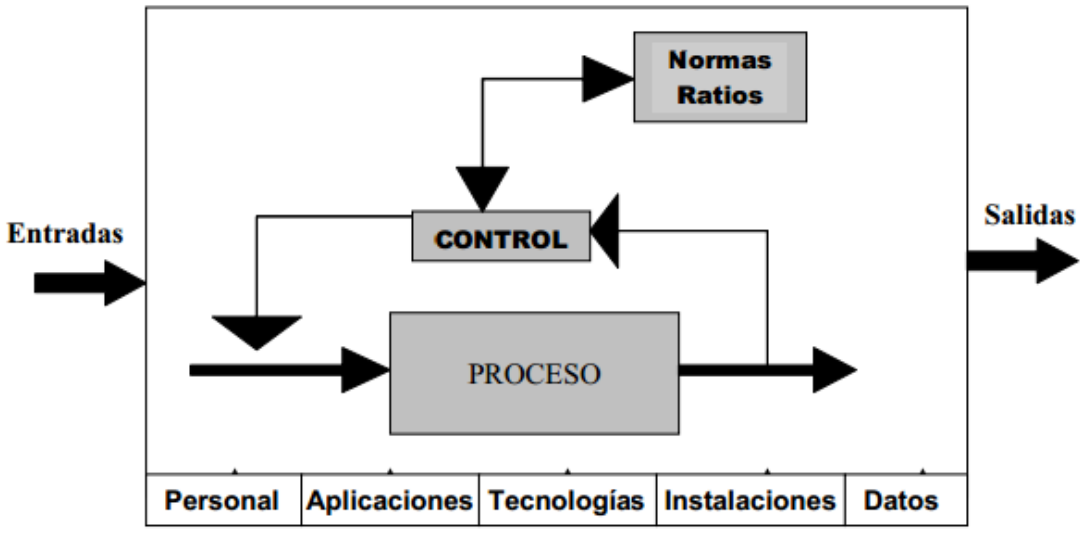

Ilustración 1 ITIL

2. Estado del Arte

1. Gestión de la Continuidad del Servicio

La Gestión de la Continuidad del Servicio[ii] se preocupa de impedir que una imprevista y grave interrupción de los servicios TI, debido a desastres naturales u otras fuerzas de causa mayor, tenga consecuencias catastróficas para el negocio.

La estrategia de la Gestión de la Continuidad del Servicio (ITSCM) debe combinar equilibradamente procedimientos Proactivos y Reactivos:

- Proactivos: que buscan impedir o minimizar las consecuencias de una grave interrupción del servicio.
- Reactivos: cuyo propósito es reanudar el servicio tan pronto como sea posible (y recomendable) tras el desastre.

La ITSCM requiere una implicación especial de los agentes involucrados pues sus beneficios sólo se perciben a largo plazo, es costosa y carece de rentabilidad directa. Implementar la ITSCM es como contratar un seguro médico: cuesta dinero, parece inútil mientras uno está sano y desearíamos nunca tener que utilizarlo, pero tarde o temprano nos alegramos de haber sido previsores.

Aunque, a priori, las políticas proactivas que prevean y limiten los efectos de un desastre sobre los servicios TI son preferibles a las exclusivamente reactivas, es importante valorar los costes relativos y la incidencia real en la continuidad del negocio para decantarse por una de ellas o por una sabia combinación de ambas.

Las principales actividades de la Gestión de la Continuidad del Servicio se resumen en:

- Establecer las políticas y alcance de la ITSCM.
- Evaluar el impacto en el negocio de una interrupción de los servicios TI.
- Analizar y prever los riesgos a los que está expuesto la infraestructura TI.
- Establecer las estrategias de continuidad del servicio TI.
- Adoptar medidas proactivas de prevención del riesgo.
- Desarrollar los planes de contingencia.
- Poner a prueba dichos planes.
- Formar al personal sobre los procedimientos necesarios para la pronta recuperación del servicio.
- Revisar periódicamente los planes para adaptarlos a las necesidades reales del negocio.

Tarde o temprano, por muy eficientes que seamos en nuestras actividades de prevención, será necesario poner en marcha procedimientos de recuperación.

En líneas generales existen tres opciones de recuperación del servicio:

- "Cold standby": que requiere un emplazamiento alternativo en el que podamos reproducir en pocos días nuestro entorno de producción y servicio. Esta opción es la adecuada si los planes de recuperación estiman que la organización puede mantener sus niveles de servicio durante este periodo sin el apoyo de la infraestructura TI.

- "Warm standby": que requiere un emplazamiento alternativo con sistemas activos diseñados para recuperar los servicios críticos en un plazo de entre 24 y 72 horas.

- "Hot standby": que requiere un emplazamiento alternativo con una replicación continua de datos y con todos los sistemas activos preparados para la inmediata sustitución de la estructura de producción. Ésta es evidentemente la opción más costosa y debe emplearse sólo en el caso de que la interrupción del servicio TI tuviera inmediatas repercusiones comerciales.

2. Plan de Contingencia

Podríamos definir a un plan de contingencias[iii] como una estrategia planificada con una serie de procedimientos que nos faciliten o nos orienten a tener una solución alternativa que nos permita restituir rápidamente los servicios de la organización ante la eventualidad de todo lo que lo pueda paralizar, ya sea de forma parcial o total.

El plan de contingencia es una herramienta que le ayudará a que los procesos críticos de su empresa u organización continúen funcionando a pesar de una posible falla en los sistemas computarizados. Es decir, un plan que le permite a su negocio u organización, seguir operando aunque sea al mínimo.

3. Objetivos del Plan de Contingencia

- Garantizar la continuidad de las operaciones de los elementos considerados críticos que componen los Sistemas de Información.

- Definir acciones y procedimientos a ejecutar en caso de fallas de los elementos que componen un Sistema de Información.

4. Automatización de operaciones y Tecnologías utilizadas en el Plan

Hoy en día, las soluciones tecnológicas que nos ofrecen productos de Software tipo Servidores de Aplicaciones, Gestión de BBDD, etc., tienen tareas básicas de administración que una vez procedimentadas y automatizadas son fáciles de traspasar o delegar. Este dato es muy importante de cara ahorrar recursos y tiempo en tareas rutinarias e incluso en resolver problemas, que en el caso que nos lleva ahora, es muy eficiente.

Estos mecanismos de automatización o procedimentados pueden ser desde una simple consulta a un log, como la limpieza de un Tablespace o incluso,

creación/instalación/configuración de una infraestructura capaz de servir una aplicación Web que se sirve de conexiones a BBDD, WebServices, etc.

Hay miles y miles de formas y herramientas en el mercado para poder realizar automatismos y procedimientos. Lo más básico, y no menos importante, sería utilizar el típico manual detallado en un procesador de textos. En el cual, un técnico avanzado crea una guía especificando paso a paso los comandos, acciones, tareas a realizar para un operador o técnico menos experimentado. Por ejemplo, un paso más avanzado sería la creación de un script que realiza automáticamente las tareas necesarias para levantar un proceso caído y además que este script sea lanzado por un sistema de alertas, que lo ejecute cuando vea que el proceso se ha caído. A este sistema, otro script lanzado por el mismo le avisó de que el proceso ya no está lanzado en la máquina... Como se ve, hay un sin fin de posibilidades para poder utilizar herramientas en pos de la pro actividad o reactividad del servicio TI.

En el caso que nos ocupa, vamos a utilizar las siguientes tecnologías expuestas en los próximos puntos.

Red Hat Linux

RHEL (Red Hat Linux)[iv] es una distribución del núcleo Linux, el cual es un núcleo libre de sistema operativo basado en Unix. Es uno de los principales ejemplos de software libre. Linux está licenciado bajo la GPL v2 y está desarrollado por colaboradores de todo el mundo.

El núcleo Linux fue concebido por el entonces estudiante de ciencias de la computación finlandés, Linus Torvalds, en 1991. Linux consiguió rápidamente desarrolladores y usuarios que adoptaron códigos de otros proyectos de software libre para su uso en nuevas distribuciones. El núcleo Linux ha recibido contribuciones de miles de programadores de todo el mundo. Normalmente Linux se utiliza junto a un empaquetado de software, llamado distribución Linux y servidores.

En este caso utilizaremos RHEL, es instalado con un ambiente gráfico llamado Anaconda, diseñado para su fácil uso por novatos. También incorpora una herramienta llamada Lokkit para configurar las capacidades de Cortafuegos.

Oracle Database

Oracle Database[v] es un sistema de gestión de base de datos objeto-relacional (o ORDBMS por el acrónimo en inglés de Object-Relational Data Base Management System), desarrollado por Oracle Corporation. Se considera a Oracle como uno de los sistemas de bases de datos más completos, con un dominio en el mercado de servidores empresariales ha sido casi total hasta hace poco, recientemente sufre la competencia del Microsoft SQL Server de Microsoft y de la oferta de otros RDBMS con licencia libre como PostgreSQL, MySQL o Firebird. Las últimas versiones de Oracle han sido certificadas para poder trabajar bajo GNU/Linux.

Bash (Shell Scripting)

Bash (Bourne again shell) [vi]es un programa informático cuya función consiste en interpretar órdenes. Está basado en la shell de Unix y es compatible con POSIX.

Fue escrito para el proyecto GNU y es el intérprete de comandos por defecto en la mayoría de las distribuciones de Linux. Su nombre es un acrónimo de Bourne-Again Shell (otro shell bourne) — haciendo un juego de palabras (born-again significa renacimiento) sobre el Bourne shell (sh), que fue uno de los primeros intérpretes importantes de Unix. Además de Mac OS X Tiger, y puede ejecutarse en la mayoría de los sistemas operativos tipo Unix. También se ha llevado a Microsoft Windows por el proyecto Cygwin.

La sintaxis de órdenes de Bash incluye ideas tomadas desde el Korn Shell (ksh) y el C Shell (csh), como la edición de la línea de órdenes, el historial de órdenes, la pila de directorios, las variables $RANDOM y $PPID, y la sintaxis de substitución de órdenes POSIX: $(...). Cuando se utiliza como un intérprete de órdenes interactivo, Bash proporciona autocompletado de nombres de programas, nombres de archivos, nombres de variables, etc., cuando el usuario pulsa la tecla TAB.

La sintaxis de Bash tiene muchas extensiones que no proporciona el intérprete Bourne.

NFS (Network File System)

El Network File System [vii](Sistema de archivos de red), o NFS, es un protocolo de nivel de aplicación, según el Modelo OSI. Es utilizado para sistemas de archivos distribuido en un entorno de red de computadoras de área local. Posibilita que distintos sistemas conectados a una misma red accedan a ficheros remotos como si se tratara de locales. Originalmente fue desarrollado en 1984 por Sun Microsystems, con el objetivo de que sea independiente de la máquina, el sistema operativo y el protocolo de transporte, esto fue posible gracias a que está implementado sobre los protocolos XDR (presentación) y ONC RPC (sesión).

El protocolo NFS está incluido por defecto en los Sistemas Operativos UNIX y la mayoría de distribuciones Linux.

Apache HTTP Server

El servidor HTTP Apache[viii] es un servidor web HTTP de código abierto, para plataformas Unix (BSD, GNU/Linux, etc.), Microsoft Windows, Macintosh y otras, que implementa el protocolo HTTP/1.12 y la noción de sitio virtual.

El servidor Apache se desarrolla dentro del proyecto HTTP Server (httpd) de la Apache Software Foundation. Apache presenta entre otras características altamente configurables, bases de datos de autenticación y negociado de contenido, pero fue criticado por la falta de una interfaz gráfica que ayude en su configuración.

Apache tiene amplia aceptación en la red: desde 1996, Apache, es el servidor HTTP más usado. Alcanzó su máxima cuota de mercado en 2005 siendo el servidor empleado en el 70% de los sitios web en el mundo, sin embargo ha sufrido un descenso en su cuota de mercado en los últimos años.

WebSphere Application Server

IBM WebSphere Application Server[ix] (WAS, servidor de aplicaciones WebSphere), un servidor de aplicaciones de software, es el producto estrella dentro de la familia WebSphere de IBM. WAS está construido usando estándares abiertos tales como J2EE, XML, y Servicios Web. Varios laboratorios de IBM alrededor del mundo participaron en la creación de los productos run-time WebSphere y las herramientas de desarrollo. Esto funciona con varios servidores web incluyendo Apache HTTP Server, Netscape Enterprise Server, Microsoft Internet Information Services (IIS), IBM HTTP Server para i5/OS, IBM HTTP Server para z/OS, y también IBM HTTP Server para el sistema operativo AIX/Linux/Microsoft Windows/Solaris.

F5 Load Balancer

Un balanceador de carga F5[x] fundamentalmente es un dispositivo de hardware o software que se pone al frente de un conjunto de servidores que atienden una aplicación y, tal como su nombre lo indica, asigna o balancea las solicitudes que llegan de los clientes a los servidores usando algún algoritmo (desde un simple Round Robin hasta algoritmos más sofisticados).

DNS

Domain Name System[xi] o DNS (en español: sistema de nombres de dominio) es un sistema de nomenclatura jerárquica para computadoras, servicios o cualquier recurso conectado a Internet o a una red privada. Este sistema asocia información variada con nombres de dominios asignado a cada uno de los participantes. Su función más importante, es traducir (resolver) nombres inteligibles para las personas en identificadores binarios asociados con los equipos conectados a la red, esto con el propósito de poder localizar y direccionar estos equipos mundialmente.

El servidor DNS utiliza una base de datos distribuida y jerárquica que almacena información asociada a nombres de dominio en redes como Internet. Aunque como base de datos el DNS es capaz de asociar diferentes tipos de información a cada

nombre, los usos más comunes son la asignación de nombres de dominio a direcciones IP y la localización de los servidores de correo electrónico de cada dominio.

WebShere MQ Series

IBM WebSphere MQ[xii] puede transportar cualquier tipo de datos como mensajes, abriendo la posibilidad a las empresas de crear arquitecturas flexibles y reutilizables, como entornos de arquitectura orientada a servicios (SOA). Funciona con una amplia gama de plataformas informáticas, aplicaciones, servicios web y protocolos de comunicación para conseguir una entrega de mensajes altamente segura. WebSphere MQ proporciona una capa de comunicaciones para la visibilidad y el control del flujo de mensajes y datos dentro y fuera de su organización.

WebSphere MQ

- Integración de mensajería versátil desde mainframe a móvil, que ofrece una única base de mensajería sólida para entornos heterogéneos dinámicos.
- Entrega de mensajes con características altamente seguras, que generan resultados auditables.
- Transporte de mensajes de alto rendimiento, para entregar los datos con mayor velocidad y fiabilidad.
- Características administrativas que simplifican la gestión de mensajería y reducen el tiempo dedicado a herramientas complejas.
- Herramientas de desarrollo de estándares abiertos que dan soporte a la extensibilidad y al crecimiento del negocio.

Harvest

CA Harvest Software Change Manager[xiii] ayuda a TI a simplificar la complicada gestión del desarrollo y mantenimiento de las aplicaciones de negocio. Automatiza la gestión del ciclo de vida, versionamiento de código, y agiliza los flujos de trabajo complejos al tiempo que proporciona auditoría integral, la protección y conservación de los bienes esenciales para las operaciones críticas de negocio de software y el cumplimiento normativo. CA Harvest SCM ayuda a entregar procesos estándar, fiables,

recurrentes que se pueden escalar para satisfacer las demandas de las grandes empresas y los proyectos de desarrollo a nivel mundial, los cuales tienen una entrega más rápida y aplicaciones de alta calidad.

3. Fases de la Metodología

Los planes de recuperación de desastres TI proporcionan unos procedimientos detallados a seguir, paso a paso, los cuales se basan en recuperar los sistemas y redes que han sufrido disrupciones y ayudan a resumir la normalidad en las operaciones. El objetivo principal de estos procesos es minimizar cualquier impacto negativo en las operaciones de la compañía, el proceso de recuperación de desastres identifica los sistemas y redes críticos de TI; fija las prioridades para su recuperación y dibuja los pasos necesarios para reiniciar, reconfigurar y recuperar dichos sistemas y redes. Es un hecho que todo plan integral de recuperación de desastres debe incluir también a todos los proveedores relevantes, las fuentes de experiencia para recuperar los sistemas afectados y una secuencia lógica de los pasos a seguir hasta alcanzar una recuperación óptima.

Ya que se tiene una evaluación de riesgos, y se han identificado las amenazas potenciales a la infraestructura de TI, el siguiente paso será determinar qué elementos de dicha infraestructura son los más importantes para las operaciones corporativas. Asumiendo que todos los sistemas y redes TI funcionan con normalidad, la empresa debería ser plenamente viable, competitiva y sólida desde el punto de vista financiero.

Cabe mencionar que cuando un incidente ya sea interno o externo afecta negativamente a la infraestructura de TI, las operaciones corporativas pueden verse amenazadas.

Según la planificación de contingencias para los sistemas de tecnologías de la información [xiv], del NIST[xv], o Instituto Nacional de Estándares y Tecnología de los Estados Unidos, la siguientes es la estructura ideal de un plan de recuperación de desastres TI.

- Elaboración de la declaración de políticas para el plan de contingencia. Contar con unas directivas formales proporciona la autoridad y orientación necesaria para elaborar un plan de contingencia efectivo.

- Realización del análisis de impacto sobre el negocio (BIA). El análisis del impacto sobre el negocio ayuda a identificar y priorizar los sistemas y componentes críticos de TI.

- Identificación de controles preventivos. Medidas que reducen los efectos de las disrupciones al sistema y pueden aumentar su disponibilidad y reducir los costos de contingencia del ciclo de vida.

- Desarrollo de estrategias de recuperación. Tener una estrategia integral garantiza que el sistema se recuperará de manera rápida y efectiva después de una disrupción.
- Desarrollo de un plan de contingencia TI. El plan de contingencia debería contener orientaciones y procedimientos detallados para la restauración del sistema dañado.

- Prueba, formación y ejecución del plan. La prueba del plan identifica lagunas en la planificación, mientras que la formación prepara al personal de recuperación para la activación del plan; ambas actividades mejoran la eficacia del plan y la preparación general de la entidad.

- Mantenimiento del plan. El plan debería ser un documento vivo que se actualiza regularmente para mantenerlo al día con mejoras al sistema.

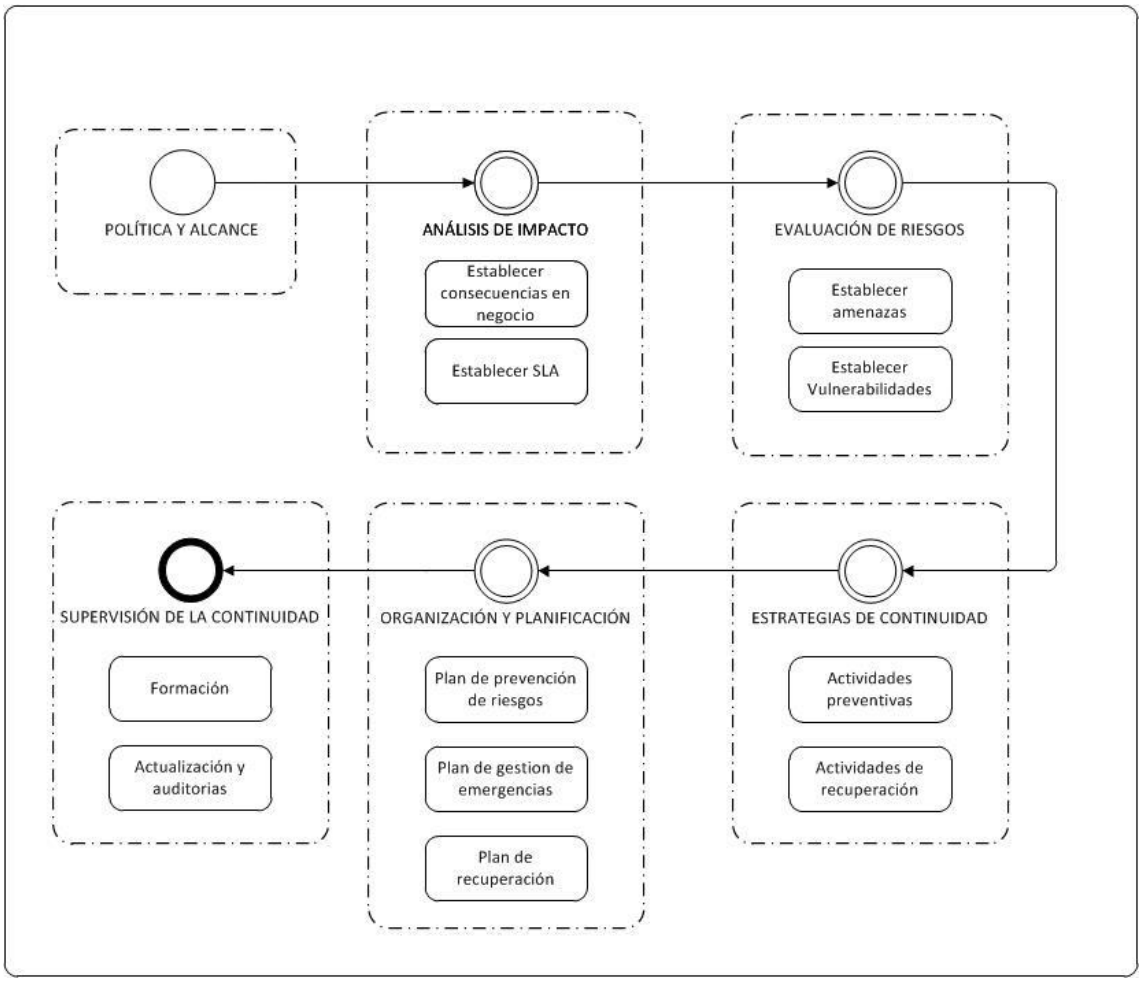

Ilustración 2 Fases de la metodología

FASE1: Política y Alcance

El primer paso necesario para desarrollar una Gestión de la Continuidad del Servicio coherente es establecer claramente sus objetivos generales, su alcance y el compromiso de la organización TI: su política.

La gestión de la empresa debe demostrar su implicación con el proceso desde un primer momento pues la implantación de la ITSCM puede resultar compleja y costosa sin la contrapartida de un retorno obvio a la inversión.

Es imprescindible establecer el alcance de la ITSCM en función de:

- Los planes generales de Continuidad del Negocio[xvi].
- Los servicios TI estratégicos.
- Los estándares de calidad adoptados.
- El histórico de interrupciones graves de los servicios TI.
- Las expectativas de negocio.
- La disponibilidad de recursos.

La Gestión de la Continuidad del Servicio está abocada al fracaso si no se destina una cantidad de recursos suficientes, tanto en el plano humano como de equipamiento (software y hardware). Su dimensión depende de su alcance y sería absurdo y contraproducente instaurar una política demasiado ambiciosa que no dispusiera de los recursos correspondientes.

Una importante parte del esfuerzo debe destinarse a la formación del personal. Éste debe interiorizar su papel en momentos de crisis y conocer perfectamente las tareas que se espera desempeñe: una emergencia no es el mejor momento para estudiar documentación y manuales.

FASE 2: Análisis de Impacto

Una correcta Gestión de la Continuidad del Servicio requiere en primer lugar determinar el impacto que una interrupción de los servicios TI pueden tener en el negocio.

En la actualidad casi todas las empresas, grandes y pequeñas, dependen en mayor o menor medida de los servicios informáticos, por lo que cabe esperar que un "apagón" de los servicios TI afecte a prácticamente todos los aspectos del negocio. Sin embargo, es evidente que hay servicios TI estratégicos de cuya continuidad puede depender la supervivencia del negocio y otros que "simplemente" aumentan la productividad de la fuerza comercial y de trabajo.

Cuanto mayor sea el impacto asociado a la interrupción de un determinado servicio mayor habrá de ser el esfuerzo realizado en actividades de prevención. En aquellos

casos en que la "solución puede esperar" se puede optar exclusivamente por planes de recuperación.

Los servicios TI han de ser analizados por la ITSCM en función de diversos parámetros:

- Consecuencias de la interrupción del servicio en el negocio:
  - Pérdida de rentabilidad.
  - Pérdida de cuota de mercado.
  - Mala imagen de marca.
  - Otros efectos secundarios.
- Cuánto se puede esperar a restaurar el servicio sin que tenga un alto impacto en los procesos de negocio.
- Compromisos adquiridos a través de los SLAs.

Dependiendo de estos factores se buscará un balance entre las actividades de prevención y recuperación teniendo en cuenta sus respectivos costes financieros.

FASE 3: Evaluación de Riesgos

Sin conocer cuáles son los riesgos reales a los que se enfrenta la infraestructura TI es imposible realizar una política de prevención y recuperación ante desastre mínimamente eficaz.

La Gestión de la Continuidad del Servicio debe enumerar y evaluar, dependiendo de su probabilidad e impacto, los diferentes riesgos factores de riesgo[xvii]. Para ello la ITSCM debe:

- Conocer en profundidad la infraestructura TI y cuáles son los elementos de configuración (CIs) involucrados en la prestación de cada servicio, especialmente los servicios TI críticos y estratégicos.
- Analizar las posibles amenazas y estimar su probabilidad.

- Detectar los puntos más vulnerables de la infraestructura TI.

Ilustración 3 riesgos

Gracias a los resultados de este detallado análisis se dispondrá de información suficiente para proponer diferentes medidas de prevención y recuperación que se adapten a las necesidades reales del negocio.

La prevención frente a riesgos genéricos y poco probables puede ser muy cara y no estar siempre justificada, sin embargo, las medidas preventivas o de recuperación frente a riesgos específicos pueden resultar sencillas, de rápida implementación y relativamente baratas.

Por ejemplo, si el riesgo de pérdida de alimentación eléctrica es elevado debido, por ejemplo, a la localización geográfica se puede optar por deslocalizar ciertos servicios TI a través de ISPs que dispongan de sistemas de generadores redundantes o adquirir generadores que proporcionen la energía mínima necesaria para alimentar los CIs de los que dependen los servicios más críticos, etcétera.

FASE 4: Estrategias de Continuidad

La continuidad de los servicios TI puede conseguirse bien mediante medidas preventivas[xviii], que eviten la interrupción de los servicios, o medidas reactivas, que recuperen unos niveles aceptables de servicio en el menor tiempo posible.

Es responsabilidad de la Gestión de la Continuidad del Servicio diseñar actividades de prevención y recuperación que ofrezcan las garantías necesarias a unos costes razonables.

Actividades preventivas

Las medidas preventivas requieren un detallado análisis previo de riesgos y vulnerabilidades. Algunos de ellos serán de carácter general: incendios, desastres naturales, etcétera, mientras que otros tendrán un carácter estrictamente informático: fallo de sistemas de almacenamiento, ataques de hackers, virus informáticos, etcétera.

La adecuada prevención de los riesgos de carácter general depende de una estrecha colaboración con la Gestión de la Continuidad del Negocio (BCM) y requieren medidas que implican a la infraestructura "física" de la organización.

La prevención de riesgos y vulnerabilidades "lógicas" o de hardware requiere especial atención de la ITSCM. En este aspecto es esencial la estrecha colaboración con la Gestión de la Seguridad.

Los sistemas de protección habituales son los de "Fortaleza" que ofrecen protección perimetral a la infraestructura TI. Aunque imprescindibles no se hallan

exentos de sus propias dificultades pues aumentan la complejidad de la infraestructura TI y pueden ser a su vez fuente de nuevas vulnerabilidades.

Actividades de recuperación

Tarde o temprano, por muy eficientes que seamos en nuestras actividades de prevención, será necesario poner en marcha procedimientos de recuperación.

En líneas generales existen tres opciones de recuperación del servicio:

- Cold standby: que requiere un emplazamiento alternativo en el que podamos reproducir en pocos días nuestro entorno de producción y servicio. Esta opción es la adecuada si los planes de recuperación estiman que la organización puede mantener sus niveles de servicio durante este periodo sin el apoyo de la infraestructura TI.
- Warm standby: que requiere un emplazamiento alternativo con sistemas activos diseñados para recuperar los servicios críticos en un plazo de entre 24 y 72 horas.
- Hot standby: que requiere un emplazamiento alternativo con una replicación continua de datos y con todos los sistemas activos preparados para la inmediata sustitución de la estructura de producción. Ésta es evidentemente la opción más costosa y debe emplearse sólo en el caso de que la interrupción del servicio TI tuviera inmediatas repercusiones comerciales.

Por supuesto, existe otra alternativa que consiste en hacer "poco o nada" y esperar que las aguas vuelvan naturalmente a su cauce.

FASE 5: Organización y Planificación

Una vez determinado el alcance de la ITSCM, analizados los riesgos y vulnerabilidades y definidas unas estrategias de prevención y recuperación es necesario asignar y organizar los recursos necesarios. Con ese objetivo la Gestión de la

Continuidad del Servicio debe elaborar una serie de documentos entre los que se incluyen:

- Plan de prevención de riesgos.
- Plan de gestión de emergencias.
- Plan de recuperación.

Plan de prevención de riesgos

Cuyo objetivo principal es el de evitar o minimizar el impacto de un desastre en la infraestructura TI.

Entre las medidas habituales se encuentran:

- Almacenamiento de datos distribuidos.
- Sistemas de alimentación eléctrica de soporte.
- Políticas de back-ups.
- Duplicación de sistemas críticos.
- Sistemas de seguridad pasivos.

Plan de gestión de emergencias

Las crisis suelen provocar "reacciones de pánico" que pueden ser contraproducentes y a veces incluso más dañinas que las provocadas por el incidente que las causó. Por ello es imprescindible que en caso de situación de emergencia estén claramente determinadas las responsabilidades y funciones del personal así como los protocolos de acción correspondientes.

En principio los planes de gestión de emergencias deben tomar en cuenta aspectos tales como:

- Evaluación del impacto de la contingencia en la infraestructura TI.
- Asignación de funciones de emergencia al personal del servicio TI.
- Comunicación a los usuarios y clientes de una grave interrupción o degradación del servicio.
- Procedimientos de contacto y colaboración con los proveedores involucrados.
- Protocolos para la puesta en marcha del plan de recuperación correspondiente.

Plan de recuperación

Cuando la interrupción del servicio es inevitable, llega el momento de poner en marcha los procedimientos de recuperación.

El plan de recuperación debe incluir todo lo necesario para:

- Reorganizar al personal involucrado.
- Reestablecer los sistemas de hardware y software necesarios.
- Recuperar los datos y reiniciar el servicio TI.

Los procedimientos de recuperación pueden depender de la importancia de la contingencia y de la opción de recuperación asociada ("cold o hot stand-by"), pero en general involucran:

- Asignación de personal y recursos.
- Instalaciones y hardware alternativos.
- Planes de seguridad que garanticen la integridad de los datos.
- Procedimientos de recuperación de datos.
- Contratos de colaboración con otras organizaciones.
- Protocolos de comunicación con los clientes.

Cuando se pone en marcha un plan de recuperación no hay espacio para la improvisación, cualquier decisión puede tener graves consecuencias tanto en la percepción que de nosotros tengan nuestros clientes como en los costes asociados al proceso.

Aunque pueda resultar paradójico, un "desastre" puede ser una buena oportunidad para demostrar a nuestros clientes la solidez de nuestra organización TI y por tanto, incrementar la confianza que tiene depositada en nosotros. Ya conocen el dicho: "No hay mal que por bien no venga".

FASE 6: Supervisión de la Continuidad

Una vez establecidas las políticas, estrategias y planes de prevención y recuperación, es indispensable que éstos no queden en papel mojado y que la organización TI esté preparada para su correcta implementación.

Ello depende de dos factores clave: la correcta formación del personal involucrado y la continua monitorización y evaluación de los planes para su adecuación a las necesidades reales del negocio.

Formación

Es inútil disponer de unos completos planes de prevención y recuperación si las personas que eventualmente deben llevarlos a cabo no están familiarizadas con los mismos.

Es indispensable que la ITSCM:

- Dé a conocer al conjunto de la organización TI los planes de prevención y recuperación.
- Ofrezca formación específica sobre los diferentes procedimientos de prevención y recuperación.
- Realice periódicamente simulacros para diferentes tipos de desastres con el fin de asegurar la capacitación del personal involucrado.
- Facilite el acceso permanente a toda la información necesaria, por ejemplo, a través de la Intranet o portal B2E de la empresa.

Actualización y auditorías

Tanto las políticas, estrategias y planes han de ser actualizados periódicamente para asegurar que responden a los requisitos de la organización en su conjunto.

Cualquier cambio en la infraestructura TI o en los planes de negocio puede requerir de una profunda revisión de los planes en vigor y una consecuente auditoría que evalúe su adecuación a la nueva situación.

En ocasiones en que el dinamismo del negocio y los servicios TI lo haga recomendable, estos procesos de actualización y auditoría pueden establecerse de forma periódica.

La Gestión de Cambios juega un papel esencial a la hora de asegurar que los planes de recuperación y prevención están actualizados, manteniendo informada a la ITSCM de los cambios realizados o previstos.

4. Marco actual

1. Entorno de trabajo actual

En este apartado vamos a realizar una explicación detallada de la infraestructura actual TI de nuestro entorno. Con el siguiente diagrama nos basaremos para informar mejor cada elemento que componen la infraestructura, que tienen como objetivo servir aplicaciones de estándar J2EE[xix].

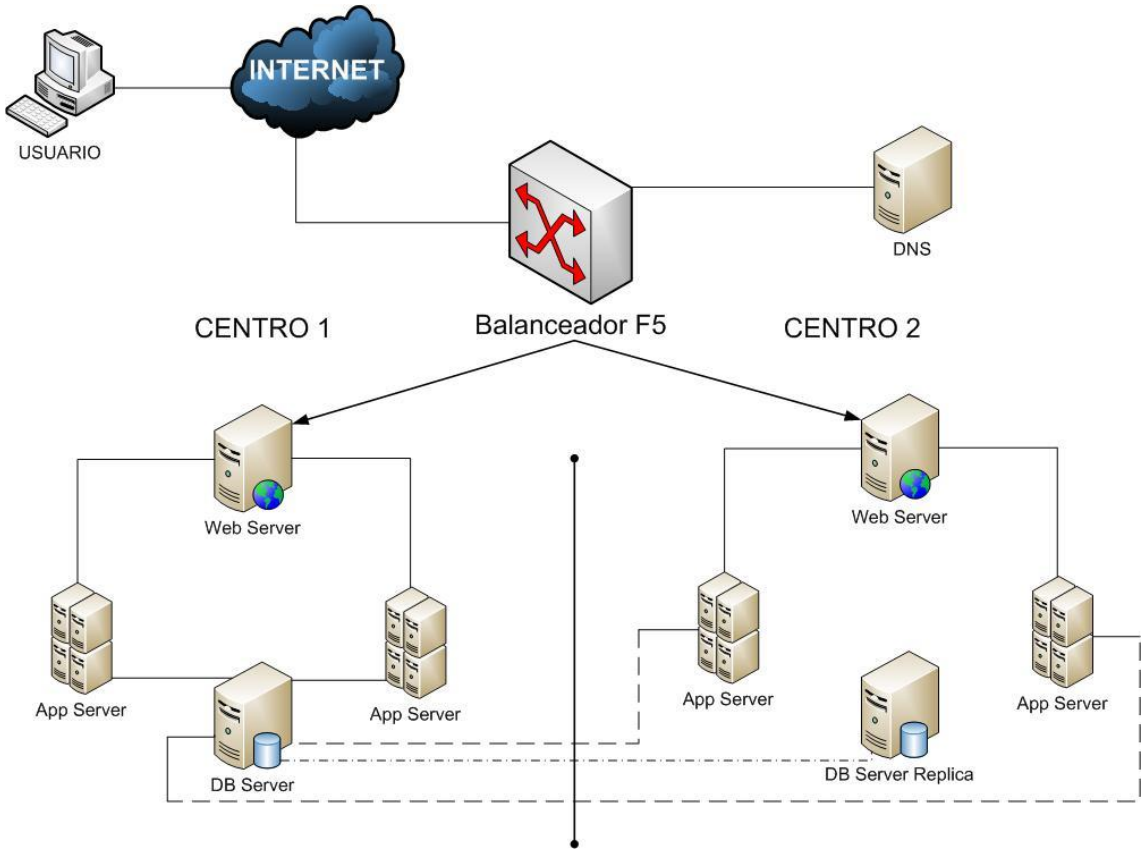

Ilustración 4 Diagrama topológico

Como se puede observar en la imagen, contamos previamente con un balanceador F5 que se sirve de un servidor DNS interno para direccionamiento virtual.

Tras esto, dividimos la infraestructura en dos centros totalmente iguales excepto en la parte de BBDD que explicaremos más adelante.

El balanceador F5 balanceara entre el Apache que escucha en el Centro 1 y en el Centro 2 dependiendo de la carga que tengan en ese momento cada uno. El que menos carga tenga en el instante de la petición recibida del usuario, es el que recibirá dicha información.

Una vez la petición llega al Apache de Centro 1 o Centro 2, este mismo la trata utilizando para redireccionar a los AppServers un plugin. Este plugin contiene un virtual host que filtra las peticiones por el host específico creado para acceder a la aplicación. Esperando esta petición detrás del Apache hay dos AppServers por cada centro, y este balanceo será mediante round robin con el mismo peso entro los dos. De cara a mejorar el rendimiento de respuesta de los servidores, los Apache sirven al usuario todo el contenido estático (jpg, gif, etc.), así liberando a los AppServers de servirlo, dejándoles servir solo el contenido dinámico (jsp, servlets, etc.)

Los AppServers reciben la petición, en concreto lo recibe uno de los dos, procesando así la información y conectando la BBDD en caso necesario. Además de utilizar el servicio de MQ instalado en cada AppServer. Los montajes de MQ, NFS y de BBDD los pasamos a explicar a continuación.

El montaje de la BBDD es de alta disponibilidad, contamos un una instancia de BBDD en centro 1, la cual se replica continuamente con una instancia en centro 2. Pero la única activa sería la BBDD de centro 1. En caso de problemas con la instancia de centro 1, si podría desactivar esta y activar la instancia de centro 2 sin pérdida de información y en cuestión de minutos.

La parte de MQ, tenemos configurado manager en cada appServer, teniendo solo activas las de las máquinas impares, y las maquinas pares estas inactivas para activar en caso de contingencia.

Como todo infraestructura de aplicaciones J2EE HA, necesitamos datos replicados entre las diferentes instancias de aplicaciones para que el usuario entre por donde entre pueda acceder a la misma información siendo trasparente para el cualquier mecanismo de replicación. Para esta funcionalidad, nuestro sistema consta de NFS, montados en cada máquina, cuyos datos se alojan en un servidor de NFS SAN externo.

En el caso concreto de los trasferencia de ficheros mediante utilizamos la tecnología XCOM, y los datos se alojan en estos NFS montados anteriormente. Pero con la excepción de que estos ficheros, solo se alojan en los servidores de centro 1, y existe un mecanismo de replicación de datos a nivel del servidor de NFS. En centro 2, se montarían los NFS en caso de contingencia pero con los puntos de montaje de contingencia del servidor NFS.

2. Análisis del problema

Tal y como hemos hablado en el anterior apartado, la infraestructura explicada es bastante compleja, con muchos elementos de infraestructura peliagudos. En cuanto al método de la división por centros facilita mucho el aislamiento de máquinas defectuosas o con problemas. Excepto para los elementos de BBDD y NFS los cuales son diferentes a los AppServers.

El planteamiento inicial es bueno, pero el problema viene cuando surgen situaciones de riesgo o caída del servicio. La situación planteada corresponde en un momento en el que la contingencia se ha de activar, ya sea porque la infraestructura de Centro1 se ha visto afectada, o la de Centro2 o algún elemento de BBDD, NFS, etc.

En este caso, nuestro problema viene en quién, cómo y cuándo realizar la activación del plan de contingencia y las tareas sucesivas a ejecutar. La deficiencia actual está presente porque estas tareas las hacen técnicos especializados del departamento de sistemas de Java, BBDD, Storage, Comunicaciones, F5, y los operadores finalmente y tanta gente implicada es deficiente, costosa y poco productiva.

A continuación exponemos una serie de tablas con tiempos medios de respuesta ante una caída del servicio, recursos utilizados y coste aproximado.

Tabla 1 ANALISIS DE TIEMPOS

Elemento de Gestion	Tiempo medio	Porcentaje Delegable a los operadores
Gestión de las BBDD	3 horas	100%
Gestión de los NFS	2 horas	100%
Gestión de los servidores Web	2 horas	100%
Gestión de los servidores de Aplicaciones	2 horas	100%
Gestión de la carga de tráfico	1 hora	100%
Gestión del DNS	1 hora	100%
Gestión de Colas de Mensajeria	1 hora	100%
Gestión de las distribuciones de SW	30 minutos	100%
TOTALES	12 horas 30 minutos	100%

Tabla 2 ANALISIS DE RECURSOS

Elemento de Gestion	Recusos Utilizados	Disponibilidad de Guardia
Gestión de las BBDD	1 especialista + 1 técnico	Sí
Gestión de los NFS	1 especialista	Sí
Gestión de los servidores Web	1 especialista + 1 técnico	Sí
Gestión de los servidores de Aplicaciones		
Gestión de la carga de tráfico	1 especialista	Sí
Gestión del DNS	1 especialista	Sí
Gestión de Colas de Mensajeria	1 especialista	Sí
Gestión de las distribuciones de SW	1 especialista	Sí
TOTALES	9 recursos	Todos

Tabla 3 ANALISIS DE PRECIOS

Elemento de Gestion	Tiempo medio	Precio Hora Fuera de horario de oficina	Gasto Medio
Gestión de las BBDD	3 horas	35€	105€
Gestión de los NFS	2 horas	35€	70€
Gestión de los servidores Web	2 horas	35€	70€
Gestión de los servidores de Aplicaciones	2 horas	35€	70€
Gestión de la carga de tráfico	1 hora	35€	35€
Gestión del DNS	1 hora	35€	35€
Gestión de Colas de Mensajeria	1 hora	35€	35€
Gestión de las distribuciones de SW	30 minutos	35€	35€ (horas absolutas)
TOTALES	12 horas 30 minutos	-	455€

5. Aplicación práctica

En el siguiente capítulo, trataremos de exponer la aplicación práctica de la teoría expuesta anteriormente para realizar un plan de contingencia TI. Siguiendo paso a paso lo explicado.

Etapa 1: Análisis y Selección de las Operaciones Críticas

En esta etapa hay que definir cuáles serán nuestras operaciones críticas y tienen que ser definidas en función a los componentes de los sistemas de información los cuales son: Datos, Aplicaciones, Tecnología Hardware y Software, instalaciones y personal.

Dentro de las cuales podemos identificar las siguientes, las cuales pueden variar de sistema a sistema:

- Gestión de las BBDD
- Gestión de los NFS
- Gestión de los servidores Web
- Gestión de los servidores de Aplicaciones
- Gestión de la carga de tráfico
- Gestión del DNS
- Gestión de Colas de Mensajeria
- Gestión de las distribuciones de SW

Se ha listado los procesos críticos de manera genérica y evaluado su grado de importancia en función a la magnitud del impacto si los procesos pueden detenerse, y luego clasificados en niveles A (Alta), M (Media) y B (Baja).

Se tiene que elaborar una tabla denominada Operaciones Críticas de los SI, que consta de tres campos:

- Operaciones críticas
- Objetivo de la Operación
- Prioridad de la Operación

Tabla 4: OPERACIONES CRÍTICAS DEL SISTEMA DE INFORMACION

Operaciones Críticas	Objetivos de la Operación	Prioridad de la Operación
Gestión de las BBDD	- Consistencia de los datos - Accesibilidad a los servidores	A
Gestión de los NFS	- Consistencia de los archivos - Accesibilidad a los archivos	M
Gestión de los servidores Web	- Disponibilidad del Servicio Web	M
Gestión de los servidores de Aplicaciones	- Disponibilidad del servicio aplicativo	A
Gestión de la carga de tráfico	- Disponibilidad del servicio de balanceo	M
Gestión del DNS	- Disponibilidad del servicio de DNS	A
Gestión de Colas de Mensajeria	- Disponibilidad de los servicios de mensajería	M
Gestión de las distribuciones de SW	- Disponibilidad del servicio distribuidor de aplicaciones	B

- Estudio Puntual de Fallas
- Considerando el contenido de cada operación, determinar franja de tiempo una interrupción puede ser tolerada.

Tabla 5 LISTA DEL PERIODOS ACEPTABLES DE INTERRUPCION

Operaciones Críticas	Recursos de operaciones	Período aceptable de Interrupción
Gestión de las BBDD	Oracle	22:00 – 06:00
Gestión de los NFS	Storage NFS	19:00 – 06:00
Gestión de los servidores Web	Apache	22:00 – 06:00

Gestión de los servidores de Aplicaciones	WebSphere	22:00 – 06:00
Gestión de la carga de tráfico	F5 Server	22:00 – 06:00
Gestión del DNS	DNS Server	22:00 – 06:00
Gestión de Colas de Mensajeria	Websphere MQ	19:00 – 06:00
Gestión de las distribuciones de SW	Harvest Server	20:00 – 06:00

- Estudie y describe el estado de fabricación de los productos que constituyen recursos
- Las soluciones varían según el período asumido de la parada.
- Calcular y describir el período que se pasará hasta la recuperación del elemento afectado, basado en la información confirmada.

Tabla 6 LISTA DE PROBLEMAS PROBABLES A OCURRIR

Operaciones Críticas	**Recursos de operaciones**	**Juicio de Técnicos**	
		Posibilidad de problema	**Periodo de recuperación**
Gestión de las BBDD	Oracle	Alta	3 horas
Gestión de los NFS	Storage NFS	Baja	1 hora
Gestión de los servidores Web	Apache	Baja	1 hora
Gestión de los servidores de Aplicaciones	WebSphere	Media	2 horas
Gestión de la carga de tráfico	F5 Server	Baja	1 hora
Gestión del DNS	DNS Server	Baja	2 horas
Gestión de Colas de Mensajeria	Websphere MQ	Media	2 horas
Gestión de las distribuciones de SW	Harvest Server	Alta	2 horas

Etapa 2: Identificación de Procesos en cada Operación

Para cada una de las operaciones críticas en la Etapa 1, se debe enumerar los procesos que tienen. Los responsables de desarrollar los planes de contingencia deben de coordinar en cooperación con el personal a cargo de las operaciones de los Sistemas Analizados, los cuales son conocedores de dichos procesos críticos.

Se debe de investigar qué recursos administrativos (equipamiento, herramientas, sistemas, etc.) son usados en cada proceso, se ha descrito y codificado cada recurso, como: sistema eléctrico, tarjetas, transporte, red de datos, PC's. A su vez también se ha determinado su novel de riesgo, como críticos y no críticos.

La tabla elaborada contiene cinco campos:

- Operación
- Procesos
- Necesidad de soporte
- Nivel de Riesgo

Tabla 7 PROCESOS DE LAS OPERACIONES

Operaciones Críticas	Procesos	Necesidad Soporte	Nivel de Riesgo
Gestión de las BBDD		Alto	Alto
Gestión de los NFS		Bajo	Medio
Gestión de los servidores Web		Bajo	Medio
Gestión de los servidores de Aplicaciones		Medio	Medio
Gestión de la carga de tráfico		Medio	Bajo
Gestión del DNS		Bajo	Medio
Gestión de Colas de Mensajeria		Bajo	Bajo

Gestión de las distribuciones de SW		Bajo	Bajo

Etapa 3: Listar los Recursos Utilizados para las Operaciones

En esta etapa se identifica a los proveedores de los servicios y recursos usados, considerados críticos, para los procesos de cada operación en la Etapa 2.

- Se tiene que identificar los recursos asociados al Sistema de Información, basados en los códigos del recurso descritos en la etapa 2.
- Se investiga y describe, si los recursos están dentro del Sistema de Información o fuera de este, (como compra a otros proveedores de servicios externos o productos).
- Se investiga y describe a los proveedores de servicios y recursos.

La siguiente tabla contiene los siguientes campos:

- Recurso
- Ubicación
- Proveedor del Servicio

Tabla 8 LISTA DE RECURSOS CRITICOS UTILIZADOS

Recursos de operaciones	Ubicación	Proveedor del Servicio
Oracle	Interno	Técnica de sistemas BBDD
Storage NFS	Externo	Proveedor
Apache	Interno	Técnica de sistemas J2EE
WebSphere	Interno	Técnica de sistemas J2EE
F5 Server	Interno	Técnica de sistemas Balanceadores
DNS Server	Interno	Técnica de Sistemas Comunicaciones
Websphere MQ	Externo	Proveedor
Harvest Server	Interno	Técnica de sistemas Harvest

Etapa 4: Especificación de Escenarios en los cuales puede ocurrir los Problemas

- En consideración de la condición de preparar medidas preventivas para cada recurso, se ha evaluado su posibilidad de ocurrencia del problema como (alta, mediana, pequeña).

- Se calculará y describirá el período que se pasará hasta la recuperación en caso de problemas, basados en información confirmada relacionada con los Sistemas de Información.

Mediante el siguiente cuadro podemos elaborar la Probabilidad de fallos de cada uno de los recursos identificados

Tabla 9 TABLA DE PROBABILIDAD DE FALLOS DE RECURSOS

Recursos de operaciones	Probabilidad			
	Alta	**Media**	**Baja**	**Ninguna**
Oracle		X		
Storage NFS			X	
Apache			X	
WebSphere		X		
F5 Server			X	
DNS Server			X	
Websphere MQ			X	
Harvest Server	X			

La siguiente tabla presenta los siguientes campos:

- Recurso
- Proveedor del Servicio (Departamento o Externalizado)
- Análisis de Riesgo (probabilidad del problema, período necesario para la recuperación, frecuencia de uso)

Tabla 10 LISTA DE PROBLEMAS PROBABLES A OCURRIR

Recursos de operaciones	**Proveedor del Servicio**	**Análisis de Riesgo**		
		Probabilidad del problema	**Periodo necesario para la recuperación**	**Frecuencia de uso**
Oracle	Técnica de sistemas BBDD	Alta	1 hora	
Storage NFS	Externalizado	Media	30 minutos	
Apache	Técnica de sistemas J2EE	Media	30 minutos	
WebSphere	Técnica de sistemas J2EE	Alta	1 hora	
F5 Server	Técnica de sistemas Balanceadores	Media	30 minutos	
DNS Server	Técnica de Sistemas Comunicaciones	Alta	30 minutos	
Websphere MQ	Externalizado	Baja	1 hora	
Harvest Server	Técnica de sistemas Harvest	Baja	1 hora	

Mediante la siguiente tabla debemos de priorizar los riesgos identificados tomando en cuenta tanto el impacto del riesgo como la probabilidad de una falla en el área como sigue:

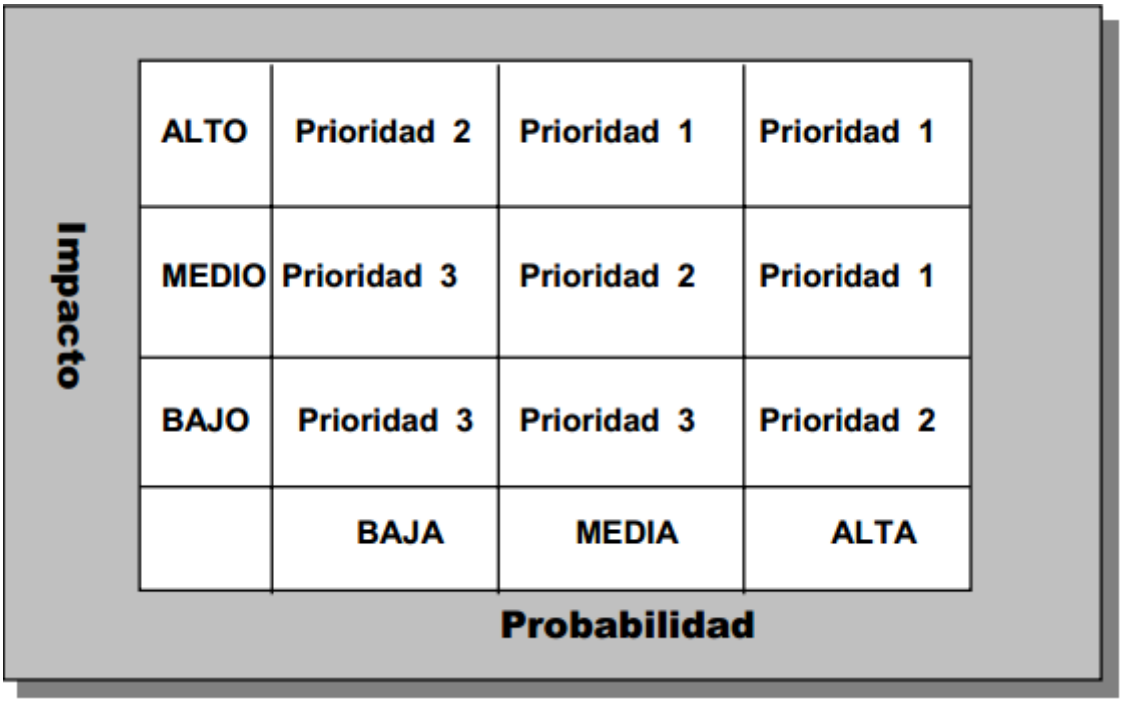

Ilustración 5 MATRIZ DE PRIORIDADES DE ATENCION DE RIESGOS

Etapa 5: Determinar y Detallar las Medidas Preventivas

Tal y como hemos hablado en los últimos puntos, nuestro problema más grande a resolver es la utilización de recursos y el tiempo empleado a la hora de activar o desactivar el plan de contingencia.

Este nuevo plan que hemos diseñado focalizará todas las tareas en un único punto de ejecución, cuyo grupo principal será el departamento de operadores de la compañía. Se conoce que las habilidades técnicas de los integrantes no son de nivel experto, pero su trabajo diario y su conocimiento de la infraestructura les permitirán seguir unos procedimientos y tareas creadas por los diferentes equipos técnicos implicados.

Como hemos comentado, como primer paso para realizar el nuevo plan, cada técnica de sistemas (BBDD, STORAGE, J2EE, DNS) deberá automatizar sus tareas para que un operador formado mínimamente pueda ejecutar tareas de administración

avanzada. Una vez cada grupo tenga las herramientas/manuales/scripts desarrollados, se creará un modelo a seguir para cada activación y desactivación de la contingencia.

Para tener un sistema centralizado de herramientas, a parte de un repositorio de documentos, a nivel técnico en cada una de las máquinas implicadas se crearán mediante Bash Scripting una serie de "Menú Operadores" en los cuales los técnicos irán implementando sus scripts para que un operador mediante este menú los utilice.

Base de Datos

Desde el grupo de sistemas de BBDD necesitarán tener las siguientes tareas automatizadas:

- Parada y arranque de BBDD: Scripts de Bash que se conecta a BBDD y realiza la parada o arranque automáticamente.
- Gestión de réplicas de BBDD: Manuales a seguir por operadores para la utilización de la herramienta de gestión de réplicas.

STORAGE

Las tareas a automatizar por el departamento de STORAGE en este caso serán:

- Gestión de réplicas NFS: Manuales explicativos de las tareas a realizar en las herramientas de gestión de réplicas de NFS.

J2EE

El departamento de sistemas de J2EE es el que engloba más tareas a realizar:

- Para/Arranque de servidores Java
- Montaje y desmontaje de NFS
- Para/Arranque de servidores virtuales Linux

DNS

Este departamento o área debe crear los manuales necesarios para que el operador pueda gestionar los diferentes nombres de dominios implicados.

HARVEST

El departamento que administra esta herramienta deberá gestionar los mecanismos suficientes para que el operador pueda gestionar las líneas de distribución de las aplicaciones. (Parada, estado, arranque)

Etapa 6: Formación y Funciones de los Grupos de Trabajo

Se debe determinar claramente los pasos para establecer los Grupos de Trabajo, desde las acciones en la fase inicial, las cuales son importantes para el manejo de la crisis de administración.

Los Grupos de Trabajo permanecerán en operación cuando los problemas ocurran, para tratar de solucionarlos.

Se elaborará un Organigrama de la estructura funcional de los Grupos de Trabajo.

Tabla 11 FUNCIONES DE LOS GRUPOS DE TRABAJO DEL SISTEMA

Dirección	Nombre	Cargo	Funciones
Técnica de sistemas BBDD		Responsable de sistemas	Responsable de los procesos y operaciones de BBDD
		Técnico Especialista	Técnico soporte experto
		Técnico Operador	Técnico soporte

Proveedor Storage		Responsable de sistemas	Responsable de los procesos y operaciones de Storage
		Técnico Especialista	Técnico soporte experto
Técnica de sistemas J2EE		Responsable de sistemas	Responsable de los procesos y operaciones de J2EE
		Técnico Especialista	Técnico soporte experto
		Técnico Operador	Técnico soporte
Técnica de sistemas Balanceadores		Responsable de sistemas	Responsable de los procesos y operaciones de Balanceadores
		Técnico Especialista	Técnico soporte experto
		Técnico Operador	Técnico soporte
Técnica de Sistemas Comunicaciones		Responsable de sistemas	Responsable de los procesos y operaciones de Comunicaciones
		Técnico Especialista	Técnico soporte experto
		Técnico Operador	Técnico soporte
Proveedor MQ		Responsable de sistemas	Responsable de los procesos y operaciones de MQ
		Técnico Especialista	Técnico soporte experto
Técnica de sistemas Harvest		Responsable de sistemas	Responsable de los procesos y operaciones de Distribuciones
		Técnico Especialista	Técnico soporte experto
		Técnico Operador	Técnico soporte

Etapa 7: Desarrollo de los Planes de Acción

ESQUEMA CONTINGENCIAS

A continuación, vamos a detallar los diferentes escenarios que nos encontramos cuando hemos de realizar una contingencia en uno de los centros de nuestra infraestructura.

ESCENARIO 1:

Activar la contingencia en Centro 1

1. Tareas previas de adecuar el entorno

    - Activar elementos de control de alarmas.
    - Parar todos los Batch.
    - Parar líneas de despliegue de HARVEST.

2. Para Aplication Servers de Centro 1 y servicio WAS de Centro 2:
   "Paramos las máquinas virtuales de Centro1 ya que no darán servicio y paramos tan solo los servicios WAS de centro2 para que los usuarios no tengan afectación durante el cambio de BBDD"

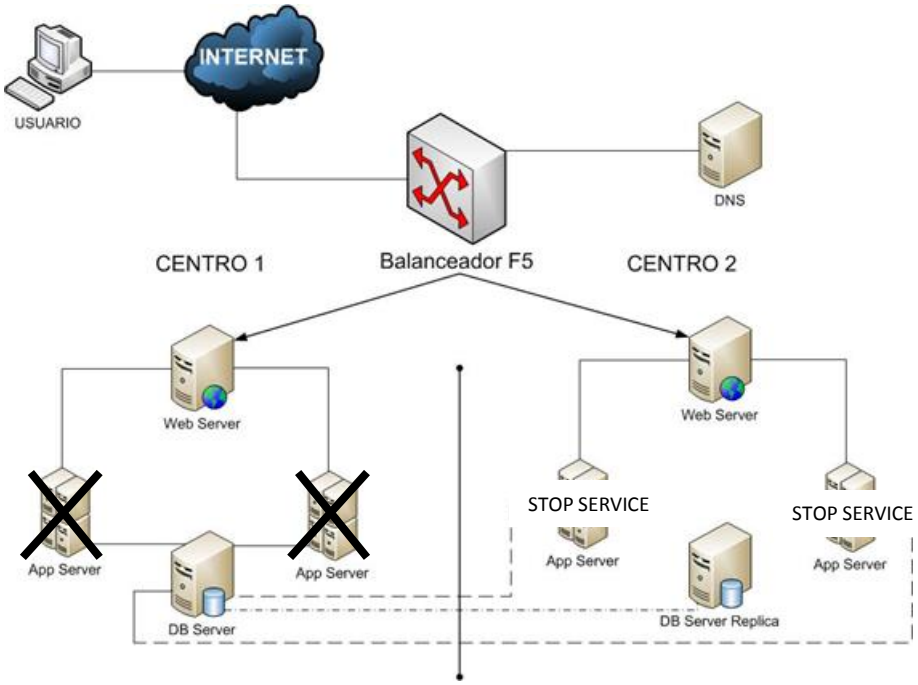

Ilustración 6 Diagrama paro AS

3. Activar Contingencia MQ

   "La contingencia de MQ trata de mover el servicio de Colas MQ a Centro2"

4. Parar de BBDD Centro 1

   "Paramos la BBDD de Centro1 para empezar a mover la BBDD a centro2"

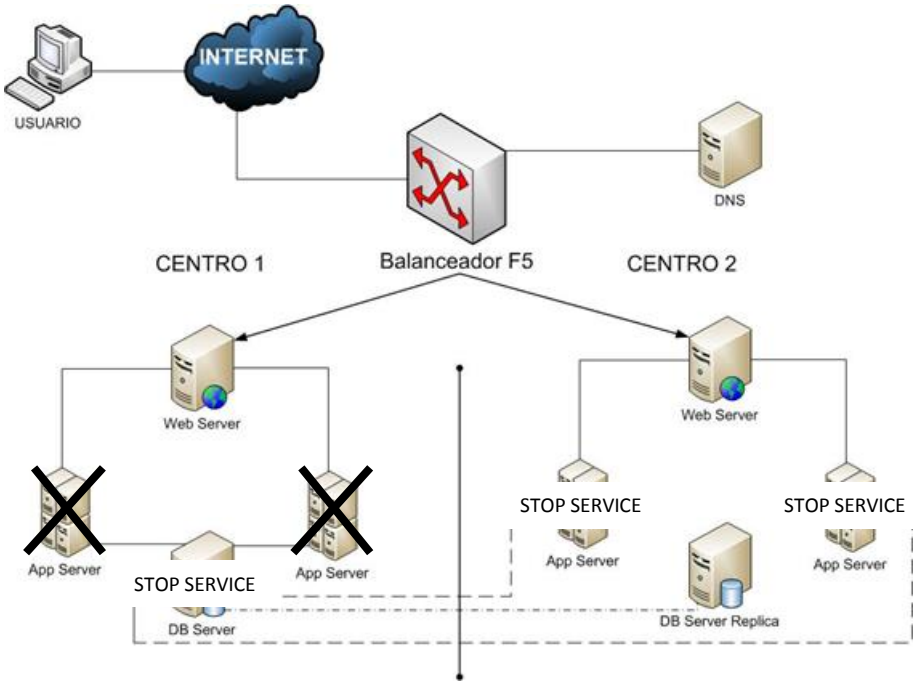

Ilustración 7 Diagrama paro BBDD

5. Cortar réplica Hur BBDD

"La réplica HUR de la BBDD de Centro1 sobre la BBDD de Centro2 la cortamos para que deje de escribir en BBDD"

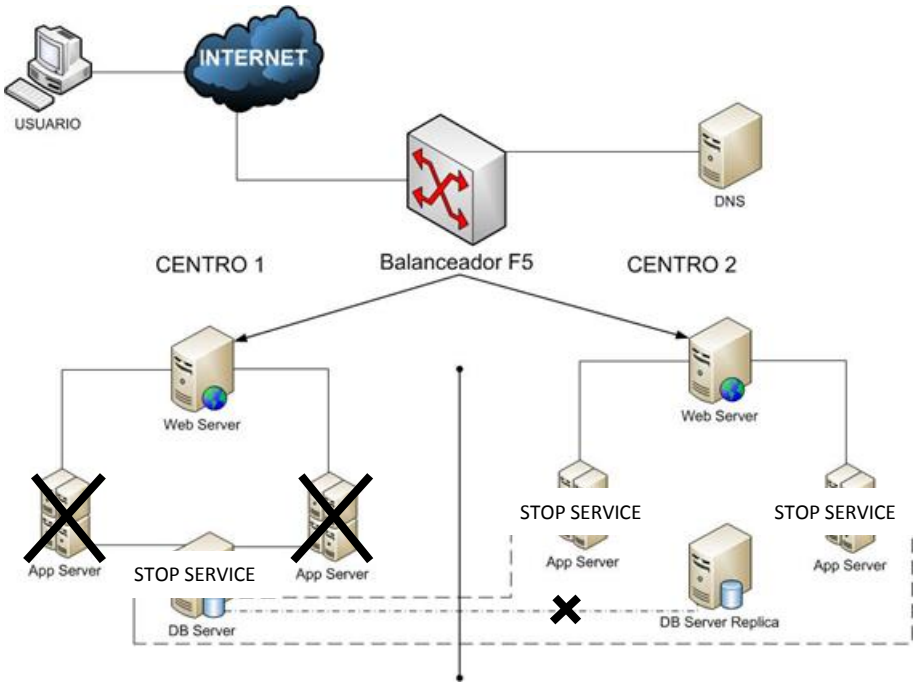

Ilustración 8 Diagrama paro replica BBDD

6. Levantar BBDD Centro 2

   "Una vez sin replica, levantamos BBDD de Centro 2 la cual dará servicio durante la contingencia"

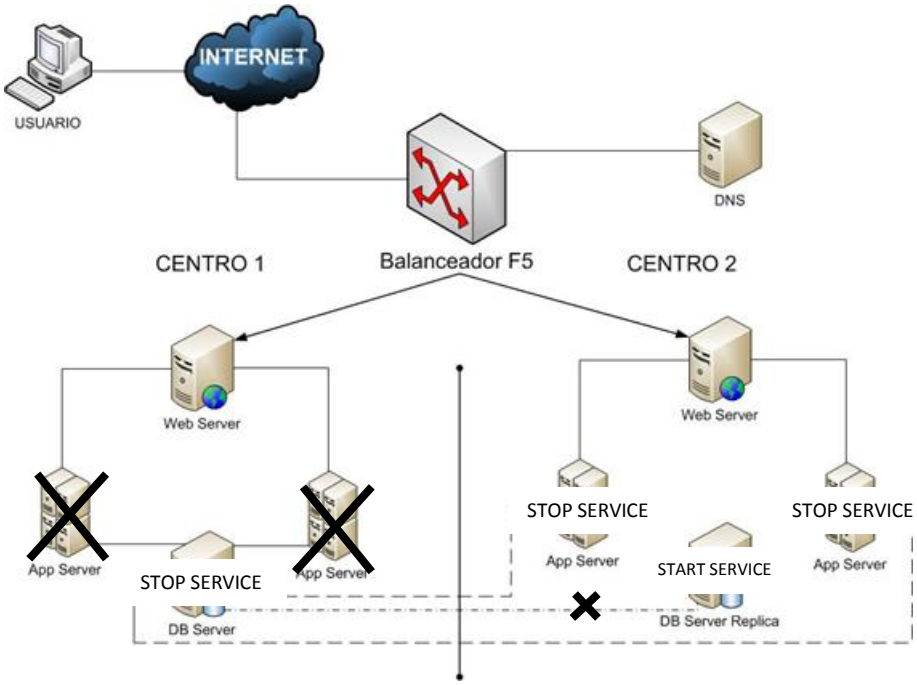

Ilustración 9 Diagrama arranque BBDD replica

7. Revisar BBDD Centro 2

   "Pedimos una revisión al equipo de BBDD para garantizar la no corrupción de los datos"

8. Activar réplica inversa

   "Activamos la réplica de BBDD de Centro 2 contra Centro 1 para no perder los datos dados de alta durante la contingencia"

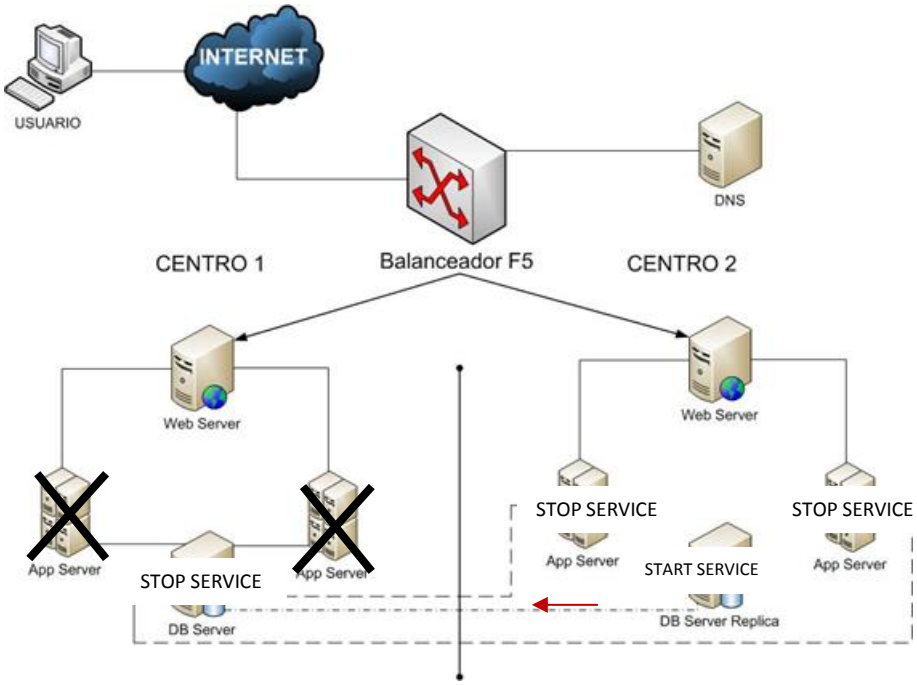

Ilustración 10 Diagrama activar replica BBDD inversa

9. Cortar réplica Hur BATCH

   "La réplica HUR del BATCH de Centro1 sobre Centro2 la cortamos para que deje de escribir"

10. Montar FS BATCH en Centro 2

    "Montamos los FS de Batch sobre Centro 2 sobre los cuales dará servicio durante la contingencia"

11. Activar replica inversa BATCH

    "Activamos la réplica de BATCH de Centro 2 contra Centro 1 para no perder los datos dados de alta durante la contingencia"

12. Acciones DNS

    "Ejecutamos las acciones DNS para que todo los nombres apunten a Centro 2"

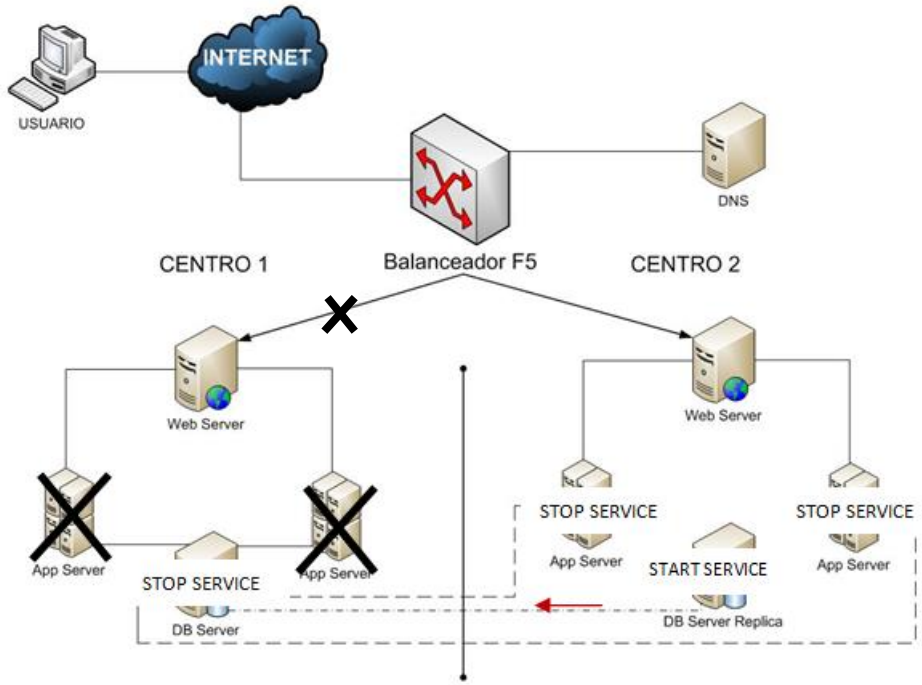

Ilustración 11 diagrama corte trafico DNS

13. Arrancar Aplication Servers Centro 2

"Arrancar los servicios WebSphere de Centro 2 los cuales darán servicio durante la contingencia"

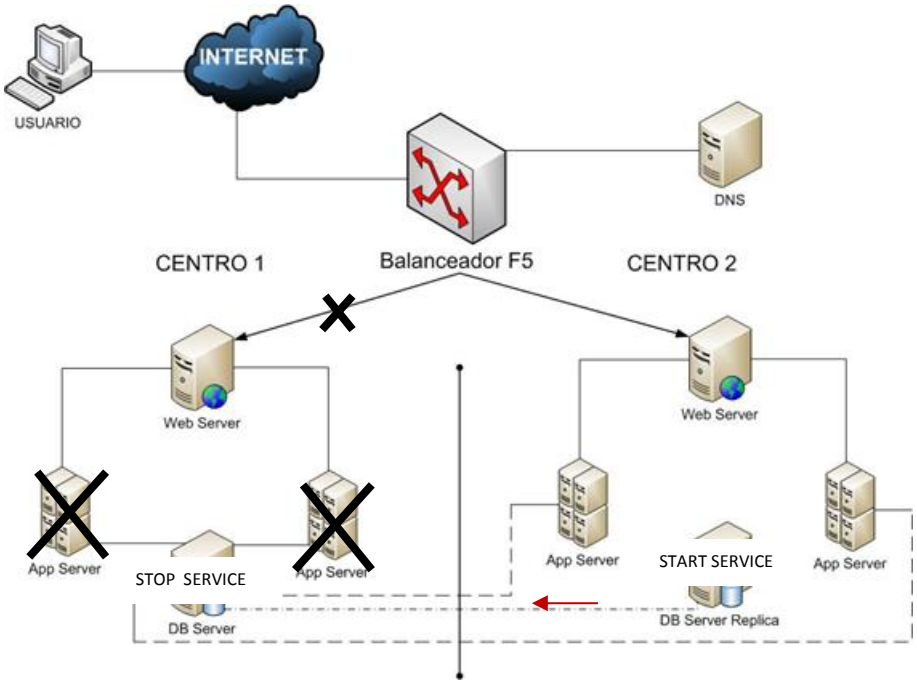

Ilustración 12 Diagrama arranque AS C2

14. Revisar Excepciones aplicativas

    "Revisar por parte aplicativa si existe alguna excepción para completar la contingencia por parte del equipo de desarrollo"

15. Validaciones

    "Realizar las validaciones oportunas por parte del equipo de desarrollo"

16. Tareas de activación el entorno:

    Desactivar elementos de control de alarmas.

    Activar todos los Batch.

    Activar líneas de despliegue teniendo en cuenta parada de control.

Desactivar contingencia en Centro 1 y volver a la situación normal

1. Tareas previas
    - Activar elementos de control de alarmas Centro 2.
    - Parar Batch.
    - Parar líneas de despliegue de HARVEST.

2. Parar Aplication Servers de Centro 2

    "Para las máquinas virtuales de Centro 2 para que no den servicio y no causar afectación al usuario"

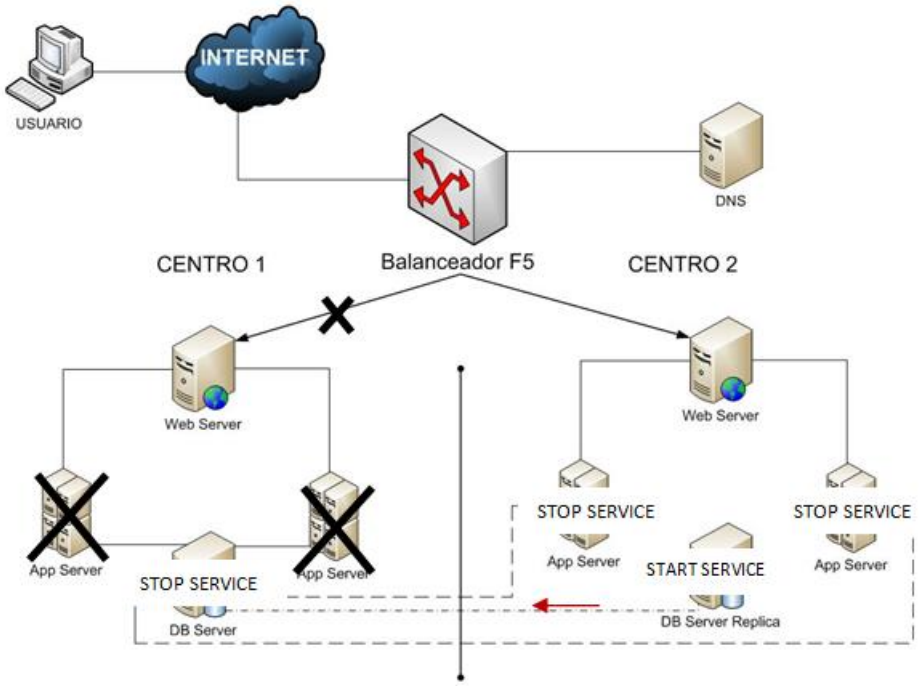

Ilustración 13 Diagrama para de AS C2

3. Desactivar replica inversa BATCH

   "Desactivar la réplica inversa para que durante el cambio de batch no haya problemas con los datos "

4. Desmontar FS BATCH en centro 2.

   "Desmontamos los FS de Batch en Centro 2 para que escriba mas datos y posteriormente se pierdan al activar los batch en Centro 1"

5. Para de BBDD replica

   "Paramos la BBDD de Centro 2 para dejar de escribir en ello y no perder datos"

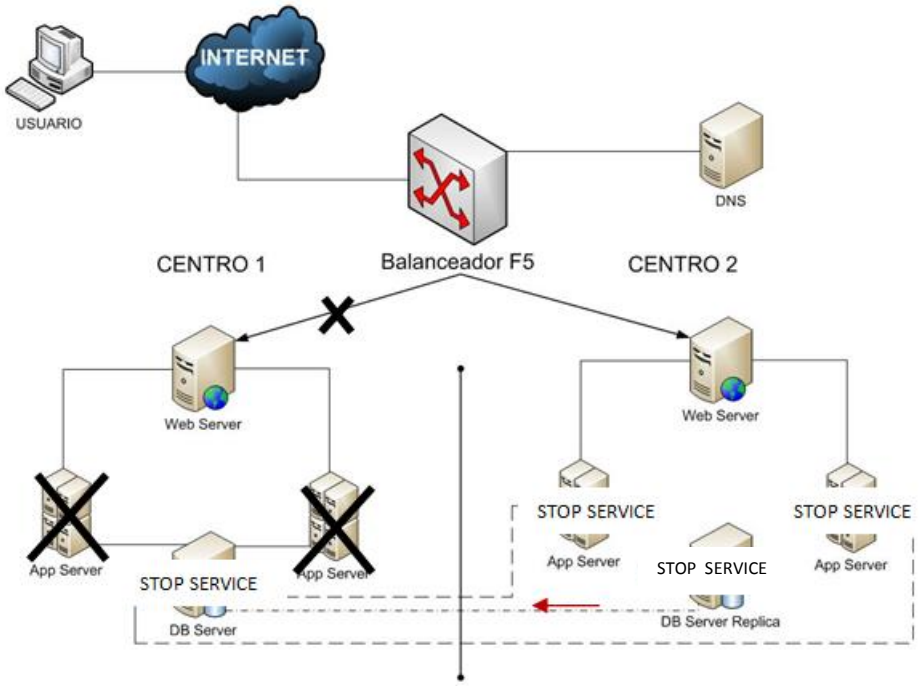

Ilustración 14 Diagrama paro BBDD replica

6. Desactivar Réplica de BBDD

"Desactivamos la réplica de BBDD para posteriormente levantar BBDD de Centro 1"

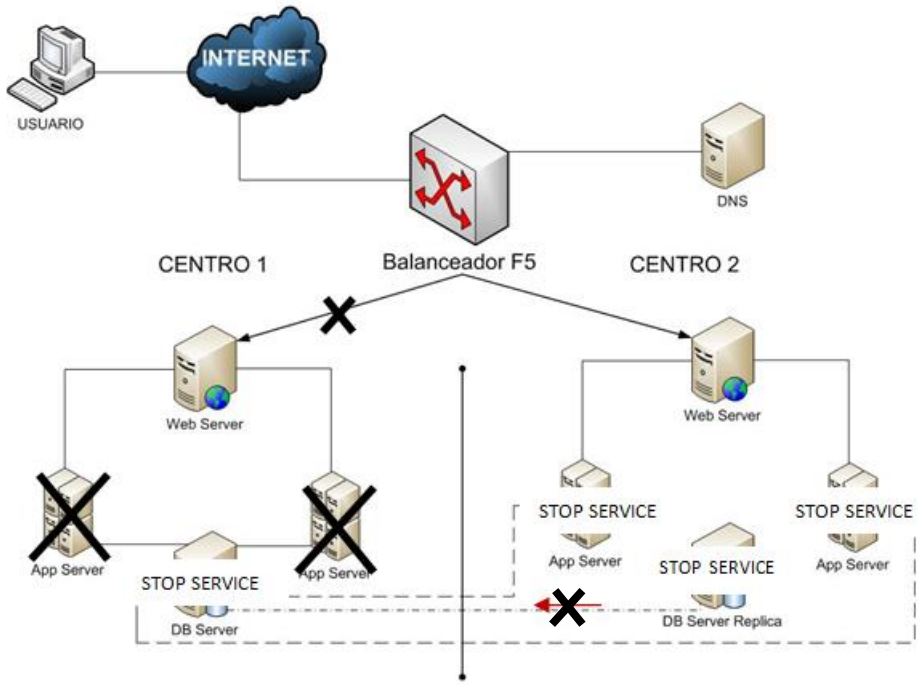

Ilustración 15 Diagrama desactivar replica BBDD inversa

7. Activar BBDD Centro 1

   "Levantamos BBDD de Centro 1 la cual dará servicio"

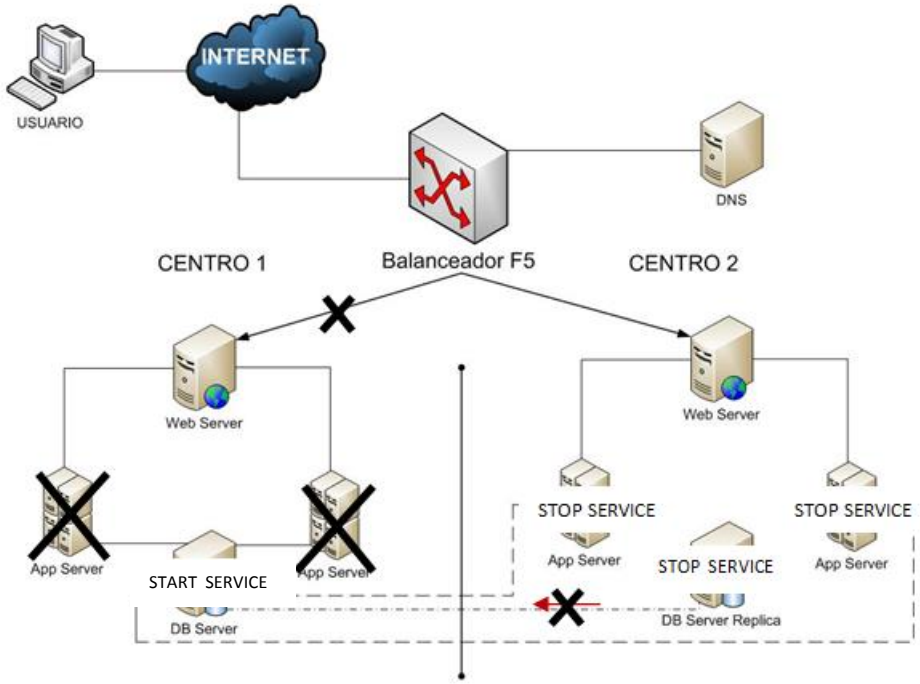

Ilustración 16 Diagrama arranque BBDD

8. Activar réplica Hur

   "Activamos de nuevo la réplica Hur para tener sincronizada la BBDD de réplica"

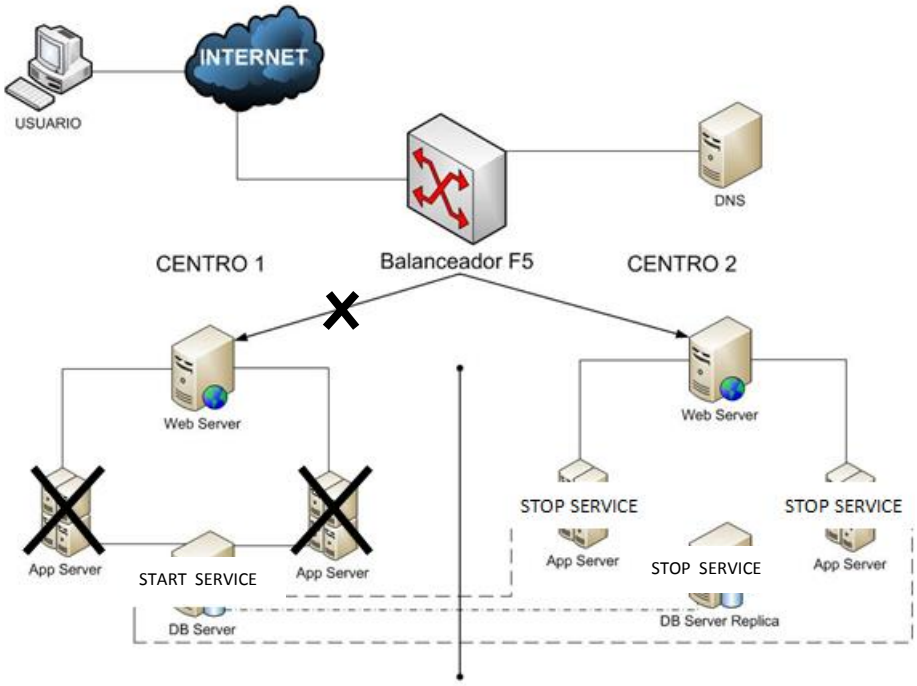

Ilustración 17 Diagrama activar replica BBDD

9. Acciones DNS

   "Realizamos las acciones DNS necesarias para que a nivel de red tanto Centro 1 como Centro 2 esté de nuevo dando servicio"

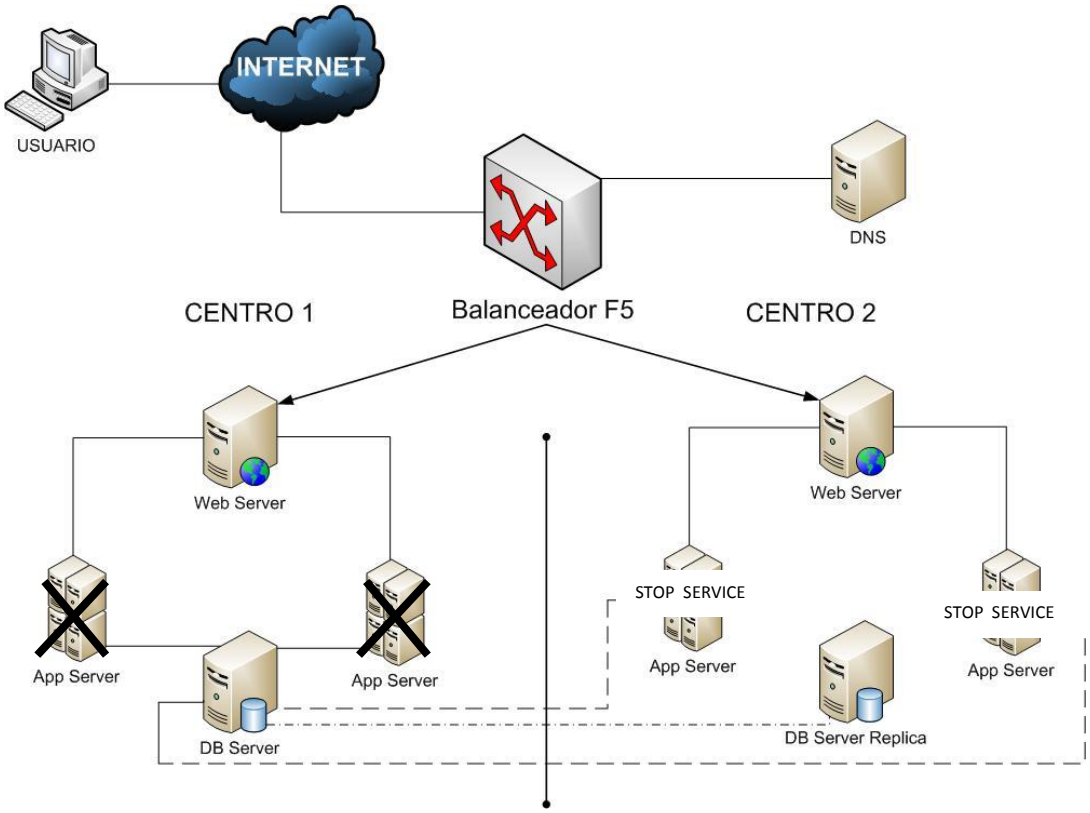

Ilustración 18 Diagrama reanudar trafico DNS

10. Desmontar Contingencia MQ

"Volvemos a montar MQ en los dos Centros"

11. Arrancar Aplication Servers de Centro 1 y Reiniciar Servicio WAS de Centro 2

"Arrancamos las máquinas paradas de Centro 1 y reiniciamos servicios WebSphere de Centro 2 para que vuelvan a conectar con BBDD"

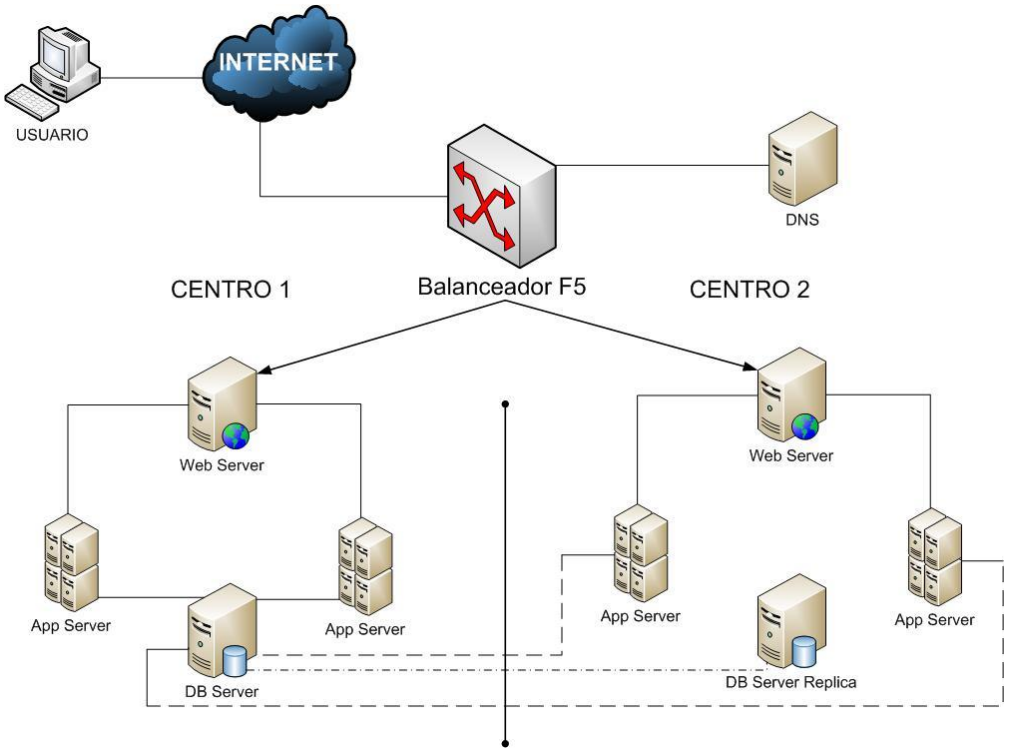

Ilustración 19 Diagrama activar AS

12. Echar marcha atrás excepciones aplicativas

    "Echamos marcha atrás a las excepciones aplicativas realizadas en la activación de la contingencia"

13. Validaciones

14. Tareas de activación:
    - Desactivar BLK Centro 2 y centro1.
    - Activar Batch.
    - Desactivar Contingencia Harvest Centro 1.

ESCENARIO 2:

Activar la contingencia en Centro 2

1. Tareas previas
    - Activar BLK Centro 2.
    - Parar distribuciones Harvest.

2. Para Aplication Servers de Centro 2

   "Paramos las máquinas virtuales de Centro 2 para que dejen de dar servicio"

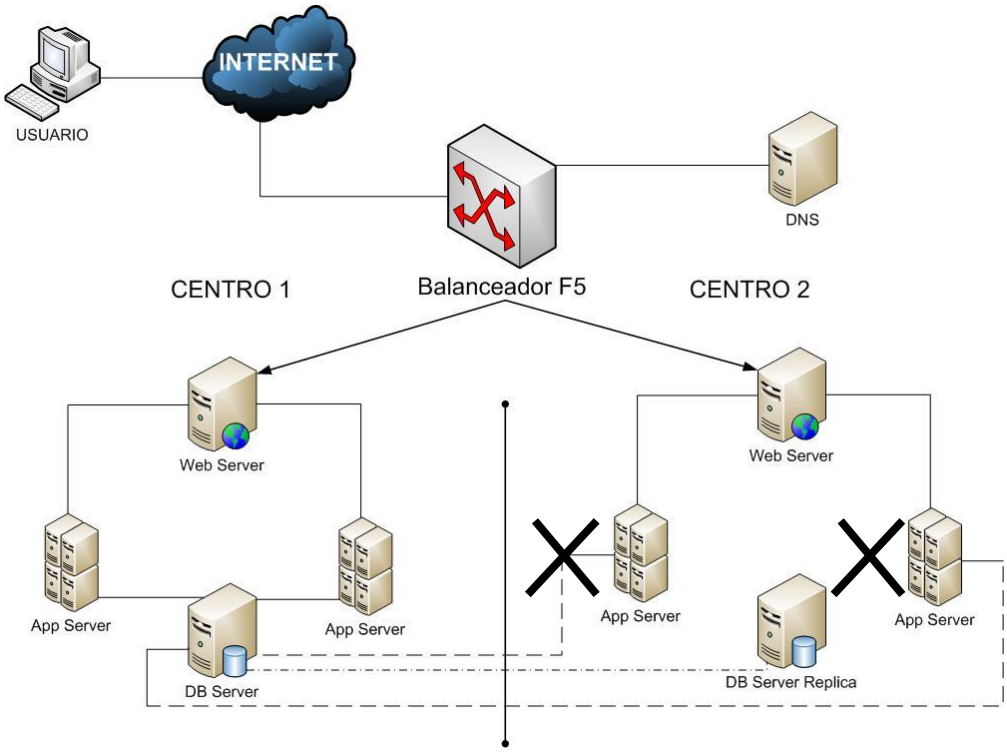

Ilustración 20 Diagrama paro AS C2

3. Contingencia MQ

   "Activamos la contingencia de MQ para que solo de servicio por Centro 1"

4. Revisar Excepciones aplicativas.

   "Revisar por parte aplicativa si existe alguna excepción para completar la contingencia por parte del equipo de desarrollo"

5. Validaciones.

6. Tareas de activación:

   Contingencia Harvest Centro 2.

Desactivar la contingencia en Centro 2

1. Tareas previas
   - Parar distribuciones Harvest.

2. Desmontar contingencia MQ

   "Volvemos a montar MQ en los dos Centros"

3. Arrancar Aplication Servers de centro 2

   "Volvemos a arrancar las máquinas virtuales de Centro 2 para volver a tener servicio por los dos centros"

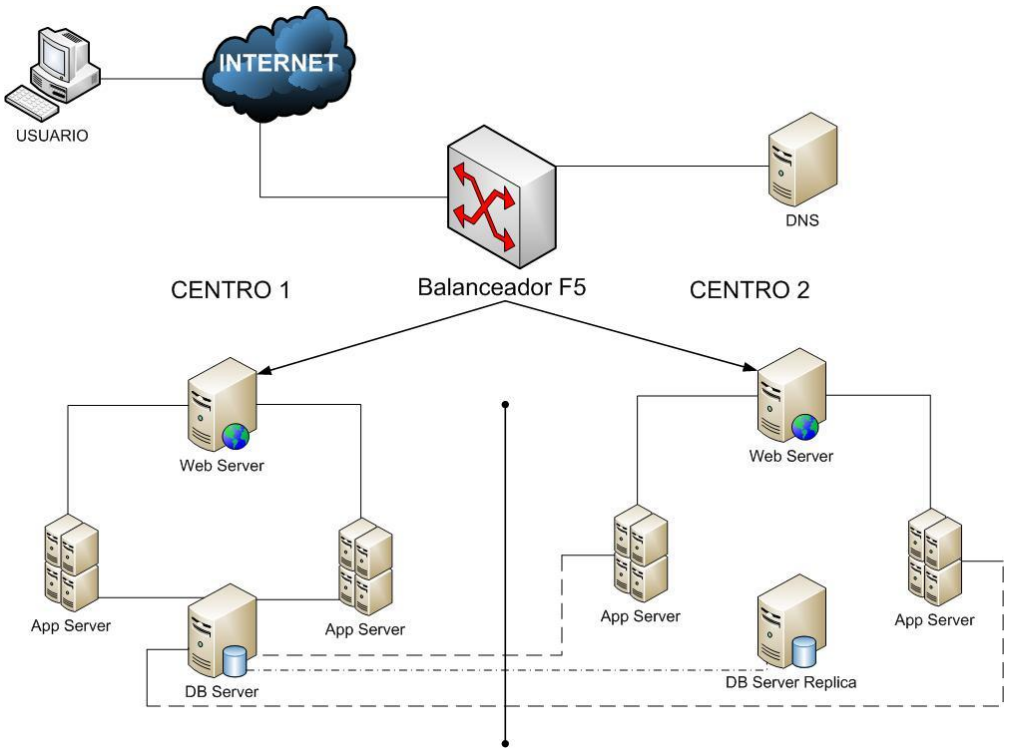

Ilustración 21 Diagrama arranque AS C2

4. Echar marcha atrás excepciones aplicativas

   "Echamos marcha atrás a las excepciones aplicativas realizadas en la activación de la contingencia"

5. Validaciones.

6. Tareas de activación
   - Desactivar BLK Centro 2.
   - Desactivar Contingencia Harvest Centro 2.

Etapa 8: Preparación de la Lista de Personas y Organizaciones para Comunicarse en Caso de Emergencia

Se creará un directorio telefónico del personal considerado esencial para la organización en esas fechas críticas, incluyendo el personal encargado de realizar medidas preventivas y los responsables para las acciones de la recuperación y preparación de medios alternativos.

A su vez también se creará un listado telefónico de todos los proveedores de servicio del recurso.

Este directorio se usa para realizar comunicaciones rápidas con los proveedores de servicio del recurso, si ocurren los problemas, para hacer que investiguen y que identifiquen las causas de los problemas y que comiencen la recuperación de los sistemas.

Por motivos de privacidad estas tablas están sin informar.

Tabla 12 FUNCIONES Y CARGOS

Función		Empleado	Número	Número	Tiempo
Dirección	Cargo				

Etapa 9: Pruebas y Monitoreo

Una vez establecido dicho plan, se deberán realizar una serie de elementos de cara a la mejora continua y optimización de dicho plan:

- Pruebas funcionales en horarios fuera de SLA de al menos un entorno productivo conjuntamente con todos los departamentos implicados en el plan.

- Prueba funcional en cada uno de los entornos simulando a la activación de dicho plan tanto en pasos como en recursos.

- Una vez validado el plan, periódicamente lanzar validaciones de dicho plan siguiendo un calendario previamente establecido.

- En cada una de las validaciones citadas anteriormente, llevar un registro de incidencias de cara a plantearlas y solucionarlas con los departamentos implicados.

- Además, llevar un registro de lecciones aprendidas de cara a realizar una mejora continua de dicho proceso tanto en optimizaciones como en pasos nuevos a añadir.

6. Conclusiones

En la fase previa a la realización de este proyecto, se establecieron una serie de objetivos y retos a cumplir los cuales a continuación expondremos. Haciendo énfasis en las conclusiones obtenidas durante la realización de las tareas realizadas para llegar a ellos:

- **Reducir los tiempos de intervención durante las etapas del plan de contingencia TI**

  Antes del desarrollo de este proyecto, el actual plan de contingencia TI tenía muchas deficiencias, pero una de las más preocupantes era su elevado coste de tiempo que llevaba ejecutar este plan.

  A continuación os expondremos una tabla con los tiempos medios para cada elemento de nuestra infraestructura:

Tabla 13 Tiempos medios plan antiguo

Elemento de Gestion	Tiempo medio	Porcentaje Delegable a los operadores
Gestión de las BBDD	3 horas	100%
Gestión de los NFS	2 horas	100%
Gestión de los servidores Web	2 horas	100%
Gestión de los servidores de Aplicaciones	2 horas	100%
Gestión de la carga de tráfico	1 hora	100%
Gestión del DNS	1 hora	100%
Gestión de Colas de Mensajeria	1 hora	100%
Gestión de las distribuciones de SW	30 minutos	100%
TOTALES	12 horas 30 minutos	100%

Una vez realizado nuestro plan de mejora, durante 9 semanas realizamos un calendario de diferentes pruebas, en las cuales el tiempo medio fue disminuyendo hasta conseguir una media de una hora, el cual os presentamos mediante la siguiente tabla:

Tabla 14Tiempo Medio Plan nuevo

Fecha de la prueba	Tiempo empleado	Necesario soporte
Semana 1	3 horas	Si
Semana 3	2 horas	Si
Semana 5	2 horas	No
Semana 6	2 horas	Si
Semana 6 (Prueba Real, caida de CPD centro2)	1,5 hora	No
Semana 7	1,5 hora	No
Semana 8	1 hora	No
Semana 9	1 hora	No

Como se puede observar, tras el antiguo plan que nos ocupaba un total de 12,5 horas, hemos conseguido reducir el tiempo a casi 1 hora y sin necesidad de soporte a operación en bastantes casos.

- **Disminuir los recursos para la realización de la contingencia TI**

En lo referente a la utilización de recursos, aunque era menos preocupante, si conlleva un gasto de dinero y una malgasto del uso de los operadores que preocupaba.

En la siguiente tabla podemos ver el uso que hacíamos de los especialistas en caso de tener que activar el plan de contingencia:

Tabla 15 Uso de recursos plan antiguo

Elemento de Gestion	Recusos Utilizados	Disponibilidad de Guardia
Gestión de las BBDD	1 especialista + 1 técnico	Sí
Gestión de los NFS	1 especialista	Sí
Gestión de los servidores Web	1 especialista + 1 técnico	Sí
Gestión de los servidores de Aplicaciones		
Gestión de la carga de tráfico	1 especialista	Sí
Gestión del DNS	1 especialista	Sí

Gestión de Colas de Mensajeria	1 especialista	Sí
Gestión de las distribuciones de SW	1 especialista	Sí
TOTALES	12 horas 30 minutos	Todos

Los cuales tras la mejora del plan como es de prever tan solo hemos utilizado los siguientes en nuestras pruebas:

Tabla 16 Uso de recursos plan nuevo

Fecha de la prueba	Necesario soporte	Técnicos necesarios
Semana 1	Si	2
Semana 3	Si	2
Semana 5	No	0
Semana 6	Si	1
Semana 6 (Prueba Real, caida de CPD centro2)	No	0
Semana 7	No	0
Semana 8	No	0
Semana 9	No	0

Y cabe mencionar, que actualmente el ahorro de coste es enorme ya que antiguamente teníamos una media de 455€ como podemos ver en la siguiente tabla por cada intervención:

Tabla 17 Gasto del plan antiguo

Elemento de Gestion	Tiempo medio	Precio Hora Fuera de horario de oficina	Gasto Medio
Gestión de las BBDD	3 horas	35€	105€
Gestión de los NFS	2 horas	35€	70€
Gestión de los servidores Web	2 horas	35€	70€

Gestión de los servidores de Aplicaciones	2 horas	35€	70€
Gestión de la carga de tráfico	1 hora	35€	35€
Gestión del DNS	1 hora	35€	35€
Gestión de Colas de Mensajeria	1 hora	35€	35€
Gestión de las distribuciones de SW	30 minutos	35€	35€ (horas absolutas)
TOTALES	12 horas 30 minutos	-	455€

Cuando actualmente, casi no ha hecho falta el uso de soporte a los operadores como hemos indicado anteriormente, hemos ahorrado mucho porque no hemos necesitado casi soporte a los operadores por técnicos expertos en las pruebas que hemos ido haciendo del CPLAN.

De cara a futuro tendremos que hacer las revisiones oportunas mediante procesos de mejora continua para adaptar y mejorar el CPLAN a las tecnologías y procedimiento que puedan ayudarnos a mejorarlo. Se establecerán reuniones periódicas en las que revisaremos los resultados de las pruebas tanto reales como planificadas para poder establecer puntos de mejora del procedimiento.

Como conclusión final se puede indicar que se han cumplido todos los objetivos planteados al inicio del proyecto. Se ha realizado una documentación completa sobre las cómo realizar un plan de contingencia y se ha desarrollado la mejora de uno ya construido sacando un beneficio de tiempo, recursos y coste que era inimaginable poco antes de su desarrollo.

7. PLANIFICACIÓN Y PRESUPUESTO DEL PROYECTO

Tabla 18 planificación del proyecto de fin de carrera

Actividades	Inicio	Duración (días)	Fin	Horas de trabajo
Análisis previo del alcance del proyecto	01/12/2012	40	10/01/2013	20
Análisis detallado del alcance	10/01/2013	20	30/01/2013	15
Ejecución de las tareas	30/01/2013	250	07/10/2013	150
Generación de los informes	07/10/2013	10	17/10/2013	16
Ejecución de las correcciones	17/10/2013	650	29/07/2015	60
Cierre formal del proyecto	29/07/2015	55	22/09/2015	5
				266

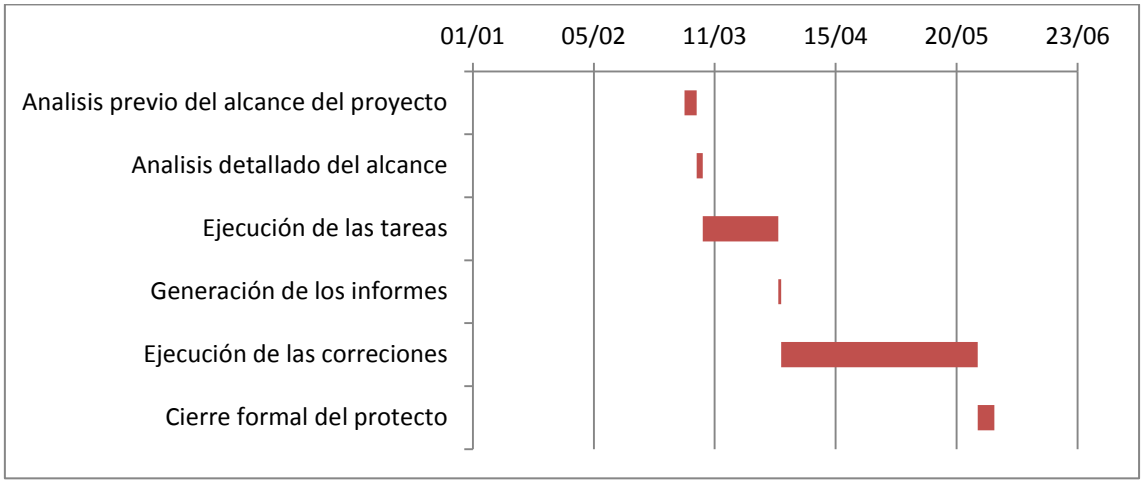

Ilustración 22 Planificación del proyecto de fin de carrera

El presupuesto final del proyecto sería un total de 10640€ (40 €/hora) desglosado en las siguientes tareas (no hay coste de recursos materiales porque no se ha utilizado material ya amortizado):

- Análisis previo del alcance del proyecto: 20 horas
- Análisis detallado del alcance: 15 horas
- Ejecución de las tareas: 150 horas
- Generación de los informes: 16 horas
- Ejecución de las correcciones: 60 horas
- Cierre formal del proyecto: 5 horas

8. TABLAS

9. ILUSTRACIONES

10. REFERENCIAS

[i] Paul Cunningham, Miriam Cunningham. (2009). *Service Level Agreements in Virtualised Service Platforms. IIMC International Information Management Corporation.*

[ii] ITIL Process Maps. *ITIL Gestion de la Continuidad del Servicio de TI – ITSCM* <http://wiki.es.it-processmaps.com/index.php/ITIL_Gestion_de_la_Continuidad_del_Servicio_de_TI_-_ITSCM>

[iii] Bridged world. *Planes de Contingencia* <http://www.bridgedworld.com/es/soluciones/planes-de-contingencia>

[iv] REDHAT. *Red Hat Enterprise Linux* <http://www.redhat.com/en/technologies/linux-platforms/enterprise-linux>

[v] ORACLE. *Oracle Database* <https://www.oracle.com/database/index.html>

[vi] The GNU Operating System and the Free Software Movement . *GNU Bash* <https://www.gnu.org/software/bash/>

[vii] Linux NFS faq – SourceForge. *Linux NFS* <http://nfs.sourceforge.net/>

[viii] The Apache HTTP Server Project. *Apache* http://httpd.apache.org/

[ix] IBM - Archives - History of IBM - United States. *WebSphere Application Server* <http://www-03.ibm.com/software/products/en/appserv-was>

[x] F5 Networks Inc. *Load Balancer* <https://f5.com/glossary/load-balancer>

[xi] Wireless/Networking - About.com . *DNS Server* <http://compnetworking.about.com/od/dns_domainnamesystem/f/dns_servers.htm>

[xii] IBM - Archives - History of IBM - United States. *IBM MQ* <http://www-03.ibm.com/software/products/en/ibm-mq>

[xiii] CA Technologies. *CA Harvest Software Change Manager* <http://www.ca.com/es/devcenter/ca-harvest-software-change-manager.aspx>

[xiv] Computer Security Resource Center. *Contingency Planning Guide for Federal* Information Systems <http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf>

[xv] National Institute of Standars and Technology <http://www.nist.gov/>

[xvi] GMV Innovating Solutions . *GESTIÓN DE LA CONTINUIDAD DE NEGOCIO* <http://www.gmv.com/export/sites/gmv/DocumentosPDF/SeguridadInfo-Documentacion/CONTINUIDAD_DE_NEGOCIO_ESP.pdf>

[xvii] ITIL® Foundation. *ITSCM: Evaluación de riesgos* <http://itilv3.osiatis.es/diseno_servicios_TI/gestion_continuidad_servicios_ti/evaluacion_riesgos.php>

[xviii] ITIL® Foundation. *ITSCM: Estrategias* <http://itil.osiatis.es/Curso_ITIL/Gestion_Servicios_TI/gestion_de_la_continuidad_del_servicio/proceso_gestion_de_la_continuidad_del_servicio/estrategia_de_continuidad_del_servicio.php>

[xix] Bodoff, Stephanie (2004). *The J2EE Tutorial.* Boston: Addison-Wesley.